Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 DS-GVO

Zwischen

– im Folgenden **„Auftraggeber“**
bzw. „Verantwortlicher“ –

und der

Töns GmbH & Co. KG

Hauptstraße 59

66953 Pirmasens

– im Folgenden **„Auftragnehmer“**
bzw. „Auftragsverarbeiter“ –

wird folgende Vereinbarung geschlossen:

Inhalt

1. Zusammenarbeit und Auswahl des Auftragsverarbeiters 3
2. Dauer des Auftrags 3
3. Art und Zweck der Verarbeitung, Kategorien betroffener Personen 3
4. Ort der Datenverarbeitung 4
5. Pflichten des Auftragnehmers als Auftragsverarbeiter 4
6. Technische und organisatorische Maßnahmen 6
7. Unterauftragsverhältnisse 6
8. Bestellung eines Datenschutzbeauftragten 7
9. Rechte und Pflichten des Auftraggebers 7
10. Weisungsbefugnis des Auftraggebers 8
11. Zusammenarbeit mit den Aufsichtsbehörden / Verarbeitungsverzeichnisse 8
12. Maßnahmen bei Datenschutzverletzungen 8
13. Haftung 9
14. Umgang mit den Daten nach Beendigung des Auftrags 10
15. Schlussbestimmungen 10
Anlagen: 11
A 1 Datenkategorien/ Betroffenengruppen 12
A 2 Kontaktdaten 13
A 3 Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO 12
A 4 Subunternehmerliste 17

1. Zusammenarbeit und Auswahl des Auftragsverarbeiters

1.1. Zwischen dem Auftraggeber und der Töns GmbH & Co. KG als Auftragnehmer besteht eine Zusammenarbeit über Leistungen im IT-Umfeld. Da es im Rahmen der Durchführung dieser Leistungen möglich oder für die Auftragserfüllung notwendig sein kann, dass der Auftragnehmer Zugriff auf personenbezogene Daten erhält, bedarf es gemäß Art. 28 Abs. 3 S. 1 DS-GVO zwischen dem Auftraggeber als Verantwortlichen und dem Auftragnehmer als Auftragsverarbeiter einer vertraglichen Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag.

1.2. Der Auftragsverarbeiter hat die DS-GVO in seinem Unternehmen umgesetzt. Hierüber existiert eine umfangreiche Dokumentation, die beim Auftragsverarbeiter eingesehen werden kann. Damit erfüllt der Auftragsverarbeiter die Anforderungen nach Art. 28 Abs. 1 DS-GVO.

1.3. Die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO obliegt allein der Verantwortung des Auftraggebers.

2. Dauer des Auftrags

2.1. Die Dauer der Datenverarbeitung im Auftrag (Vertragslaufzeit) richtet sich nach der Laufzeit des zwischen den Parteien geschlossenen Hauptvertrags.

2.2. Darüber hinaus ist eine vorzeitige Beendigung dieses Auftrags, ohne Einhaltung einer Kündigungsfrist im Falle einer schwerwiegenden Verletzung von gesetzlichen oder vertraglichen Datenschutzbestimmungen zulässig, sofern ein Festhalten an dieser Vereinbarung für die jeweilige Vertragspartei nicht zumutbar ist.

2.3. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt eine schwerwiegende Verletzung dar.

3. Art und Zweck der Verarbeitung, Kategorien betroffener Personen

3.1. Der Umfang, die Art und der Zweck der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten richtet sich nach den im zwischen den Parteien im Hauptvertrag konkret vereinbarten Leistungen. Das Leistungsspektrum des Auftragnehmers umfasst Leistungen in den Bereichen Büromaterial, Lösungen für Dokumenten-Management, Büromöbelsysteme und Bürotechnik. Dabei bietet der Auftragnehmer insbesondere auch die Leistungsbilder IT-Fernwartung, -Monitoring und Datensicherung an. Dafür erhält der Auftragnehmer Zugriff auf die Kundensysteme soweit dies für die Auftragserfüllung notwendig ist.

3.2. Der Auftragnehmer verarbeitet dabei die personenbezogenen Daten des Auftraggebers ausschließlich im Auftrag und nach Weisung des Auftraggebers gemäß dem vorliegenden Vertrag.

3.3. Der Auftraggeber ist dafür verantwortlich die Datenkategorien und die Kategorien der Betroffenen die im Rahmen der Vertragserfüllung durch den Auftragnehmer im Auftrag verarbeitet werden in einer Anlage zu diesem Vertrag auszuweisen. Darüber hinaus besteht die Pflicht zur fortlaufenden Prüfung und Ergänzung der Anlage 1, soweit durch weitere Beauftragungen neue Kategorien hinzukommen können.

4. Ort der Datenverarbeitung

4.1. Die Verarbeitung und Nutzung der Daten durch den Auftraggeber findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

4.2. Die Übermittlung personenbezogener Daten in ein Drittland oder an internationale Organisationen bedarf der vorherigen Zustimmung des Auftraggebers. Sie wird nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 bis 50 DS-GVO erfüllt sind.

5. Pflichten des Auftragnehmers als Auftragsverarbeiter

5.1. Der Auftragnehmer und ihm unterstellte Personen, die Zugang zu den personenbezogenen Daten haben, werden die personenbezogenen Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind (Art. 29 DS-GVO).

5.2. Der Auftragnehmer beachtet, dass alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf die für die Auftragsverarbeitung einschlägigen rechtlichen Vorschriften der DS-GVO und das Datengeheimnis verpflichtet sind und über die sich aus diesem Auftrag ergebende Weisungs- bzw. Zweckbindung belehrt wurden.

5.3. Der Auftragnehmer wird die Datenverarbeitung mittels geeigneter technischer und

organisatorischer Maßnahmen gemäß Art. 32 DS-GVO durchführen.

5.4. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit dabei unterstützen, seinen Pflichten hinsichtlich der in Art. 16 bis 20 und Art. 32 bis 36 DS-GVO genannten Rechte der betroffenen Personen nachkommen zu können.

5.5. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen als die vereinbarten, insbesondere nicht für eigene Zwecke.

5.6. Der Auftragnehmer wird den Auftraggeber darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 S. 3 DS-GVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

5.7. Der Auftragnehmer wird dem Auftraggeber alle erforderlichen Informationen im Hinblick auf die Kontrollverpflichtungen des Auftraggebers zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und unterstützen. Der Auftraggeber hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung der gesetzlichen Pflichten und dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

6. Technische und organisatorische Maßnahmen

6.1. Der Auftragnehmer ist gemäß Art. 28 Abs. 3 S. 2 lit. c DS-GVO verpflichtet, diejenigen technischen und organisatorischen Maßnahmen (TOM) zu treffen und während der Vertragslaufzeit aufrechtzuerhalten, die erforderlich sind, um die in Art. 32 DS-GVO genannten Anforderungen zu gewährleisten. Der Auftragnehmer hat seine TOM in einer Anlage zu diesem Vertrag zusammengefasst.

6.2. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

6.3. Die technischen und organisatorischen Maßnahmen unterliegen dem Stand der Technik und dem technischen Fortschritt. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen und Produkte um- und einzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen.

7. Unterauftragsverhältnisse

7.1. Der Auftragnehmer nimmt Auftragsverarbeiter als Subunternehmer nicht ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragnehmer den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

7.2. Nimmt der Auftragnehmer die Dienste eines Subunternehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag zwischen dem Auftraggeber als Verantwortlichen und dem Auftragnehmer als Auftragsverarbeiter festgelegt sind. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer als Auftragsverarbeiter gegenüber dem Auftraggeber als Verantwortlichen für die Einhaltung der Pflichten des Subunternehmers.

7.3. Bei der Unterbeauftragung sind dem Auftraggeber Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragnehmer einzuräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

7.4. Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

7.5. Für die bereits zum Zeitpunkt des Abschlusses dieses Vertrages feststehenden Subunternehmer erfolgt die schriftliche Genehmigung für die in einer Anlage zu diesem Vertrag benannten juristischen oder natürlichen Personen.

7.6. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme, vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

8. Bestellung eines Datenschutzbeauftragten

8.1. Der Auftragnehmer verpflichtet sich zur schriftlichen Bestellung eines Datenschutzbeauftragten, soweit gesetzlich vorgeschrieben, gemäß Art. 37 DS-GVO.

8.2. Die Kontaktdaten des bestellten Datenschutzbeauftragten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme in einer Anlage zu diesem Vertrag mitgeteilt.

9. Rechte und Pflichten des Auftraggebers

9.1. Der Auftraggeber ist im Verhältnis zum Auftragnehmer wie ein Eigentümer der Daten anzusehen (§ 903 BGB analog) und Inhaber aller etwaigen Rechte.

9.2. Der Auftraggeber als Verantwortlicher ist gemäß Art. 5 Abs. 2 DS-GVO für die Einhaltung der in Art. 5 Abs. 1 DS-GVO festgeschriebenen Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich (Rechenschaftspflicht).

9.3. Der Auftraggeber ist für die rechtmäßige Erhebung, Verarbeitung und Nutzung der Daten sowie für die Implementierung eigener geeigneter technischer und organisatorischer Maßnahmen und die Wahrung der Betroffenenrechte verantwortlich.

9.4. Der Auftraggeber hat den Auftragnehmer unverzüglich darüber zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

9.5. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse über Geschäftsgeheimnisse und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrags bestehen.

10. Weisungsbefugnis des Auftraggebers

10.1. Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers gemäß Art. 29 DS-GVO. Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

10.2. Der Weisungsberechtigte auf Seiten des Auftraggebers sowie der Weisungsempfänger auf Seiten des Auftragnehmers sind schriftlich zu fixieren. Dies erfolgt in einer Anlage zu diesem Vertrag. Bei einem Wechsel der zuständigen Ansprechpartner ist dem Vertragspartner unverzüglich und schriftlich der jeweilige Nachfolger mit Kontaktdaten mitzuteilen.

11. Zusammenarbeit mit den Aufsichtsbehörden / Verarbeitungsverzeichnisse

11.1. Dem Auftragnehmer ist bekannt, dass er gemäß Art. 31 DS-GVO verpflichtet ist, auf Anfrage mit dem Auftraggeber und der Aufsichtsbehörde bei der Erfüllung von Aufgaben zusammenzuarbeiten.

11.2. Dem Auftragnehmer ist bekannt, dass er gemäß Art. 30 Abs. 2 DS-GVO verpflichtet ist, ein eigenes Verzeichnis von Verarbeitungstätigkeiten für alle Kategorien von im Auftrag durchgeführten Tätigkeiten der Verarbeitung zu führen. Diese müssen der Aufsichtsbehörde auf Anfrage vorgelegt werden.

12. Maßnahmen bei Datenschutzverletzungen

12.1. Der Auftragnehmer ist gemäß Art. 33 Abs. 2 DS-GVO verpflichtet, jede ihm bekanntwerdende Verletzung des Schutzes personenbezogener Daten unverzüglich an den Verantwortlichen zu melden.

12.2. Der Auftragnehmer erstattet dem Auftraggeber in allen Fällen und unverzüglich eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

12.3. Der Auftragnehmer verpflichtet sich darüber hinaus unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen, den Auftraggeber bei den zu ergreifenden Maßnahmen und Meldepflichten gemäß Art. 33 und 34 DS-GVO zu unterstützen.

13. Haftung

13.1. Die nachfolgenden Haftungsklauseln betreffen ausschließlich das Vertragsverhältnis zwischen dem Auftraggeber und dem Auftragnehmer. Sie stellen keine Ausschlussklausel im Hinblick auf die Betroffenenrechte nach Art. 82 Abs. 1 DS-GVO dar.

13.2. Die Haftung des Auftragnehmers, seiner gesetzlichen Vertreter und Erfüllungsgehilfen, gleich aus welchem Rechtsgrund, ist unbegrenzt für Schäden, die vorsätzlich oder grob fahrlässig verursacht werden oder die aus der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit resultieren.

13.3. Der Auftragnehmer, seine gesetzlichen Vertreter oder Erfüllungsgehilfen haften nicht bei leichter Fahrlässigkeit. Dieser Ausschluss für die Haftung bei leichter Fahrlässigkeit gilt jedoch dann nicht, wenn es sich um die Verletzung einer wesentlichen Vertragspflicht (Kardinalpflicht) handelt. Kardinalpflichten bzw. wesentliche Vertragspflichten sind solche Pflichten des Auftragnehmers, deren Erfüllung die ordnungsgemäße Durchführung dieses konkreten Vertrages überhaupt erst ermöglichen und auf deren Einhaltung der Kunde regelmäßig vertrauen darf; mithin also Pflichten, deren Verletzung ein Erreichen des Vertragszwecks gefährden würde.

13.4. Wenn und soweit der Auftragnehmer, seine gesetzlichen Vertreter und Erfüllungsgehilfen für leichte Fahrlässigkeit haften, ist die Haftung bei Sach- und Vermögensschäden auf den vertragstypischen und vorhersehbaren Schaden beschränkt. Die Haftung für sonstige, entfernte Folgeschäden ist ausgeschlossen.

13.5. Alle Schadensersatzansprüche des Auftraggebers gegen den Auftragnehmer verjähren in 12 Monaten ab Schadensfall. Dies gilt nicht für Ansprüche wegen unerlaubter Handlung oder vorsätzlicher Schädigung.

13.6. Soweit die Haftung des Auftragnehmers ausgeschlossen ist, gilt dies auch für die persönliche Haftung der Angestellten, Arbeitnehmer, Mitarbeiter, Vertreter und Erfüllungsgehilfen des Auftragnehmers.

13.7. Der Auftragnehmer haftet im Innenverhältnis zum Auftraggeber dann nicht, wenn er den Nachweis nach Art. 82 Abs. 3 DS-GVO erbringt.

14. Umgang mit den Daten nach Beendigung des Auftrags

14.1. Gemäß Art. 28 Abs. 3 S. 2 lit. g DS-GVO wird der Auftragnehmer nach Wahl des Auftraggebers nach Abschluss der Erbringung der Verarbeitungsleistungen, spätestens aber mit Beendigung der Leistungsvereinbarung sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse, sowie Datenbestände dem Auftraggeber aushändigen oder nach vorheriger Zustimmung datenschutzgerecht vernichten, soweit nicht das Unionsrecht oder das Recht der Mitgliedstaaten eine Speicherung der personenbezogenen Daten vorschreibt.

14.2. Ein Löschen bzw. Vernichten von Daten ist dem Auftraggeber mit Zeitangabe schriftlich zu bestätigen. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind darüber hinaus durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

15. Schlussbestimmungen

15.1. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, so bleiben die übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelungen eine solche rechtlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelungen am nächsten kommt.

15.2. Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere einem Hauptvertrag, gehen die Regelungen dieses Vertrags vor. Nebenabreden, Änderungen und Ergänzungen dieses Vertrages bedürfen der Schriftform. Dies gilt auch für die Änderung dieser Schriftformvereinbarung.

15.3. Dieser Vertrag und alle im Rahmen seiner Durchführung geschlossenen Rechtsgeschäfte unterliegen deutschem Recht unter Ausschluss des internationalen UN-Kaufrechts (UNCITRAL).

15.4. Für alle Streitigkeiten aus diesem Vertrag gilt der gesetzliche Gerichtsstand.

15.5. Alle zu diesem Vertrag geführten Anlagen (A 1 bis einschließlich A 4) sind Vertragsbestandteil.

_____	Pirmasens, 01.01.2021
Ort / Datum	Ort / Datum
Auftraggeber	Töns GmbH & Co. KG

Anlagen:

A 1 Datenkategorien/ Betroffenengruppen

Art der Daten

Gegenstand der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien:

- ☐ Personenstammdaten (z.B. Name, Vorname, Anschrift und Geburtsdatum)
- ☐ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☐ Vertragsstammdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☐ Vertragsabrechnungs- und Zahlungsdaten (z.B. Lohn, Gehalt und Reisekosten)
- ☐ IT-Nutzungsdaten (z.B. UserID, Passwörter und Rollen)
- ☐ Bankdaten (z.B. Kontoverbindung und Kreditkartennummer)
- ☐ Bonitätsdaten (z.B. Zahlungsverhalten und Bilanzen)
- ☐ Sonstige:

Kreis der Betroffenen

Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen, umfasst:

- ☐ Kunden / Leistungsempfänger des Auftraggebers
- ☐ Beschäftigte des Auftraggebers
- ☐ Lieferanten / Dienstleister des Auftraggebers
- ☐ Sonstige:

A 2 Kontaktdaten

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner die Nachfolger bzw. die Vertreter mitzuteilen.

1. Weisungsberechtigte und Weisungsempfänger

Auftraggeber als Weisungsberechtigter

Name	Telefon	E-Mail

Töns GmbH & Co. KG als Weisungsempfänger

Name	Telefon	E-Mail
Ulli Könnel	+49 631 341 55 0	u.koennel@toens.de
Johannes Schröter	+49 631 341 55 0	dispatch@toens.de
Torben Christmann	+49 631 341 55 0	t.christmann@toens.de

2. Datenschutzbeauftragter des Auftraggebers

Name	Telefon	E-Mail

3. Kontaktdaten Datenschutzbeauftragter der Töns GmbH & Co. KG

Telefon	E-Mail	
+49 (0) 6331 266 00	datenschutz@toens.de	

A 3 Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO

Es wird vom Auftragnehmer ein für die konkrete Auftragsverarbeitung angemessenes Schutzniveau gewährleistet. Dies wird wie folgt beschrieben:

1. Pseudonymisierung

Die Pseudonymisierung ist wie folgt umgesetzt:

☒ Verwendung von (Personal-, Kunden- oder Patienten-) Kennziffern statt Namen

☒ Vier-Augen-Prinzip zur Identifikation

2. Maßnahmen zur Verschlüsselung

☒ Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones

☒ Verschlüsselung von mobilen Speichermedien (CD / DVD- ROM, USB-Stick, externe Festplatten)

☒ Verschlüsselung von Dateien

☒ Verschlüsselte Aufbewahrung von Passwörtern

☒ Verschlüsselung von Email bzw. Email-Anhängen

☒ Gesicherte Datenweitergabe (z.B. SSL, FTPS, TLS)

☒ Gesichertes WLAN

3. Maßnahmen zur Sicherstellung von Vertraulichkeit

a. *<u>Maßnahmen, durch die Unbefugten der Zutritt verwehrt wird:</u>*

☒ Zutrittskontrollsystem, Ausweisleser (Magnet / Chipkarte)

☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)

☒ Sicherheitstüren / -fenster

☒ Zaun-Anlagen

☒ Schlüsselverwaltung / Dokumentation der Schlüsselvergabe

☒ Alarmanlage

☒ Videoüberwachung

☒ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern

☒ Nicht-reversible Vernichtung von Datenträgern

☒ Besucherregelung (z.B. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)

b. *Maßnahmen, die verhindern, dass Unbefugte die Verarbeitungssysteme nutzen können:*

☒ Persönlicher und individueller User-Log-In bei der Anmeldung am System bzw. am Unternehmensnetzwerk
☒ Autorisierungsprozess für Zugangsberechtigungen
☒ Begrenzung der befugten Benutzer
☒ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
☒ Personalisierte Chipkarten, Token, PIN / TAN, etc.
☒ Protokollierung des Zugangs
☒ Zusätzlicher System-Log-In für bestimmte Anwendungen
☒ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne User-Aktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
☒ Firewall

c. *Maßnahmen, die gewährleisten, dass nur berechtigte Personen auf die Verarbeitungssysteme zugreifen und personenbezogene Daten nicht unbefugt lesen, kopieren, verändern oder entfernen können:*

☒ Verwaltung und Dokumentation von differenzierten Berechtigungen
☒ Auswertungen / Protokollierungen von Datenverarbeitungen
☒ Autorisierungsprozess für Berechtigungen
☒ Profile / Rollen
☒ Verschlüsselung von CD / DVD- ROM, externen Festplatten und / oder Laptops (etwa per Betriebssystem, Safe Guard Easy, PGP)
☒ Funktionstrennung „Segregation of Duties“
☒ Fachkundige Akten- und Datenträgervernichtung, gemäß DIN 66399
☒ Nicht-reversible Löschung von Datenträgern

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

☒ Speicherung der Datensätze in physikalisch getrennten Datenbanken
☒ Getrennte Systeme
☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit

☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

☒ Mandantenfähigkeit von IT-Systemen

☒ Verwendung von Testdaten

☒ Trennung von Entwicklungs- und Produktionsumgebung

4. Maßnahmen zur Sicherstellung von Integrität

☒ Zugriffsrechte

☒ Systemseitige Protokollierungen

☒ Dokumenten Management System (DMS) mit Änderungshistorie

☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten

☒ Mehraugenprinzip

☒ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)

5. Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

☒ Sicherheitskonzept für Software- und IT-Anwendungen

☒ Back-Up Verfahren

☒ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)

☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk

☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates

☒ Spiegeln von Festplatten

☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)

☒ Geeignete Archivierungsräumlichkeiten für Papierdokumente

☒ Brand- und / oder Löschwasserschutz des Serverraums

☒ Brand- und / oder Löschwasserschutz der Archivierungsräumlichkeiten

☒ Klimatisierter Serverraum

☒ Virenschutz

☒ Firewall

☒ Notfallplan

☒ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)

6. Maßnahmen zur Sicherstellung der Belastbarkeit

☒ Ausreichende Kapazität von IT-Systeme und Anlagen

☒ Redundante Systeme / Anlagen

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit

☒ Verfahren für regelmäßige Kontrollen / Audits

☒ Konzept für regelmäßige Überprüfung, Bewertung und Evaluierung

☒ Notfalltests

8. Weisungskontrolle / Auftragskontrolle

☒ Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 Abs. 3 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragsverarbeiters und Verantwortlichen.

☒ Prozess zur Erteilung und / oder Befolgung von Weisungen

☒ Bestimmung von Ansprechpartnern und / oder verantwortlichen Mitarbeitern

☒ Schulungen / Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragsverarbeiter

☒ Verpflichtung der Mitarbeiter zur Vertraulichkeit

☒ Benennung eines Datenschutzbeauftragten gemäß Art. 37 ff. DS-GVO

☒ Datenschutzmanager / -koordinator

☒ Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DS-GVO

☒ Dokumentations- und Eskalationsprozess für Verletzungen des Schutzes personenbezogener Daten

☒ Richtlinien / Vorgaben zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Sicherheit der Verarbeitung

☒ Prozess zur Weiterleitung von Betroffenenanfragen

A 4 Subunternehmerliste

Unterauftragnehmer (Firma, Anschrift, Ansprechpartner)	**Verarbeitete Datenkategorien**	**Verarbeitungsschritte / Zweck der Unterauftragsverarbeitung**
ALSO Deutschland GmbH Lange Wende 43 59494 Soest	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
DIS Daten-IT-Service Mainhardter Weg 11 71577 Grosserlach	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
EBERT LANG Distribution GmbH Garbenheimer Str. 36 35578 Wetzlar	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
ELO Digital Office GmbH Tübinger Str. 43 70178 Stuttgart	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
Fujitsu Technology Solution GmbH Mies-van-der-Rohe-Str. 8 80807 München	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
HP Deutschland GmbH Schikardstr. 32 71034 Böblingen	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
Microsoft Deutschland GmbH Konrad-Zuse-Str. 1 85716 Unterschleißheim	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen

ProLogis GmbH Hagsdorfer Straße 3 85368 Sixthaselbach	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
RICOH Deutschland GmbH Vahrenwalder Str. 315 30179 Hannover	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
Sophos Ltd The Pentagon, Abingdon Science Park Vereinigtes Königreich	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
TeamViewer GmbH Jahnstr. 30 73037 Göppingen	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
Telekom Deutschland GmbH Landgrabenweg 151 53227 Bonn	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen
Veeam Software GmbH Konrad-Zuse-Platz 8 81829 München	Datenkategorien gemäß Anlage 1 (A1)	Supportdienstleistungen