Verarbeiter-Vereinbarung

Datum: 19-06-2026

Version: 9.0

DIE UNTERZEICHNENDEN:

_____,
eingerichtet unter _____, in diesem Fall gesetzlich vertreten durch _____
(Titel, Name und Funktion) (nachfolgend „Auftraggeber“ genannt)

und

Archive-IT Crossen GmbH, mit Sitz in der Am Rautenanger 2, D-07613 CROSSEN AN DER ELSTER eingetragen im Register der Handelskammer unter der Nummer HRB 508264, Prozessbevollmächtigter: P. de Meulemeester, CEO (nachfolgend „Auftragnehmer“ genannt).

- nachfolgend zusammen die „Parteien“ genannt -

1. PRÄAMBEL

Für diesen Auftragsverarbeitungsvertrag gelten die Begriffe und Definitionen der Verordnung (EU) 2016/679 (nachfolgend „DSGVO“), insbesondere des Art. 4 DSGVO.

1. GEGENSTAND

1.1 Gegenstand dieses Auftragsverarbeitungsvertrages ist die Festlegung des datenschutzrechtlichen Rahmens für die vertraglichen Beziehungen zwischen den Parteien.

1.2 Die Beschreibung des jeweiligen Auftrags mit den Angaben über Gegenstand des Auftrags, Umfang, Art und Zweck der Datenverarbeitung, Art der personenbezogenen Daten sowie Kategorien der betroffenen Personen befindet sich in der Anlage unter der Ziffer 1.

2. ORT DER DATENVERARBEITUNG

2.1 Die vertraglich vereinbarte Verarbeitung durch den Auftragnehmer findet in höchstpersönlicher Form, d.h. durch eigene Mitarbeiter, ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, sofern sich aus der Anlage nichts anderes ergibt. Jede Verlagerung der Verarbeitung in ein Drittland bedarf der vorherigen ausdrücklichen Einwilligung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen für die Übermittlung in ein Drittland nach Art. 44 ff. DSGVO erfüllt sind. Andernfalls wird der Auftragnehmer diese unterlassen.

3. LAUFZEIT

3.1 Dieser Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Partei mit einer Frist von drei Monaten ordentlich gekündigt werden. Soweit im Zeitpunkt der Kündigung noch ein Hauptvertrag oder mehrere Hauptverträge, bei denen der Auftragnehmer im Auftrag personenbezogene Daten des Auftraggebers verarbeitet, in Kraft sind, gelten die Bestimmungen dieses Vertrages bis zu der regulären Beendigung des Hauptvertrages/der Hauptverträge fort.

3.2 Das Recht zur außerordentlichen, fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Der Auftraggeber kann diesen Vertrag ohne Einhaltung einer Frist insbesondere kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

4. WEISUNG

4.1 Der Auftragnehmer verarbeitet die personenbezogenen Daten nur im Rahmen der vom Auftraggeber erteilten Weisungen. Dies gilt nicht, soweit der Auftragnehmer durch zwingendes Recht, insbesondere das Recht der EU oder der Mitgliedsstaaten, dem der Auftragnehmer unterliegt, zur Verarbeitung verpflichtet ist. In diesem Fall teilt der Auftragnehmer diese rechtlichen Anforderungen vor der Verarbeitung in Schrift- oder Textform mit, es sei denn, die Mitteilung ist durch das betreffende Recht wegen eines wichtigen öffentlichen Interesses verboten.

4.2 Falls Weisungen, die unter Ziffer 1 der Anlage dieses Vertrages getroffenen Festlegungen ändern, aufheben oder ergänzen, sind sie nur zulässig, wenn eine entsprechende neue Vereinbarung erfolgt.

4.3 Unabhängig von der Form der Erteilung dokumentieren sowohl der Auftragnehmer als auch der Auftraggeber jede Weisung des Auftraggebers in Textform. Die Weisungen sind für ihre Geltungsdauer dieses Vertrages und anschließend noch für drei Jahre von den Parteien aufzubewahren.

4.4 Der Auftragnehmer weist den Auftraggeber unverzüglich darauf hin, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen gesetzliche Vorschriften verstößt. In einem solchen Fall ist der Auftragnehmer nach rechtzeitiger vorheriger Ankündigung gegenüber dem Auftraggeber berechtigt, die Ausführung der Weisung auszusetzen, bis der Auftraggeber die Weisung geändert hat oder diese bestätigt. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers bei objektiver Betrachtung zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

4.5 Der Auftraggeber legt den oder die Weisungsberechtigten fest. Der Auftragnehmer legt Weisungsempfänger fest. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und in schriftlicher oder elektronischer Form die Nachfolger oder Vertreter mitzuteilen.

5. UNTERSTÜTZUNGSPFLICHTEN DES AUFTRAGNEHMERS

5.1 Der Auftragnehmer ergreift angesichts der Art der Verarbeitung geeignete technische und organisatorische Maßnahmen (z.B. Aufbau eines Speicherverzeichnisses), um den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen der betroffenen Personen nach Art. 12 bis 22 DSGVO zu unterstützen.

5.2 Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer den Verantwortlichen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO z.B. durch unverzügliche Erteilung von benötigten Auskünften. Im Einzelnen bei der Sicherheit der Verarbeitung, bei Meldungen von Verletzungen an die Aufsichtsbehörde, der Benachrichtigung betroffener Personen bei einer Verletzung, der Datenschutz-Folgeabschätzung und bei der Konsultation der zuständigen Aufsichtsbehörde.

5.3 Sofern sich eine betroffene Person oder eine Datenschutzaufsichtsbehörde im Zusammenhang mit den unter dieser Vereinbarung verarbeiteten personenbezogenen Daten direkt an den Auftragnehmer wendet, informiert der Auftragnehmer den Auftraggeber hierüber unverzüglich und stimmt die weiteren Schritte mit ihm ab.

6. PRÜFUNGSRECHTE DES AUFTRAGGEBERS

6.1 Der Auftragnehmer stellt dem Auftraggeber auf dessen Anfrage unverzüglich unentgeltlich alle erforderlichen Informationen zum Nachweis der in diesem Vertrag und Art. 28 DSGVO geregelten Pflichten zur Verfügung. Insbesondere erteilt der Auftragnehmer dem Auftraggeber unverzüglich Auskünfte über die gespeicherten Daten und die Datenverarbeitungsprogramme.

6.2 Der Auftraggeber oder von ihm beauftragte Dritte sind mit angemessener Ankündigungsfrist, bei Vorliegen eines wichtigen Grunds (z.B. objektive

Anhaltspunkte für einen Verstoß gegen die aus dieser Vereinbarung übernommenen Verpflichtungen) während der üblichen Betriebszeiten des Auftragnehmers berechtigt, die Einhaltung der Pflichten aus diesem Vertrag und aus Art. 28 DSGVO zu überprüfen und beim Auftragnehmer Inspektionen vor Ort durchzuführen. Der Auftragnehmer ermöglicht dies und trägt dazu bei. Die Parteien verpflichten sich dabei alle datenschutzrechtlichen Belange, insbesondere in Bezug auf Daten Dritter, zu berücksichtigen.

6.3 Der Auftragnehmer hat dem Auftraggeber auf Anforderung jeweils unverzüglich geeigneten Nachweis über die Einhaltungen der Verpflichtungen gemäß Art. 28 Abs. 1 und Abs. 4 DSGVO zu erbringen. Dieser Nachweis kann durch die Bereitstellung von Dokumenten und Zertifikaten, die genehmigten Verhaltensregeln i. S. v. Art. 40 DSGVO oder genehmigten Zertifizierungsverfahren i. S. v. Art. 42 DSGVO abbilden, erbracht werden.

7. DATENSCHUTZBEAUFTRAGTER DES AUFTRAGNEHMERS

7.1 Der Datenschutzbeauftragte des Auftragnehmers ist in der Anlage dieses Vertrages unter Ziffer 3 angeführt, soweit für den Auftragnehmer ein Datenschutzbeauftragter bestellt sein muss oder freiwillig bestellt ist.

8. VERTRAULICHKEIT

8.1 Der Auftragnehmer gewährleistet, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er wahrt bei der Verarbeitung der personenbezogenen Daten des Auftraggebers das Datengeheimnis sowie die Vertraulichkeit, soweit nicht eine gesetzliche oder behördliche Offenbarungsverpflichtung besteht. Diese Pflicht besteht auch nach Beendigung dieses Vertragsverhältnisses für einen Zeitraum von 5 Jahren fort, soweit nicht eine gesetzliche längere Pflicht zur Einhaltung besteht.

8.2 Der Auftragnehmer gewährleistet, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Er verpflichtet diese Mitarbeiter durch schriftliche Vereinbarung für die Zeit der Tätigkeit und auch nach Beendigung des Beschäftigungsverhältnisses (soweit arbeitsrechtlich zulässig) zur Wahrung der Vertraulichkeit, sofern sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Unternehmen.

8.3 Auskünfte an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Einwilligung in einem elektronischen Format, durch den Auftraggeber erteilen.

9. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

9.1 Der Auftragnehmer führt geeignete technische und organisatorische Maßnahmen so durch, dass die Verarbeitung jeweils stets im Einklang mit den Anforderungen der

DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist. Er gestaltet seine innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des einschlägigen Datenschutzrechtes gerecht wird und ein danach angemessenes Schutzniveau erreicht wird. Insbesondere gewährleistet der Auftragnehmer unter Berücksichtigung des jeweiligen Stands der Technik während der Vertragslaufzeit die angemessene Sicherheit der Verarbeitung, insbesondere die Vertraulichkeit (inklusive Pseudonymisierung und Verschlüsselung), Verfügbarkeit, Integrität, und Belastbarkeit der für die Datenverarbeitung verwendeten Systeme und Dienstleistungen.

9.2 Die vollständig ausgefüllte Vorlage für technische und organisatorische Maßnahmen in der Anlage oder ein eigenes Sicherheitskonzept des Auftragnehmers wird als verbindlich festgelegt. Die Auswahl zwischen diesen beiden Alternativen kann in Ziffer 5 der Anlage getroffen werden.

9.3 Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen Weiterentwicklung angepasst werden. Dabei müssen die angepassten Maßnahmen mindestens dem Sicherheitsniveau der in der Anlage unter der Ziffer 5 vereinbarten Maßnahmen entsprechen. Wesentliche Änderungen sind in schriftlicher Form oder einem elektronischen Format zu vereinbaren.

10. INFORMATIONSPFLICHTEN DES AUFTRAGNEHMERS UND VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

10.1 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich in Schrift- oder Textform über jegliche Verstöße oder vermutete Verstöße gegen diesen Vertrag oder Vorschriften, die den Schutz personengezogener Daten betreffen.

10.2 Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Untersuchung, Schadensbegrenzung und Behebung der Verstöße.

10.3 Sollten die personenbezogenen Daten, die unter dieser Vereinbarung verarbeitet werden beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang relevanten Stellen unverzüglich auch darüber informieren, dass die Herrschaft über die Daten beim Auftraggeber liegt.

10.4 Soweit Prüfungen der Datenschutzaufsichtsbehörden durchgeführt werden, verpflichtet sich der Auftragnehmer das Ergebnis dem Auftraggeber schriftlich oder in Textform bekannt zu geben, soweit es die Verarbeitung der personenbezogenen Daten unter diesem Vertrag betrifft. Die im Prüfbericht feststellten Mängel wird der Auftragnehmer unverzüglich abstellen und den Auftraggeber darüber informieren.

10.5 Diese Ziffer 10 gilt entsprechend für Vorkommnisse bei Prozessen, die von Unterauftragnehmern ausgeführt werden.

11. UNTERAUFTRAGNEHMER

11.1 Die Beauftragung und/oder der Einsatz von Unterauftragnehmern durch den Auftragnehmer zur Datenverarbeitung im Rahmen des zwischen den Parteien geschlossenen Hauptvertrages ist nur nach Einwilligung des Auftraggebers in schriftlicher oder elektronischer Form zulässig, soweit diese nicht gemäß Ziff. 11.4 erfolgt ist. Ohne diese wird der Auftragnehmer diese/n unterlassen.

11.2 Der Auftragnehmer gewährleistet, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber Unterauftragnehmern gelten. Der Vertrag des Auftragnehmers mit dem Subunternehmer muss schriftlich oder in elektronischem Format abgeschlossen werden.

11.3 Eine Beauftragung von Subunternehmern in Drittstaaten erfolgt nur, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

11.4 Der Auftraggeber erteilt hiermit seine Zustimmung zur Beauftragung der in der Anlage unter der Ziffer 4 abschließend aufgeführten Unterauftragnehmer.

11.5 Der Auftragnehmer gewährleistet, dass der Auftraggeber gegenüber dem Unteraufragnehmer dieselben Weisungsrechte und Kontrollrechte wie gegenüber dem Auftragnehmer nach diesem Vertrag hat. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragnehmers, wie für eigenes Handeln/Unterlassen.

12. LÖSCHUNG UND RÜCKGABE PERSONENBEZOGENER DATEN

12.1 Der Auftragnehmer ist nach Abschluss, der jeweils im Hauptvertrag vereinbarten Verarbeitungsleistungen verpflichtet, alle personenbezogenen Daten, die er im Zuge der Auftragsverarbeitung erhalten hat, nach Wahl des Auftraggebers an den Auftraggeber zurückzugeben oder zu löschen. Dies schließt insbesondere die Ergebnisse der Datenverarbeitung, überlassene Dokumente und überlassene Datenträger und Kopien der personenbezogenen Daten mit ein. Die Pflicht zur Löschung oder Rückgabe besteht nicht, sofern der Auftragnehmer nach dem Recht der EU oder der Mitgliedstaaten zur weiteren Speicherung der Daten gesetzlich verpflichtet ist. Besteht eine weitere Verpflichtung zur Speicherung, hat der Auftragnehmer die Verarbeitung der personenbezogenen Daten einzuschränken und die Daten nur für die Zwecke zu nutzen, für die eine gesetzliche Verpflichtung zur Speicherung besteht. Die Pflichten zur Sicherheit der Verarbeitung bestehen für den Zeitraum der Speicherung fort. Der Auftragnehmer hat die Daten unverzüglich zu löschen, sobald die Pflicht zur Speicherung entfällt.

12.2 Die Löschung hat so zu erfolgen, dass die Daten nicht wiederherstellbar sind.

12.3 Die Vorgänge sind mit Angabe von Datum und durchführender Person zu protokollieren. Die Protokolle sowie ein Nachweis der Durchführung in schriftlicher

Form sind dem Auftraggeber innerhalb von 48 Stunden nach Durchführung der Vorgänge zur Verfügung zu stellen.

13. HAFTUNG; FREISTELLUNG / VERSICHERUNG

13.1 Jede Partei ist für ihre eigenen Handlungen verantwortlich und haftbar. Die in diesem Artikel 7 geregelte Haftung bezieht sich ausschließlich auf Bußgelder und Schäden, die sich aus der schuldhaften Nichteinhaltung der Verarbeitungsvereinbarung ergeben.

13.2 Der Auftragnehmer haftet nach den gesetzlichen Vorschriften.

13.3 Der Auftragnehmer stellt den Auftraggeber von allen Ansprüchen Dritter (einschließlich von durch eine Aufsichtsbehörde verhängter Bußgelder) frei, die auf einer schuldhaften Verletzung von Pflichten des Auftragnehmers aus dieser Vereinbarung beruhen. Die Freistellung umfasst dabei auch die angemessenen und unüblichen Aufwendungen des Auftraggebers, auch solche zur Rechtsverteidigung. § 254 BGB (Mitverschulden) bleibt unberührt.

13.4 Der Auftragnehmer wird eine angemessene Berufshaftpflicht- und Cyberkriminalitätsversicherung abschließen und während der Vertragsdauer aufrechterhalten, sowie die Aufrechterhaltung und Prämienzahlung dem Auftraggeber auf erste Anforderung nachweisen.

14. SCHLUSSBESTIMMUNGEN

14.1 Die Einrede des Zurückbehaltungsrechts im Sinne von § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten ausgeschlossen.

14.2 Die Anlage oder im Falle mehrerer abgeschlossener Hauptverträge die Anlagen zu diesem Vertrag sind wesentlicher Bestandteil desselben.

14.3 Für Änderungen oder Nebenabreden ist die Schriftform oder ein elektronisches Format erforderlich. Dies gilt auch für Änderungen dieses Formerfordernisses. § 305b BGB (Vorrang der Individualabrede) bleibt unberührt.

14.4 Sollte eine Bestimmung dieses Vertrages aus Gründen des Rechtes der Allgemeinen Geschäftsbedingungen nach §§ 305 bis 310 BGB ganz oder teilweise unwirksam/nichtig oder nicht durchführbar sein oder werden, gelten die gesetzlichen Regelungen. Beruht die Unwirksamkeit einer Bestimmung dieses Vertrages ausschließlich auf einem anderen Grund gilt: Die Unwirksamkeit oder Undurchführbarkeit einer oder mehrerer Regelungen dieser Vereinbarung lässt die Wirksamkeit der übrigen Regelungen dieser Vereinbarung unberührt. Dasselbe gilt für den Fall, dass die Vereinbarung eine an sich notwendige Regelung nicht enthält. Die Parteien werden in einem solchen Fall, die unwirksame oder undurchführbare Regelung oder Regelungslücke durch eine gesetzlich zulässige und durchführbare Regelung, die dem wirtschaftlichen Sinn und Zweck der unwirksamen, undurchführbaren oder fehlenden Regelung nach der Vorstellung der Parteien wirtschaftlich am nächsten kommt, ersetzen. Der Rechtsgedanke des § 139 BGB

findet – auch im Sinne einer Beweislastregel – keine Anwendung.

	Für den Auftraggeber	Für den Auftragnehmer
Ort		Crossen
Datum		
Name *		Paul de Meulemeester
Postition		CEO
Unterschrift		

*Name des bevollmächtigten Vertreters

Anlage zum Auftragsverarbeitungsvertrag

vom [Datum]

zwischen
<Kunde>
<Adresse>
<Postleitzahl – Ort>
- (nachfolgend „Auftraggeber“ genannt) -

und

Archive-IT Crossen GmbH
Am Rautenanger 2
D-07613 CROSSEN AN DER ELSTER
- (nachfolgend „Auftragnehmer“ genannt) -

- nachfolgend zusammen die „Parteien“ genannt -

ANHANG 1: Gegenstand des Auftrages

1.1 Gegenstand des Auftrages:

1.2 Umfang, Art (Art. 4 Nr. 2 DSGVO) und Zweck der Datenverarbeitung:

Anzahl der beteiligten Personen , deren personenbezogene Daten verarbeitet werden :

_____

Zweck: Archive-IT Crossen GmbH archiviert und/oder digitalisiert Akten mit datenschutzrelevanten Dateien für den Auftraggeber.

1.3 Art der Daten:

	Datenkategorie	Auflistung konkret verarbeiteter Daten	Beispiele
☐	Bauakten		Baupläne, Schriftverkehr, Notarielle Dokumente
☐	Daten zu beruflichen Verhältnissen		Berufsbezeichnung, beruflicher Werdegang, Betriebszugehörigkeit, Aufgaben, Tätigkeiten, Log-File-Auswertung, Eintritts- und Austrittsdaten, Qualifikationen, Beurteilungen, Tarifgruppe, Entgeltabrechnung, Sonderzahlungen, Pfändung, tägliche Anwesenheitszeiten, Abwesenheitsgründe
☐	Private Kontakt- und Identifikationsdaten		Name, Vorname, Geschlecht, Anschrift, EMail-Adresse, Telefonnummer, Mobiltelefonnummer, Geburtsdatum/ort, Identifikationsnummern, Nationalität
☐	Vertragsdaten		Gekaufte Produkte, Datum Kaufvertrag, Kaufpreis, Garantien
☐	Positionsdaten		GPS, Funknetz-Ortung, Bewegungsprofil, WLAN-Hotspot-Ortung
☐	Daten zu persönlichen Verhältnissen		Daten zum Ehegatten oder Kindern, Familienstand, Portraitfoto, Ehrenamt

☐	Bonitäts- und Bankdaten		Zahlungsverhalten, Bilanzen, Daten von Auskunfteien, Vermögensverhältnisse, Kontoverbindung, Kreditkartennummer
☐	Besonders sensible personenbezogene Daten		Art. 9 Abs. 1 DSGVO: rassische und Ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur Eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.
☐	Sonstiges		

1.4 Kreis der Betroffenen

	Betroffenengruppe	Beschreibung	Beispiele
☐	Mitarbeiter des Auftraggebers/des Verantwortlichen	Eigene Mitarbeiter des Auftraggebers/ des Verantwortlichen	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
☐	Mitarbeiter anderer Unternehmen	Mitarbeiter anderer Unternehmen, deren personenbezogene Daten für den Auftraggeber/den Verantwortlichen verarbeitet werden	Arbeitnehmer, Auszubildende, Bewerber, ehem. Beschäftigte
☐	Kunden des Auftraggebers/des Verantwortlichen	Jede Person, mit der eine Kunden Geschäftsbeziehung besteht (mit der jeweiligen verantwortlichen Stelle)	Käufer, Versicherungsnehmer, Mieter, Kunden einer Dienstleistung
☐	Sonstige Geschäftspartner	Jede natürliche Person, mit der eine Geschäftsbeziehung besteht (mit dem Auftraggeber) außer Kunden	Lieferanten, Importeure, Dienstleister, Vermittler, Freelancer
☐	Außenstehende	Jede Person, die in keiner Geschäftsbeziehung mit der jeweiligen Konzerngesellschaft (verantwortlichen Stelle) steht	Besucher, Gäste, Interessenten

ANHANG 2: Kontaktdaten

Kontaktperson des Verantwortlichen für die Datenverarbeitung 1 – Auftraggeber

Name	
Funktion	
Telefoonnummer	
E-Mail-Adresse	

Kontaktperson des Verantwortlichen für die Datenverarbeitung 2 – Auftraggeber

Name	
Funktion	
Telefoonnummer	
E-Mail-Adresse	

Datenschutzbeauftragter (eingetragen bei der Aufsichtsbehörde für Datenschutz) - Auftraggeber

Name	
Funktion	
Telefoonnummer	
E-Mail-Adresse	

Kontaktperson des Verantwortlichen für die Datenverarbeitung 1 – Auftragnehmer

Name	Roy Peeters
Funktion	Privacy Officer
Telefoonnummer	+31 77 750 11 00
E-Mail-Adresse	privacy-officer@archive-it.group

Kontaktperson des Verantwortlichen für die Datenverarbeitung 2 – Auftragnehmer

Name	**Ferenc Langheinrich**
Funktion	Security support
Telefoonnummer	+49 36693 4480
E-Mail-Adresse	f.langheinrich@archive-it.de

Datenschutzbeauftragter (eingetragen bei der Aufsichtsbehörde für Datenschutz) - Auftragnehmer

Name	Herr Drs A.E. Klaassen RE CIPP/E CIPM
Funktion	Datenschutzbeauftragter
Telefoonnummer	+31 77 750 11 00
E-Mail-Adresse	alex.klaassen@newdayriskservices.nl

ANHANG 3: Unterauftragnehmer

☐ Es werden keine Unterauftragnehmer eingesetzt.

☒ Zum Kreis der genehmigten Unterauftragnehmer bei Abschluss dieses Vertrages gehören:

Nr.	Unterauftragnehmer	Verarbeitete Datenkategorien	Beschreibung der Tätigkeit	Ort der Datenverarbeitung
1	NetPlans	Siehe Anhang 1, Artikel 1.3	Hosting der digitalen Daten	ETTLINGEN (DE)
2	Archive-IT Niederlande	Siehe Anhang 1, Artikel 1.3	Scannen, Lagerung, Transport	REUVER (NL)
3	TGW Logistik GmbH	Siehe Anhang 1, Artikel 1.3	Akten bei Kunden abholen	GERA (DE)
4	DHL Paket GmbH	Siehe Anhang 1, Artikel 1.3	Kunden physisch angeforderte Unterlagen per Post zusenden Kleine Mengen bei Kunden abholen	BONN (DE)
5	Becker & SDR GmbH	Siehe Anhang 1, Artikel 1.3	Vernichtung von Akten	CHEMNITZ (DE)
6	Heiko Drescher	Siehe Anhang 1, Artikel 1.3	Digitalisierung von Mikrofilmen	DRESDEN (DE)

ANHANG 4: Technische und organisatorische Maßnahmen

Der Auftragnehmer

☒ fügt dieser Anlage sein eigenes Sicherheitskonzept bei oder

☐ füllt die nachfolgende Vorlage für die technischen und organisatorischen Maßnahmen aus (Ziffer 5.2).

Vorlage für die technischen und organisatorischen Maßnahmen:

4.1 Zutrittskontrolle zu Räumlichkeiten und Einrichtungen, in denen Daten verarbeitet werden

Ein unbefugter Zutritt zu den Räumlichkeiten, in den die daten verarbeitet oder gespeichert werden ist vom Auftragnehmer zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Der Auftragnehmer hat folgende Maßnahmen ergriffen - detaillierte Beschreibung:

Der Zugang der Mitarbeiter zu Informationen wird auf der Grundlage eines autorisierten Arbeitsablaufs verstärkt, geändert oder entzogen. Der Zugang wird nur auf einer Need-to-know-Basis gewährt und eingehalten von Zugangskontrolle Systeme. Überwachungskameras, Alarmsystem, Datenschutzerklärung der Mitarbeiter und Besucher liegen vor, so wie auch Brandmeldeanlagen.

4.2 Zugangs- und Zugriffskontrolle

Das Eindringen Unbefugter in die Datenverarbeitungs (DV)-Systeme (IT-Systeme) ist vom Auftragnehmer nach dem jeweils aktuellen Stand der Technik zu verhindern. Ebenso sind Tätigkeiten in DV-Systemen (IT-Systemen) außerhalb eingeräumter Berechtigungen sowie unerlaubte Zugriffe auf das System von außen zu verhindern.

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Zugriffskontrollen sind klar definiert und geregelt. Die Gewährung, Änderung und Verweigerung des Zugangs zu den Archivräumen erfolgt im Rahmen eines autorisierten Verfahrens. Der Zugang ist nur auf einer Need-to-know-Basis erlaubt. Überwachungssystem und IT-Sicherheitssysteme sind installiert.

Für die Archive-IT-Software finden regelmäßig (externe) Pen-Tests (Penetration Tests) statt. Der Auftragnehmer gewährleistet ein angemessenes Patch-Management der Software, so dass wir immer über die neuestens Sicherheitsupdates verfügen.

4.3 Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist vom Auftragnehmer zu gewährleisten.

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Die Frontend- (für Kunden) und Backend-Software von Archive-IT ist mit einer Protokollierung ausgestattet. In dieser Protokollierung können Sie sehen, welche Person welche Art von Aktionen durchgeführt hat. Die Versionskontrolle ist in den digitalen Akten innerhalb der Archive-IT-Software vorhanden.

4.4 Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist vom Auftragnehmer zu gewährleisten. Eine Datenverarbeitung durch Dritte (vgl. Art. 28 DSGVO) ist nur mit Einwilligung des Auftraggebers/Datenexporteurs erlaubt. Maßnahmen (technisch und organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber/Datenexporteur und Auftragnehmer/Datenimporteur.

Der Auftragsverarbeiter hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Als Auftragsverarbeiter verarbeitet Archive-IT die Daten gemäß den (schriftlichen) Anweisungen des Datenverantwortlichen. Zusätzlich zu dieser Vereinbarung wird eine Verarbeitungsvereinbarung erstellt.

Archive-IT gibt seinerseits die Anweisungen schriftlich an einen möglichen Unterauftragsverarbeiter (z.B. Spediteur, Hosting-Partner, Aktenvernichter) weiter und mit dem Unterauftragsverarbeiter wird ebenfalls ein Verarbeitungsvertrag geschlossen.

Darüber hinaus müssen Besucher und Mitarbeiter von Unternehmen, die Zugang zu Akten in den Räumlichkeiten des Auftragnehmers haben, eine Vertraulichkeitserklärung unterzeichnen. Zum Beispiel Mechaniker für technische Anlagen.

4.5 Getrennte Verarbeitung von Daten/Trennungskontrolle

Die getrennte Verarbeitung von Daten, die für unterschiedliche Zwecke erhoben wurden, muss sichergestellt werden. Maßnahmen zur getrennten Verarbeitung der Daten unterschiedlicher Auftraggeber sind zu gewährleisten.
Der Auftragnehmer hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Sowohl die physischen als auch die digitalen Informationen (Dateien) seiner Kunden sind getrennt und nur mit dem jeweiligen Kunden verbunden und können daher nur von autorisierten Mitarbeitern dieses Kunden eingesehen und abgerufen werden. Die

Informationssicherheitspolitik und -Stufe von Archive-IT ist auf dem höchsten Level für alle verarbeitenden Daten.

4.6 Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln (elektronische Übertragung, Datentransport, Übermittlungskontrolle usw.), um einen Verlust, eine Veränderung oder eine unbefugte Veröffentlichung zu verhindern. Maßnahmen zu Transport, Übertragung, Übermittlung oder Speicherung auf Datenträgern (manuell oder elektronisch) sowie zur nachträglichen Überprüfung sind zu treffen.

Der Auftragnehmer hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Digitale Daten werden beim Transport verschlüsselt. Die digitalen Daten werden gesichert. Die verwendeten Anwendungen sind gegen Eindringlinge von außen geschützt. Mit den Beförderern von physischen Akten werden Vereinbarungen darüber getroffen, wie der Transport sicher organisiert werden kann. Mit Unterauftragsverarbeitern werden Verarbeitungsverträge geschlossen.

4.7 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Die Daten sind gegen zufällige Zerstörung und Verlust zu schützen. Maßnahmen zur Datensicherung (physikalisch/logisch).

Der Auftragnehmer hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Der Zweck der Informationssicherheit besteht darin, dass Archive-IT als Auftragsverarbeiter die für die Erfüllung des Vertrages erforderlichen Daten gegeneinander abgesichert hat:

- Unbefugter Zugang und Nutzung
- Verlust von (personenbezogenen) Daten, infolge von Katastrophen/ Unfällen, Schäden an Geräten und / oder Infrastruktur (einschließlich Backups).

Archive-IT ergreift die folgenden technischen Sicherheitsmaßnahmen:

- Erkennung von Antiviren und Mallware
- Sichere Entwicklungsumgebung
- Datensicherung
- Protokolldateien, Überprüfung der Protokollinformationen
- Patch-Verwaltung-Systeme
- Schutz von Anwendungen in öffentlichen Netzen

Archive-IT ergreift die folgenden technischen Sicherheitsmaßnahmen:

- Verwaltung von Rechten und Privilegien
- Sammlung von Beweisen im Falle von Sicherheitsvorfällen
- Geschäftskontinuitätsplan

- Anmeldung von Besuchern
- Klare Bildschirm- und Schreibtischrichtlinien
- Kontinuierliches Sensibilisierungsprogramm
- Disziplinarverfahren
- Externe Prüfung
- Verhaltenskodex
- Funktions-/Rollenbeschreibung, Informationssicherheit
- Prozess des Vorfallsmanagements
- Zugangspolitik physisch und digital (Zugang nach Bedarf)
- Videoüberwachung

Im Hinblick auf die AVG.Gesetzgebung verfügt der Auftragnehmer unter anderem über Folgendes:

Artikel 24: Datenschutzpolitik
Artikel 25: Datenschutz durch Technik und Datenschutz durch Voreinstellung
Artikel 28: Verarbeitervereinbarung
Artikel 30: Register der Verarbeiter
Artikel 32: Sicherheitsmaßnahmen (siehe oben)
Artikel 35: Private Folgenabschätzungen
Artikel 37: Datenschutzbeauftragter (DSB)
Kapitel 3: Rechte der betroffenen Personen

4.8 Privacy by Default

Treffen Sie Maßnahmen zur Einhaltung der Anforderung Privacy by Default?

Privacy by Default bedeutet übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“. Das heißt, bereits die Werkseinstellungen sollen datenschutzfreundlich ausgestaltet werden. Hierdurch sollen vor allem die Nutzer geschützt werden.

Der Auftragnehmer hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

In der Auftragnehmer-Software ist das möglich:

- Felder im Rahmen der Datenminimierung deaktivieren
- Zuweisung von Merkmalen zu den Dateien (z.B: Aufbewahrungsfrist, Jahr der Vernichtung), um die Anforderung zu erfüllen, Daten nicht länger als nötig zu speichern. Die Listen der zu vernichtenden Dateien können mit der Auftragnehmer-Software erstellt werden.
- Versehen Sie Ausdrucke mit einem Wasserzeichen, dass darauf hinweist, dass es sich bei dem Papierdokument um eine Kopie handelt und/oder datenschutzrelevanten Daten enthält.

4.9 Organisationskontrolle

Wie wird die reibungslose Organisation des Datenschutzes und der Sicherheit der Daten im Unternehmen sichergestellt?
Der Auftragnehmer hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Die Grundlage der Qualitäts-, Informationssicherheits- und Datenschutzpolitik innerhalb des Auftragnehmers bildet ein Qualitätsmanagement- und Informationssicherheitssystem namens GRC-Control. Diese zentrale Anwendung wird für alle Bereiche des Auftragnehmers genutzt.

In dieser Anwendung gelten:

+ Interne Audits werden geplant und durchgeführt. Maßnahmen werden ergriffen und nachverfolgt.
+ Risikoanalysen werden geplant, durchgeführt und mögliche Maßnahmen werden festgelegt und weiterverfolgt.
+ Registrierung und Weiterverfolgung von Vorfällen, Beschwerden, Abweichungen und Verbesserungsvorschlägen.
+ Regelmäßige Kontrollaufgaben werden geplant und überwacht. Zum Beispiel die Bewertung von Lieferanten und die Kontrolle von Einrichtungen.

Schriftliche Verfahren, Arbeitsanweisungen und Grundsatzdokumente sind in Sharepoint (im PDF-Format) verfügbar und können von den Mitarbeitern eingesehen werden.

4.10 Wirksamkeitskontrolle

Alle Handlungen, die zu einem Nachweis führen, dass die eingesetzten Maßnahmen funktionieren.

Der Auftragnehmer hat folgende Maßnahmen ergriffen – detaillierte Beschreibung:

Einer der wichtigsten Beweise für die ergriffenen Maßnahmen ist, dass Archive-IT seit vielen Jahren nach ISO9001 und ISO27001 zertifiziert ist und nur wenige Nichtkonformitäten / Verbesserungsvorschlägen pro Jahr aufweisen muss, da unsere Systeme stets auf dem besten Stand sind.

4.11 Ergänzende oder erklärende Dokumente und/oder Zertifikate

Der Auftragsverarbeiter hat folgende Dokumente/Zertifikate erhalten:
Zertifiziert nach ISO 27001 und ISO 9001. An diese Informationsabläufe und dieses Qualitätsmanagement wird sich gehalten.

Für den Auftraggeber:

Unterschrift _____
Ort:
Datum:

Für den Auftragnehmer:
Paul de Meulemeester, CEO Archive-IT Crossen GmbH

Unterschrift _____
Ort: Crossen
Datum:

ANHANG 5: Zusatzvereinbarung zu dem Auftragsverarbeitungsvertrag vom _____ ** Kirchliches Unternehmen** _____

5.1 Weisungsgebundene Verarbeitung und Remonstrationspflicht

5.1.1 Für Weisungen des Auftraggeber gegenüber dem Auftragsverarbeiter[1] (Artikel 29 i. V. m. Artikel 28 Absatz 3 Buchstabe a DSGVO) sind die in Anhang 2: Kontaktdaten aufgeführten Ansprechpartner zuständig. Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Im Rahmen einer Weisung kann für den Auftragnehmer ein Ermessensspielraum bestehen bleiben, mit welchen geeigneten technischen und organisatorischen Maßnahmen die Weisung umgesetzt wird. Darüber hinaus erfolgt die Verarbeitung durch den Auftragnehmer gemäß etwaiger in Anhang 2: Kontaktdaten festgelegter Weisungen.

5.1.2 Weisungen werden vom Auftraggeber grundsätzlich in Textform (z. B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom Auftragnehmer entsprechend in Textform (z. B. per E-Mail) bestätigt. Der Auftragnehmer gewährleistet, dass alle erteilten Weisungen des Auftraggebers seinen insoweit zuständigen Beschäftigten zugehen (z. B. durch zentrale Ablage aller Weisungen).

5.1.3 Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach seiner Ansicht gegen die DSGVO oder eine andere Vorschrift über den Datenschutz verstößt (Remonstrationspflicht). Wenn der Verantwortliche den Hinweis als berechtigt erachtet, wird er die entsprechende Weisung so anpassen, dass diese nicht mehr gegen den Datenschutz verstößt.

5.2 Vertraulichkeits-/ Verschwiegenheitspflicht und Vereinbarung zur Wahrung des Berufsgeheimnisses nach § 203 StGB[2]

---

[1] Dieses Vertragsmuster findet regelmäßig nur Anwendung für Auftragsverarbeiter, die in einem EWR-Mitgliedstaat belegen sind oder in einem Drittland, für das gemäß Artikel 45 DSGVO ein Angemessenheitsbeschluss der EU-Kommission vorliegt. Ansonsten könnten ggf. die Standarddatenschutzklauseln der EU-Kommission gemäß Artikel 46 Abs. 2 DSGVO verwendet werden.

[2] Strafgesetzbuch

5.2.1 Der Auftragnehmer wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Insoweit gewährleistet der Auftragnehmer, dass diese Personen nur im Rahmen der Erforderlichkeit auf personenbezogene Daten der beauftragten Verarbeitungstätigkeit zugreifen („Need to know").

5.2.2 Im Rahmen der Durchführung des Vertrages werden auch Daten verarbeitet, die unter ein Berufsgeheimnis (im Sinne von § 203 StGB) fallen.[3]
Der Auftragnehmer verpflichtet sich, über Berufsgeheimnisse Stillschweigen zu bewahren und sich nur insoweit Kenntnis von diesen Daten zu verschaffen, wie dies zur Erfüllung der ihm zugewiesenen Aufgaben erforderlich ist.

5.2.3 Der Auftragnehmer gewährleistet, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggeber befassten Beschäftigten und andere für den Auftragnehmer tätigen Personen (z. B. weitere Auftragnehmer), die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Der Verantwortliche weist den Auftragnehmer darauf hin, dass sich eine mitwirkende Person nach § 203 Abs. 4 S. 2 StGB strafbar macht, sollte sie sich einer weiteren mitwirkenden Person bedienen, die ihrerseits unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, und die mitwirkende Person nicht dafür Sorge getragen hat, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

5.2.4 Der Auftragnehmer ist unter Beachtung der Regelungen in Ziffer 6 berechtigt, weitere Auftragnehmer zur Vertragserfüllung heranzuziehen. Der Auftragnehmer wird etwaige weitere Auftragnehmer sorgfältig auswählen und diese, soweit sie im Rahmen ihrer Tätigkeit Kenntnis von fremden Geheimnissen im Sinne dieser Vereinbarung erlangen könnten, zur Geheimhaltung verpflichten. Der Auftragnehmer wird ferner etwaige weitere Auftragnehmer dazu verpflichten, sämtliche von diesen eingesetzten Personen und etwaige weitere Unterauftragnehmer, die bestimmungsgemäß mit in Berührung kommen, welche der Geheimhaltung unterliegen, oder bei denen dies nicht auszuschließen ist, nach den zuvor genannten Grundsätzen zur Verschwiegenheit zu verpflichten und über die Folgen einer Pflichtverletzung zu belehren.
Des Weiteren werden etwaige weitere Auftragnehmer, über das bestehende Schweigerecht gemäß § 53a StPO sowie den Beschlagnahmeschutz gemäß § 97

[3] Die Regelung in Ziffer 4.2 – 4.6 sind in enger Anlehnung dem Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen entnommen (https://www.gesundheitsdatenschutz.org/download/Muster-AV-Vertrag_2018.pdf; Lizenz: https://creativecommons.org/licenses/by-sa/4.0/deed.de; vollständiger Lizenztext: https://creativecommons.org/licenses/by-sa/4.0/legalcode).

StPO informiert; dies beinhaltet auch den Hinweis bzgl. des Rechts des Berufsgeheimnisträgers, über dieses Recht zu entscheiden und der damit verbundenen Pflicht, unverzüglich den Auftraggeber bzgl. der Wahrnehmung dieser Rechte zu kontaktieren.
Diese Verpflichtung gilt für sämtliche weitere Auftragsverarbeitungen.

5.2.5 Der Auftragnehmer wird darauf hingewiesen, dass Daten, die er im Auftrag eines Berufsgeheimnisträgers verarbeitet u. U. dem Zeugnisverweigerungsrecht von sogenannten mitwirkenden Personen unterliegen (§ 53a Strafprozessordnung (StPO)). Entsprechend § 53a StPO entscheidet jedoch der Berufsgeheimnisträger über die Ausübung des Schweigerechts. Im Falle einer Befragung wird der Auftragnehmer unter Hinweis auf § 53a StPO dieser widersprechen und unverzüglich den Auftraggeber informieren, der daraufhin bzgl. der Wahrnehmung des Schweigerechts entscheidet.

5.2.6 Der Auftragnehmer wird darauf hingewiesen, dass die in seinem Gewahrsam befindlichen Geheimnisschutzdaten dem Beschlagnahmeverbot gemäß § 97 StPO unterliegen. Die Daten dürfen nicht ohne das Einverständnis des Auftraggebers (Berufsgeheimnisträger) herausgegeben werden. Im Falle einer Beschlagnahme wird der Auftragnehmer dieser widersprechen und unverzüglich den Auftraggeber informieren.

5.3 Technische und organisatorische Maßnahmen gemäß Artikel 32 DSGVO und § 7 GDSG NW

5.3.1 Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Artikel 32 DSGVO. Diese werden in Anhang 4: Technische und organisatorische Maßnahmen spezifiziert. Darüber hinaus wird der Auftragnehmer Patientendaten aus dem ärztlichen Bereich des Auftraggebers auf physisch getrennten Dateien verarbeiten (§ 7 Abs. 3 S. 2 GDSG NW).