AUFTRAGSVERARBEITUNGSVERTRAG
gem. Art 28 DSGVO

zwischen

im Folgenden: Auftraggeber

und

Novaline Informationstechnologie GmbH

Birkenallee 177

48432 Rheine

im Folgenden: Auftragnehmer

Präambel

Diese Anlage konkretisiert die Verpflichtungen von Auftraggeber und Auftragnehmer zum Datenschutz, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.

In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

1. Gegenstand, Dauer und Spezifizierung der Verarbeitung

Aus dem Vertrag ergeben sich Gegenstand, Dauer des Auftrags sowie Art und Zweck der Verarbeitung.

1.1 Gegenstand:

Als IT-Dienstleister kann auf Seiten des Auftragnehmers ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.

Der Auftragnehmer übernimmt folgende Verarbeitungen:

- IT-Support/ Fernwartung/ Implementierung

Die Verarbeitung beruht auf der zwischen den Parteien bestehenden Software-Pflege- und Wartungsvereinbarung gem. § 13 der Allgemeinen Vertragsbedingungen für Software und Softwarepflege (im Folgenden „Hauptvertrag“).

1.2 Dauer

Die Laufzeit dieses Vertrages richtet sich nach der Laufzeit des Hauptvertrages.

1.3 Art und Zweck der Verarbeitung

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

1.3.1. Art der Daten

Es werden folgende Daten verarbeitet:

- Personenbezogene Daten
- Systemdaten

1.3.2. Kategorien der betroffenen Personen

Von der Verarbeitung betroffen sind:

- Mitarbeiter des Auftraggebers
- Geschäftspartner
- Kunden
- Lieferanten
- Interessenten

2. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrages vertraut gemacht wurden.

(6) Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

(7) Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(8) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Für alle im Rahmen dieses Vertrages anfallenden Datenschutzfragen ist der Ansprechpartner mit dessen aktuellen Kontaktdaten auf der Internetseite des Auftragnehmers leicht zugänglich hinterlegt.

(9) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrages erfolgen.

(10) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.

3. Technische und organisatorische Maßnahmen (TOMs)

(1) Die in Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(3) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(4) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(5) Der Auftragnehmer stellt sicher, seinen Pflichten nach Art. 32 I b DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

4. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit, auch über die Beendigung dieses Vertrages hinaus, Folge leisten.

5. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsdienstleistungen, Post-/Transportdienstleistungen, Wartung- und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software in Anspruch nimmt.

(2) Die Beauftragung von Subunternehmern (=weitere Auftragsverarbeiter) ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

(3) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind.

(4) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

(5) Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

6. Rechte und Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung, sowie für die Wahrung der Rechte von Betroffenen, ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen, vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer, soweit erforderlich, Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate, statt. Die Kontrolle soll sich auf Stichproben beschränken.

7. Mitteilungspflichten

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis, an eine vom Auftraggeber benannte Adresse zu erfolgen.

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

(3) Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 DSGVO im erforderlichen Umfang zu unterstützen. Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

8. Weisungen

(1) Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor. Weisungen können schriftlich, per Fax, per E-Mail oder mündlich erfolgen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform oder in einem dokumentierten elektronischen Format.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

9. Beendigung des Auftrags

(1) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers, hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

(2) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

(3) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber auf Anforderung vorzulegen.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer, den jeweiligen Aufbewahrungsfristen entsprechend, auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

10. Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

11. Informationspflicht, Schriftform, Rechtswahl

(1) Sollten die Daten des Auftraggebers bei 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 Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutzgrundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung zum Datenschutz und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format erfolgen kann und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung der Bedingungen aus dieser Vereinbarung zum Datenschutz handelt.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

(4) Es gilt deutsches Recht.

Die folgenden Anlagen werden Vertragsbestandteil:

- Anlage 1 Technische und organisatorische Maßnahmen
- Anlage 2 Zugelassene Subdienstleister

Auftraggeber	Auftragnehmer
_____, den _____,_____,_____	Rheine, den _____,_____,_____
	Horst Ramnitz (Geschäftsführer)
Vor- und Nachname	Vor- und Nachname
Firmenstempel/Unterschrift	Firmenstempel/ Unterschrift

Anlage 1

Technische und organisatorische Maßnahmen (TOMs)
Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität, Verfügbar- und Belastbarkeit der im Auftrag verarbeiteten Informationen.

I. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1. Zutrittskontrolle

- Sicherheitsschlösser
- besetzter Empfangsbereich
- Dokumentierte und nachprüfbare Schlüsselregelung
- Serverräume sind stets verschlossen
- Sorgfältige Auswahl von Reinigungspersonal

2. Zugangskontrolle

- Mitarbeiter haben individuelle Benutzernamen und Kennwörter für die Anmeldung am PC –Arbeitsplatz
- Einsatz von Anti-Viren Software
- Einsatz einer Software-Firewall
- Sicherheitsschlösser
- Schlüsselregelung
- Sorgfältige Auswahl von Reinigungspersonal

3. Zugriffskontrolle

- Verwaltung der Rechte durch Systemadministrator
- Sichere Aufbewahrung von Datenträgern
- Mitarbeiter sind dazu verpflichtet, ausschließlich vom Unternehmen ausgegebene externe Datenträger zu verwenden
- Nicht mehr benötigte IT-gestützte Datenträger werden datenschutzgerecht entsorgt
- Einsatz von Aktenvernichtern bzw. Dienstleistern
- Physische Löschung von Datenträgern vor Wiederverwendung

4. Trennungsgebot

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logische Mandantentrennung (softwareseitig)
- Festlegung von Datenbankrechten
- Trennung von Produktiv- und Testsystemen

5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

II. Integrität gem. Art. 32 Abs. 1 lit. b DSGVO

1. Weitergabekontrolle

- Verschlüsselung der Datenverbindung
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –Fahrzeugen

2. Eingabekontrolle

- Bei Einsatz von Standardsoftware ist sichergestellt, dass ausreichende und den Datenschutzanforderungen entsprechende Protokollierungen aktiv sind

III. Verfügbarkeit und Belastbarkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1. Verfügbarkeitskontrolle

- Unterbrechungsfreie Stromversorgung (USV)
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverraum
- Testen von Datenwiderherstellung
- Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- und Recoverykonzepts
- Erstellen eines Notfallplans

2. Rasche Wiederherstellbarkeit gem. Art. 32 Abs. 1 lit. c DSGVO

- Prüfung der Verfügbarkeit von erforderlichen Systemen, Datenträgern, Lizenzkeys etc. zur Sicherstellung der schnellen Wiederherstellbarkeit von Daten und Programmen (Desaster-Recovery-Szenarien)
- Datenrücksicherungsszenarien: jeweiligen Applikation muss auch im Versionsstand der Datensicherung vorliegen um Rücksicherung zu gewährleisten

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung gem. Art. 32 Abs. 1 lit. d DSGVO; Art 25 Abs. 1 DSGVO

1. Datenschutzmanagement

- Bestellung eines Datenschutzbeauftragten
- Verpflichtung auf das Datengeheimnis
- Unterweisungen für Mitarbeiter
- Datenschutzdokumentation

2. Incident-Response-Management

- Informationen der Mitarbeiter zum Verhalten bei Eintreten eines Datenschutzvorfalls
- Gewährleistung von Meldepflicht und Fristen gegenüber Behörden bei Datenpannen

3. Datenschutzfreundliche Voreinstellungen

- Implementierung von datenschutzfreundlichen Voreinstellungen in Produkten
- Voreinstellung des Personenkreises dem Daten zugänglich gemacht werden
- Zugriffsbeschränkung

4. Auftragskontrolle

- Auswahl weiterer Auftragnehmer unter Sorgfaltsgesichtspunkten (insb. hinsichtlich Datensicherheit)
- Schriftliche Weisungen z.B. durch Auftragsdaten-verarbeitungsvertrag
- Datenschutzbeauftragter im Unternehmen
- Verpflichtung der Mitarbeiter auf das Datengeheimnis

Anlage 2

Zugelassene Subdienstleister

Es sind keine Subdienstleister für Dienstleistungen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen, beauftragt.