DynaNet
Dein IT-Komfortpartner

Einfach.
Ehrlich.
Swiss-IT.

AUFTRAGSDATENVEREINBARUNG

zwischen

DynaNet GmbH
Schachenstrasse 2
9016 St. Gallen

(nachstehend Auftragnehmerin genannt)

und

Kunde
Als Kunde wird jede natürliche oder juristische Person bezeichnet, die mit DynaNet GmbH einen Vertrag zur Erbringung der vereinbarten Dienstleistungen abschliesst und im Rahmen dessen personenbezogene Daten zur Verarbeitung übermittelt.

(nachstehend Verantwortlicher/Auftraggeber genannt)

1 Allgemeine Bestimmungen

1.1 Gegenstand dieser Vereinbarung

1.1.1 Die vorliegende Vereinbarung regelt die im Rahmen der Zusammenarbeit zwischen der Auftragnehmerin und dem Auftraggeber (nachfolgend: Grundverhältnis) erfolgte Datenbearbeitung durch die Auftragnehmerin. Das Grundverhältnis ist in erster Linie in bereits bestehenden Vereinbarungen (inkl. AGB der Auftragnehmerin) geregelt, dessen ergänzender Bestandteil die vorliegende Vereinbarung ist.

1.1.2 Bei allfälligen Widersprüchen zwischen dieser Vereinbarung und anderen Vertragsbestandteilen, sind die Bestimmungen dieser Vereinbarung in jedem Fall vorrangig.

1.1.3 In Ergänzung zu diesem Vertrag ist die Datenschutzerklärung der Auftragnehmerin zu beachten, einsehbar unter https://www.dynanet.ch/datenschutz/. Der Auftraggeber erklärt ausdrücklich, diese zur Kenntnis genommen zu haben.

1.2 Laufzeit dieser Vereinbarung

1.2.1 Diese Vereinbarung ist an die Laufzeit des Grundverhältnisses gekoppelt, soweit sich aus den nachfolgenden Bestimmungen nicht etwas Abweichendes ergibt.

2 Bestimmungen zur Auftragsdatenbearbeitung

2.1 Grundsätze

2.1.1 Im Zusammenhang mit dem Grundverhältnis bearbeitet die Auftragnehmerin für den Auftraggeber Personendaten. Es geht um Daten des Auftraggebers selbst, von allfälligen Hilfspersonen sowie von weiteren Dritten, insbesondere von Kunden des Auftraggebers.

2.1.2 Die Auftragnehmerin bearbeitet die ihr vom Auftraggeber anvertrauten Daten nur so, wie es der Auftraggeber selbst tun dürfte. Sie führt ein Verzeichnis über die durchgeführten Bearbeitungstätigkeiten.

2.1.3 Die Auftragnehmerin verpflichtet sich, alle im Rahmen des Vertragsverhältnisses bearbeiteten Personendaten vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung des Vertrags bestehen.

2.1.4 Die Auftragnehmerin verpflichtet sich sodann generell zur Einhaltung der auf sie anwendbaren datenschutzrechtlichen Bestimmungen (z.B. DSG, DSGVO [soweit anwendbar]).

2.1.5 Der Auftraggeber bestätigt, dass die Übertragung der Datenbearbeitung an die Auftragnehmerin nicht im Widerspruch zu gesetzlichen oder vertraglichen Geheimhaltungspflichten steht. Bestehen gesetzliche oder vertragliche Geheimhaltungspflichten, ist es in der alleinigen Verantwortung des Auftraggebers, die nötigen Vorkehrungen zur Wahrung der Geheimnisse (z.B. Entbindung) zu ergreifen.

2.2 Zweck, Ort und Art der Datenbearbeitung

2.2.1 Die Datenbearbeitung durch die Auftragnehmerin erfolgt grundsätzlich ausschliesslich zwecks Abwicklung des Grundverhältnisses. Eine anderweitige Bearbeitung (z.B. zu Marketingzwecken) ist ohne vorgängige Zustimmung des Auftraggebers unzulässig.

2.2.2 Die Datenbearbeitung erfolgt in erster Linie elektronisch auf den Servern / Rechnern der Auftragnehmerin. Es ist der Auftragnehmerin allerdings ebenfalls gestattet, Daten (z.B. zwecks Sicherung) physisch zu bearbeiten.

2.2.3 Die Bearbeitungstätigkeiten der Auftragnehmerin erfolgen grundsätzlich in der Schweiz. Der Auftraggeber nimmt aber zur Kenntnis und akzeptiert ausdrücklich, dass Daten unter Umständen auch ins Ausland bekanntgegeben werden können, dies namentlich auch in Staaten, die über kein mit der Schweiz vergleichbares Datenschutzniveau gewährleisten (z.B. USA). Dies kann beispielsweise im Zusammenhang mit der Nutzung von Diensten wie Microsoft 365, Microsoft Teams u.ä. geschehen.

2.2.4 Die Auftragnehmerin trennt die im Rahmen dieses Vertrages zu bearbeitenden Daten streng von anderen Datenbeständen.

2.3 Arten und Kategorien von betroffenen Daten

2.3.1 Von der Datenbearbeitung sind je nach Grundverhältnis folgende Arten / Kategorien von Daten betroffen:

- Personendaten (z.B. Name, Vorname, Adresse, Geburtsdatum);
- Buchhaltungsdaten (z.B. Lohnbuchhaltung);
- Bewerbungsdaten (z.B. Lebenslauf usw.);
- Kontakt- und Kommunikationsdaten (z.B. Telefon, E-Mail);
- Vertragsdaten (z.B. Vertragsbeziehung, Produkt- bzw. Vertragsinteresse);
- IT-Nutzungsdaten (z.B. UserID, Passwörter);
- Bankdaten (z.B. Kontoverbindung, Kreditkartennummern).

2.4 Weisungen des Auftraggebers

2.4.1 Die Auftragnehmerin bearbeitet Daten ausschliesslich gemäss den Bestimmungen dieses Vertrags und allfälligen Weisungen des Auftraggebers.

2.4.2 Weisungen durch den Auftraggeber erfordern Schriftlichkeit (Art. 12 ff. OR).

2.4.3 Weisungen, die gegen gesetzliche Bestimmungen verstossen, sind für die Auftragnehmerin unbeachtlich. Die Auftragnehmerin weist den Auftraggeber auf allfällige gesetzeswidrige Weisungen hin, es sei denn, sie sei gesetzlich an dieser Information gehindert.

2.5 Hilfspersonen, Subunternehmer

2.5.1 Die von der Auftragnehmerin zur Datenbearbeitung eingesetzten Personen (nachfolgend: Hilfspersonen) kennen und achten die einschlägigen datenschutzrechtlichen Bestimmungen sowie die Bestimmungen dieser Vereinbarung. Sie sind von der Auftragnehmerin im erforderlichen Umfang zur Vertraulichkeit verpflichtet worden.

2.5.2 Der Beizug Dritter zur Datenbearbeitung (nachfolgend: Subunternehmer) ist zulässig. Der Auftraggeber hat dabei jederzeit das Recht, bei der Auftragnehmerin eine Übersicht ihrer aktuellen Subunternehmer einzufordern.

2.5.3 Beabsichtigt die Auftragnehmerin, weitere Subunternehmer beizuziehen, informiert sie den Auftraggeber im Voraus. Erfolgt innert 5 Kalendertagen seit der Mitteilung kein Widerspruch, ist der Auftragnehmer befugt, wie beabsichtigt zu verfahren.

2.5.4 Die Auftragnehmerin hat alle Subunternehmer zur Einhaltung des Datenschutzes nach Gesetz und Vertrag zu verpflichten.

2.6 Technische & organisatorische Massnahmen zur Gewährleistung von Datenschutz

2.6.1 Die Auftragnehmerin stellt die erforderlichen technischen und organisatorischen Massnahmen zur Gewährleistung von Datenschutz sicher. Die Massnahmen stellen insbesondere sicher, dass

- ein Datensicherheitsniveau besteht, das den Risiken für die Rechte der betroffenen Personen angemessen ist und Schutz vor versehentlicher oder unrechtmässiger Zerstörung, Verlust, Veränderung, unbefugter Offenlegung oder Zugriff auf übermittelte, gespeicherte oder anderweitig bearbeitete Personendaten bieten;
- Unbefugten der Zutritt zu bzw. die Nutzung von zu Datenbearbeitungsanlagen verwehrt ist;
- Unbefugte keine Möglichkeit haben, auf Datenbearbeitungssysteme zuzugreifen;
- Daten Unbefugten nicht weitergegeben werden;
- nachträglich noch festgestellt werden kann, ob und von wem Daten eingegeben, verändert oder entfernt worden sind;
- zu unterschiedlichen Zwecken erhobene Daten getrennt bearbeitet werden.

2.6.2 Die konkreten technischen Massnahmen sind im Punkt 3 einzeln aufgelistet. Die Auftragnehmerin kann den Punkt 3 jederzeit einseitig ändern, wobei Änderungen in geeigneter Form zu dokumentieren sind.

2.7 Unterstützung, Information und Kontrolle

2.7.1 Die Auftragnehmerin teilt dem Auftraggeber allfällige Störungen, Verstösse, Unregelmässigkeiten oder Verletzungen der Datensicherheit und damit zusammenhängende Umstände (z.B. Ermittlungen und Massnahmen der Aufsichtsbehörde) unverzüglich mit, ohne diese vorher Dritten bekannt zu geben.

2.7.2 Die Auftragnehmerin unterstützt den Auftraggeber angemessen bei der Erfüllung der Rechte der von einer Datenbearbeitung betroffenen Person (z.B. Auskunft) und bei der Erfüllung besonderer Pflichten (z.B. Meldungen von Verletzungen der Datensicherheit). Sie wird allfällige Anfragen des Auftraggebers im Zusammenhang mit der Bearbeitung der Personendaten unverzüglich und ordnungsgemäss beantworten.

2.7.3 Reichen die Antworten der Auftragnehmerin nicht aus zum Nachweis der Einhaltung der gesetzlichen und vertraglichen Pflichten, ist der Auftraggeber berechtigt, bei der Auftragnehmerin Überprüfungen selbst oder durch beauftragte Prüfer vorzunehmen. Die Terminfestsetzung erfolgt einvernehmlich und mit angemessener Vorlaufzeit.

2.8 Berichtigung, Einschränkung und Löschung

2.8.1 Die Auftragnehmerin darf, die ihr vom Auftraggeber anvertrauten Daten nicht eigenmächtig, sondern nur nach Weisungen des Auftraggebers berichtigen, löschen oder deren Bearbeitung einschränken.

2.8.2 Kopien oder Duplikate dürfen nur mit Zustimmung des Auftraggebers erstellt werden. Hiervon ausgenommen sind solche zu Sicherungszwecken (Backups sowie solche, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

2.8.3 Nach Beendigung des Grundverhältnisses kann der Auftraggeber die Löschung oder Rückgabe sämtlicher Datenbestände im Zusammenhang mit diesem Vertrag verlangen. Vorbehalten bleiben allfällige gesetzliche Aufbewahrungspflichten sowie die gemäss Grundverhältnis erstellten Backups, die nachträglich nicht mehr geändert werden können und in Bezug auf diese daher lediglich ein Rückgabeanspruch besteht. Das Protokoll der Löschung ist auf Nachfrage hin vorzulegen und dauerhaft zu speichern. Für die Aufwände der Auftragnehmerin im Zusammenhang mit Löschung und / oder Rückgabe von Datenbeständen gelten die Konditionen des Grundverhältnisses.

2.8.4 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Die Auftragnehmerin kann sie zu ihrer Entlastung bei Vertragsende dem Auftraggeber übergeben.

3 Anhang – Technisch-organisatorische Massnahmen

3.1 Vertraulichkeit

Zutrittskontrolle

Folgende Massnahmen werden getroffen, um einen unbefugten Zutritt zu den DataCenter und physischen Datenablagen zu verhindern.

- ☒ Die DataCenter befinden sich in Sicherheitsbereichen mit eingeschränktem Zugang
- ☒ Es ist gewährleistet, dass keine betriebsfremden Personen Zutritt zu den DataCenter haben
- ☒ Zutrittskontrollsysteme (Lesegeräte und Badges) sind vorhanden
- ☒ Schlüsselverwaltung
- ☒ Personenkontrolle durch Empfang/Portier
- ☒ Alarmanlage
- ☒ Gebäudeüberwachung durch Sicherheitspersonal
- ☒ Überwachungseinrichtungen, (Video/CCTV-Monitor, Alarmanlage, etc.)
- ☒ für diese Bereiche werden Anwesenheits- und oder Berechtigungsnachweise geführt
- ☒ Der Zutritt durch Personen, die nicht allgemein zum Zutritt zu den Systemen befugt sind (d.h. unbefugte Mitarbeiter und externe Personen wie z.B. Wartungstechniker, Reinigungskräfte, Besucher) ist geregelt

Zugangskontrolle

Folgende Massnahmen werden getroffen um einen unbefugten Zugang zu den DataCenter und physischen Datenablagen zu verhindern.

- ☒ Benutzerautorisierung und -authentifizierung
- ☒ Sicherheitsmassnahmen hinsichtlich Nutzer-IDs/Passwörtern (z.B. Sonderzeichen, Mindestlänge, Pflicht zur Änderung von Passwörtern)
- ☒ automatische Sperrung (z.B. Bildschirmsperre bei Auszeiten und Aufforderung zur Eingabe des Passworts)
- ☒ Wichtige Systemaktivitäten werden protokolliert
- ☒ Überwachung von Einbruchsversuchen und automatische Sperre bei mehrfach eingegebenen falschen Passwörtern
- ☒ Verschlüsselung archivierter Datenmedien

Zugriffskontrolle

Folgende Massnahmen sollen gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☒ Zugriffsrechte (Profile, Rollen) basierend auf einem Rechte- und Rollenkonzept
- ☒ Überwachung und Aufzeichnung von Zugriffen, Zugriffsberichte
- ☒ Verschlüsselter Zugriff (z. B. https, SSL, etc.)
- ☒ Verschlüsselte Datenspeicherung
- ☒ Verfahren zur Sicherstellung für die Vernichtung von gebrauchten Medien sind eingerichtet
- ☒ Fernwartungen der IT-Systeme sind gesichert (Verschlüsselung, Einmalpasswörter, etc.)
- ☒ interne Richtlinien und Verfahren

Trennungskontrolle

Folgende Massnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

- ☒ Trennung von Datenbanken
- ☒ Die für die Verarbeitung genutzten IT-Systeme sind mandantenfähig und werden entsprechend betrieben. Ist dies nicht möglich, so werden dedizierte Systeme genutzt.
- ☒ Trennung von Funktionen (Produktion/Test)

Pseudonymisierung

Es erfolgt keine Pseudonymisierung von Ordnerstrukturen und Daten.

3.2 Integrität

Weitergabekontrolle

Folgende Massnahmen gewährleisten, dass personenbezogene Daten, die elektronisch oder auf Datenträgern (manuell oder elektronisch) gespeichert sind, bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft werden kann, an welche Stellen die personenbezogenen Daten weitergegeben wurden.

- ☒ Verschlüsselte Medien (USB-Sticks, externe Festplatten, etc.)
- ☒ Verschlüsselte Übertragungswege (SSL, HTTPS, SCP, SFTP, etc.)
- ☒ Virenschutz
- ☒ Firewalls
- ☒ Netzwerke und Netzwerkzugriffspunkte werden dokumentiert
- ☒ VPN (Virtual Private Networks) oder Tunnel
- ☒ Inhaltsfilter / Proxy
- ☐ IPS / IDS (Systems zur Erkennung/ Verhinderung von Einbrüchen)
- ☒ Aktive Netzwerkkomponenten (z.B. Switches oder Router) sind so konfiguriert, dass wichtige Ereignisse und die Netzwerklast aufgezeichnet werden, um Angriffe, ungewöhnliche Ereignisse oder Vorfälle zu entdecken bzw. derartige Ereignisse zumindest zu analysieren.
- ☒ Soweit technisch möglich, zeichnen Betriebssysteme, Anwendungen und Dienste den Austausch von Daten auf.

Eingabekontrolle

Folgende Massnahmen überwachen, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt (gelöscht) worden sind.

- ☒ Protokollierungs- und Berichtssysteme
- ☒ Jeder Nutzer hat ein personalisiertes Konto. Bietet eine Anwendung oder ein System keine Möglichkeit für die Verwendung von personalisierten Konten, so ist gewährleistet, dass nur diejenigen Personen, die ein Konto zur Erfüllung ihrer Pflichten zwingend nutzen müssen, Zugriff auf dieses Konto haben.
- ☒ Die Verwaltung von Nutzerkonten und Zugriffsberechtigungen ist organisiert und dokumentiert.

Auftragskontrolle

Folgende Massnahmen gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Datenverantwortlichen verarbeitet werden.

- ☒ Definierte Prozesse für die Beauftragung von Vertragspartnern
- ☒ Organisiertes Vertragswesen
- ☒ Kriterien zur Auswahl des Subunternehmers sind definiert
- ☒ Subunternehmer, die mit der Verarbeitung personenbezogener Daten beauftragt werden, sind vertraglich verpflichtet, die personenbezogenen Daten mindestens in dem Umfang zu schützen, wie es in diesem Vertrag vereinbart ist.

3.3 Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Folgende Massnahmen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust (physisch und logisch) geschützt werden.

- ☒ Es werden regelmässige Datensicherungen durchgeführt (täglich inkrementell sowie wöchentlich und monatlich vollständig), deren Richtigkeit und Vollständigkeit regelmässig überprüft wird.
- ☒ Speicherung von Datensicherungen an einem sicheren ausgelagerten Ort
- ☒ Spiegelung von Festplatten (z.B. RAID-Technik)
- ☒ Es besteht ein Notfall-/ Notfallwiederherstellungsplan, der den Schutz von Datenverarbeitungssystemen sowie die Speicherung personenbezogener Daten umfasst.
- ☒ Bei einem unbefugten Zutritt zu den Serverräumen wird ein Alarm ausgelöst
- ☒ Unterbrechungsfreie Stromversorgung für Speichersysteme und Server
- ☒ Geräte zur Überwachung der Temperatur und Luftfeuchtigkeit in Serverräumen
- ☒ Klimatisierte Serverräume
- ☒ Rauch- und Brandmelder, Feuerlöschgeräte in Serverräumen
- ☒ Serverräume befinden sich nicht unterhalb von Sanitärräumen

3.4 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management

Folgende Massnahmen gewährleisten ein effektives Datenschutzmanagement.

- ☒ Incident-Response-Management;
- ☒ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- ☒ Auftragskontrolle;
- ☒ Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.