Vereinbarung zur Auftragsverarbeitung

Regelungen zu Datenschutz und Datensicherheit in Auftragsverhältnissen

zwischen

[Bitte eintragen:
Firmenname
Straße Hausnummer
Postleitzahl Ort]

– Verantwortlicher –

(nachfolgend „Auftraggeber“ genannt)

und

Gedys Intraware GmbH

Eigilstraße 2

36043 Fulda

– Auftragsverarbeiter –

(nachfolgend „Auftragnehmer“ genannt)

(beide gemeinsam nachfolgend „Vertragsparteien“ genannt)

Präambel

Diese Vereinbarung zur Auftragsverarbeitung spiegelt die Vereinbarung der Parteien in Bezug auf die Bedingungen wider, die die Verarbeitung der personenbezogenen Daten des Kunden (nachfolgend „Auftraggeber" genannt) durch die Gedys Intraware GmbH (nachfolgend „Auftragnehmer" genannt) unter den zwischen den Parteien bestehenden Vertragsverhältnisses regeln. Die Vereinbarung zur Auftragsverarbeitung wird durch Bezugnahme in jeweiligen Vertragsdokumenten zwischen den Parteien rechtswirksam als Anlage in die zwischen den Parteien bestehenden Vertragsverhältnis aufgenommen.

Für Bestandskunden gilt, dass durch das Bereitstellen dieser Vereinbarung vom Auftragnehmer an den Auftraggeber das zwischen den Parteien bestehende Vertragsverhältnis rechtswirksam ergänzt und somit zwischen den Parteien rechtsverbindlich vereinbart wird.

Der Auftraggeber hat den Auftragnehmer mit der Bereitstellung von Services aus dem Produkt- und Serviceportfolio des Auftragnehmers beauftragt. In diesem Zuge verarbeitet der Auftragnehmer auch personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers.

Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung aus Art. 28 DSGVO zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

1. Gegenstand des Auftrags, Art und Zweck der Verarbeitung

(1) Beratung, Implementierung, Betreuung, Support, Wartung und Präsentationen des Gedys CXM/CRM-Systems mit allen Modulen. Der Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung ergeben sich im Weiteren aus Anlage 1.

(2) Im Übrigen ergibt sich der Gegenstand des Auftrags aus den spezifischen Projektvereinbarungen, den einzelnen Bestellungen sowie den dazugehörigen Folgeaufträgen.

2. Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Art der Daten:

Die Art der personenbezogenen Daten ergibt sich aus Anlage 1.

(2) Kreis der betroffenen Personen:

Der Kreis der betroffenen Personen ergibt sich aus Anlage 1.

3. Dauer des Auftrages

Die Verarbeitung beginnt mit der Unterzeichnung dieses Vertrags und erfolgt auf unbestimmte Zeit. Der Vertrag kann von beiden Parteien mit einer Frist von 3 Monaten zum Jahresende schriftlich gekündigt werden. Nach Beendigung des Vertrags endet die Verarbeitung personenbezogener Daten. Die Verpflichtung zur Vertraulichkeit sowie der Schutz personenbezogener Daten bestehen jedoch über das Vertragsende hinaus fort.

4. Verantwortlichkeit und Weisungsbefugnis

(1) Der Auftraggeber ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DSGVO). Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Etwas anderes gilt nur in dem in Absatz 2 genannten Umfang.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn es besteht eine anderweitige Verpflichtung durch Unionsrecht oder dem Recht des Mitgliedsstaates, dem der Auftragnehmer unterliegt. Im Falle einer anderweitigen Verpflichtung teilt der Auftragnehmer dem Auftraggeber vor der Verarbeitung unverzüglich die entsprechenden rechtlichen Anforderungen mit.

(3) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er gemäß Art. 28 Abs. 3 S. 3 DSGVO unverzüglich den Auftraggeber. Bis zur Bestätigung oder Änderung der entsprechenden Weisung ist der Auftragnehmer berechtigt, die Durchführung der Weisung auszusetzen.

5. Vertraulichkeit

Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die gemäß Art. 28 Abs. 3 S. 2 lit. b DSGVO auf die Vertraulichkeit verpflichtet worden sind und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

6. Datensicherheit

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen zum angemessenen Schutz der personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. c DSGVO in Verbindung mit Art. 32 Abs. 1 DSGVO, um die Sicherheit der Verarbeitung im Auftrag zu gewährleisten. Dazu wird der Auftragnehmer

- die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, sicherstellen sowie
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung unterhalten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen.

(2) Die Vertragsparteien vereinbaren die in dem Anlage 3 zu dieser Vereinbarung niedergelegten konkreten Datensicherheitsmaßnahmen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber über das Trustcenter (https://gedys.com/de/unternehmen/trustcenter/) mitzuteilen.

7. Einbeziehung weiterer Auftragsverarbeiter (Subunternehmer)

(1) Als Subunternehmer im Sinne dieser Regelung gelten vom Auftragnehmer beauftragte Auftragsverarbeiter, deren Dienstleistungen sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht dazu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen und Reinigung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer erteilt dem Auftraggeber hiermit die allgemeine Genehmigung zur Hinzuziehung von Subunternehmern. Die bereits mit der Unterzeichnung genehmigten eingesetzten Subunternehmer sind in Anlage 2 genannt. Über den geplanten Einsatz eines weiteren Subunternehmers oder den Austausch eines bestehenden Subunternehmers hat der Auftragnehmer den Auftraggeber rechtzeitig vorab über das Trustcenter zu informieren. Die Zustimmung zur Untervergabe gilt als erteilt, wenn der Auftraggeber nicht innerhalb von 6 (sechs) Wochen, beginnend mit Zugang der Information in vorstehendem Sinne, dem Einsatz des betreffenden Subunternehmers widerspricht. Ein solcher Widerspruch ist nur aus berechtigten Gründen zulässig, wie z. B. nicht ausreichende Zuverlässigkeit des Subunternehmers.

Widerspricht der Auftraggeber dem Einsatz eines vom Auftragnehmer gewünschten Subunternehmers, so ist der Auftragnehmer berechtigt, die Vertragsbeziehung ohne Einhaltung einer Kündigungsfrist und mit sofortiger Wirkung zu kündigen.

(3) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus. Mit dem Subunternehmer ist eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 und 4 DSGVO abzuschließen, die den Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit dieser Vereinbarung entspricht.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Die Verarbeitung der Daten durch den Auftragsverarbeiter und die vom Verantwortlichen genehmigten Subdienstleister findet grundsätzlich in Mitgliedstaaten der Europäischen Union, Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und/oder solchen Ländern statt, für die ein gültiger, auf die Verarbeitung anwendbarer Angemessenheitsbeschluss der Kommission im Sinne des Art. 45 Abs. 3 DSGVO vorliegt. Es ist dem Auftragsverarbeiter gestattet,

Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb der EU/des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und sicherstellt, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Die Regelung aus 7 (2) dieser Vereinbarung gilt somit auch für die Beauftragung von Subdienstleistern im Drittstaat.

(6) Eine weitere Auslagerung durch den Subunternehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Subunternehmer aufzuerlegen.

8. Unterstützung bei der Wahrung von Betroffenenrechten

(1) Der Auftragnehmer ist verpflichtet, den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen bei der Wahrung der in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen zu unterstützen (Art. 28 Abs. 3 S. 2 lit. e DSGVO). Insbesondere wird der Auftragnehmer den Auftraggeber darin unterstützen, Ansprüche Betroffener auf Löschung ihrer personenbezogenen Daten gemäß Art. 17 DSGVO zu erfüllen.

(2) Der Auftragnehmer darf personenbezogene Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken (Art. 28 Abs. 3 S. 2 lit. g DSGVO). Auskünfte an Dritte oder den betroffenen Personen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(3) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, um ihre Rechte gemäß Art. 12 bis 22 DSGVO geltend zu machen, wird der Auftragnehmer das Ersuchen unverzüglich an den Auftraggeber weiterleiten.

9. Unterstützung bei Dokumentations- und Meldepflichten

(1) Ist der Auftragnehmer nach Art. 37 DSGVO, § 38 BDSG gesetzlich dazu verpflichtet, einen Datenschutzbeauftragten zu benennen, teilt der Auftragnehmer dem Auftraggeber die Kontaktdaten des Datenschutzbeauftragten auf Anfrage zum Zweck der direkten Kontaktaufnahme mit.

(2) Wenn dem Auftragnehmer eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Auftraggeber unverzüglich, Art. 28 Abs. 3 lit. f, Art. 33 Abs. 2 DSGVO. Das Gleiche gilt, wenn beim Auftragnehmer beschäftigte Personen gegen diese Vereinbarung verstoßen.

(3) Nach Absprache mit dem Auftraggeber trifft der Auftragnehmer unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(4) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde gemäß Art. 33 DSGVO und ggf. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen gemäß Art. 34 DSGVO.

(5) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei einer vorherigen Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 DSGVO.

(6) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

10. Beendigung des Auftrages

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, vor Beginn der Verarbeitungsleistungen und währenddessen regelmäßig die technischen und organisatorischen Maßnahmen sowie die Einhaltung dieser Vereinbarung und datenschutzrechtlicher Vorgaben zu kontrollieren.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, nach Anmeldung und unter Berücksichtigung einer angemessenen Vorlaufzeit (mindestens 72 Zeitstunden, werktäglich) durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem direkten Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist diejenigen Auskünfte zu erteilen, die zum Nachweis der Einhaltung der Pflichten unter diesem Auftragsverarbeitungsvertrag sowie zum Nachweis der technischen und organisatorischen Maßnahmen erforderlich sind. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit vorlegen. Der Auftraggeber hat dem Auftragnehmer den durch die Erteilung der Auskünfte entstehenden Aufwand zu vergüten.

12. Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gemäß Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz, oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung entspricht.

13. Schlussbestimmungen

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Auftraggebers.

(2) Sollten einzelne oder mehrere Regelungen dieser Vereinbarung unwirksam sein, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht.

(3) Im Falle eines Widerspruchs zwischen der Auftragsbestätigung und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(4) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(5) Sollten die übermittelten Daten bzw. die entsprechenden Datenträger beim Auftragsverarbeiter durch Maßnahmen Dritter einschließlich hoheitlicher Akte (z.B. Pfändung, Beschlagnahme) oder durch sonstige Ereignisse in ihrem Bestand oder hinsichtlich des uneingeschränkten Zugriffs des Auftraggebers gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich zu verständigen und – soweit möglich – Sicherungsmaßnahmen zu ergreifen.

(6) Die folgenden Anhänge sind Bestandteil dieser Vereinbarung:

- Anlage 1: Angaben zur Datenverarbeitung
- Anlage 2: Genehmigte Subunternehmer
- Anlage 3: Technische und organisatorische Maßnahmen

Unterschriften

[Bitte eintragen: Ort, Datum]

_____	_____
Auftraggeber	Auftragnehmer
[Bitte eintragen: Name Auftraggeber]	[Bitte eintragen: Name Auftragnehmer]

Anlage 1

Angaben zur Datenverarbeitung (Art. 28 Abs. 3 S. 1 DSGVO)

Diese Anlage 1 enthält die auftragsspezifischen Leistungen und Datenverarbeitung i.S.d. Art. 28 Abs. 3 S. 1 DSGVO für die jeweils vom Auftragnehmer erbrachten Services. Die für diese Vereinbarung geltenden Angaben richten sich stets nach den konkreten Services, die Inhalte des Angebots sowie ergänzender Vereinbarungen sind.

Der Auftragnehmer stellt dem Auftraggeber eine Software zur Verfügung, in welcher dieser personenbezogene Daten verarbeitet. Im Zuge der Implementierung der Lösung sowie im Falle von Supportleistungen hat der Auftragnehmer Zugriff auf die Systeme des Auftraggebers. Ein Zugriff auf personenbezogene Daten des Auftraggebers kann hierbei nicht ausgeschlossen werden. Je nach konkretem Einsatz und Kundenkonfiguration bestimmt sich der Gegenstand der Verarbeitung und werden die Daten verarbeitet, welche der Kunde über das System abbilden lässt.

Gedys CXM/CRM (On-Premises-Leistung)

Gegenstand der Verarbeitung	**Art der Daten**	**Kreis der Betroffenen**	**Zweck**
Bereitstellung und Einführung des Gedys CXM/CRM-Systems im unternehmensinternen Umfeld des Auftraggebers zur Verwaltung und Analyse von Kundendaten Zugriff im Rahmen des Supports, der Wartung und Systemkonfigurationen und -aktualisierungen sowie Anpassungen der CXM/CRM-Software Schnittstellenverwaltung.	Alle Daten, die im Rahmen Nutzung der CXM/CRM-Software durch den Auftraggeber verarbeitet werden, insbesondere: ▪ Kunden-/Lieferanten-/ Mitarbeiterstammdaten ▪ Kommunikationsdaten ▪ Kontakt-/ Kundennummer ▪ Vertragsstammdaten ▪ Kundenhistorie ▪ Vertragsabrechnungs- und Zahlungsdaten ▪ Vertriebsdaten	Alle Betroffenen, deren Daten im Rahmen der Gedys-Systeme durch den Auftraggeber verarbeitet werden, insbesondere: ▪ Kunden ▪ Partner ▪ Interessenten ▪ Lieferanten ▪ Ansprechpartner der Kunden/ Partner/ Interessenten/ Lieferanten ▪ Beschäftigte/ Mitarbeitende	Unterstützung bei Implementierung, Konfiguration, Programmierung, Fehlerbehebung und Support, Wartung und Update des Systems.

Gedys CXM/CRM (SaaS/Hosting-Leistung)

Gegenstand der Verarbeitung	**Art der Daten**	**Kreis der Betroffenen**	**Zweck**
Implementierung und Betrieb des Gedys CXM/CRM in der Cloud: Bereitstellung der cloudbasierten Lösung inklusive Datenspeicherung und -sicherung. Zugriff im Rahmen des Supports, der Wartung und Systemkonfigurationen und -aktualisierungen sowie Anpassungen der CXM/CRM-Software, inkl. Revisionsmanagement Schnittstellenverwaltung Berichtswesen und Monitoring Zugriffskontrollen und Authentifizierung.	Alle Daten, die im Rahmen Nutzung der CXM/CRM-Software durch den Auftraggeber verarbeitet werden, insbesondere: ▪ Kunden-/Lieferanten-/ Mitarbeiterstammdaten ▪ Kommunikationsdaten ▪ Kontakt-/ Kundennummer ▪ Vertragsstammdaten ▪ Kundenhistorie ▪ Vertragsabrechnungs- und Zahlungsdaten ▪ Vertriebsdaten	Alle Betroffenen, deren Daten im Rahmen der GEDYS-Systeme durch den Auftraggeber verarbeitet werden, insbesondere: ▪ Kunden ▪ Partner ▪ Interessenten ▪ Lieferanten ▪ Ansprechpartner der Kunden/ Partner/ Interessenten/ Lieferanten ▪ Beschäftigte/ Mitarbeitende	Unterstützung bei Implementierung, Konfiguration, Programmierung, Fehlerbehebung und Support, Wartung und Update des Systems.

Anlage 2

Subunternehmerliste siehe hier: https://gedys.com/de/unternehmen/trustcenter/

Anlage 3

Technische und organisatorische Maßnahmen

Die Gedys Intraware GmbH als Anbieter von CRM-Software und zugehörigen Services hat eine Vielzahl technischer und organisatorischer Maßnahmen implementiert, um die vom Auftraggeber übermittelten Daten zu schützen. Diese Maßnahmen sind darauf ausgelegt, den Anforderungen des Datenschutzes und der Datensicherheit gerecht zu werden und gewährleisten insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Die festgelegten Sicherheitsvorkehrungen werden kontinuierlich überwacht und gepflegt, um einen hohen Standard im Bereich des Datenschutzes zu gewährleisten. Dabei wird stets berücksichtigt, dass detaillierte Informationen zu spezifischen Sicherheitsmaßnahmen aus Gründen des Schutzes vor unbefugtem Zugriff und zur Vermeidung von Sicherheitslücken nicht in vollem Umfang offengelegt werden können. Dies ist besonders im Kontext von Datenschutz und Datensicherheit erforderlich, da der Schutz dieser Maßnahmen gegen unbefugte Offenlegung mindestens ebenso wichtig ist wie die Sicherheitsmaßnahmen selbst.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle

Die Zutrittskontrolle dient dem physischen Schutz von Datenverarbeitungsanlagen, die personenbezogene Daten verarbeiten, indem sie unbefugtem Zugang wirksam vorbeugt. Der Begriff „Zutritt" bezieht sich dabei auf den räumlichen Zugang zu den betroffenen Anlagen.

- Sicherheitsschlösser
- Zutrittsberechtigungskonzept
- Manuelles Schließsystem
- Schließsystem mit Codesperre
- Schlüsselregelung/Schlüsselbuch
- Chipkarten-/Transponder-Schließsystem
- Rechenzentren mit Standort in Deutschland oder der EU
- separate Serverräume
- Sorgfältige Auswahl von Reinigungspersonal

Zugangskontrolle

Die Zugangskontrolle stellt sicher, dass das Eindringen Unbefugter in DV-Systeme sowie deren unbefugte Nutzung verhindert wird, indem nur autorisierte Personen Zugang zu den Systemen erhalten.

- Getrenntes Gäste-WLAN
- Detaillierte Benutzerprofile
- Authentifikation mit Benutzer + Passwort
- Passwortregelungen
- Verwendung von individuellen Passwörtern
- Passwörter mit einer Mindestlänge

- Anzahl von aufeinanderfolgenden Fehlversuchen ist begrenzt
- Passworthistorie
- Schlüsselregelung
- Verschlüsselung von mobilen Datenträgern
- Autonome Fernwartung
- Zugriff nur per VPN auf internem Server
- Zentrale Änderung der Zugangsberechtigungen durch IT-Verantwortliche
- Protokollierung der Serverzugriffe auf Benutzerebene

Zugriffskontrolle

Die Zugriffskontrolle sorgt dafür, dass nur befugte Nutzer auf EDV-Systeme zugreifen können und dieser Zugriff auf die für ihre Aufgaben notwendigen Daten beschränkt ist. Unerlaubte Tätigkeiten außerhalb der eingeräumten Berechtigungen werden effektiv verhindert.

- Detailliertes Berechtigungskonzepts
- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduzieren
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (i.d.R. Möglichkeit mit Zertifikat)
- Einsatz von Intrusion-Detection-Systemen
- Einsatz von VPN-Technologie
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Einsatz von Anti-Viren-Software

Trennungskontrolle

Die Trennungskontrolle stellt sicher, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt verarbeitet werden.

- Festlegung von Datenbankrechten
- Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten
- anderer Kunden Rechnung trägt
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)

Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, dass personenbezogene Daten während der Übertragung, des Transports oder der Speicherung auf Datenträgern vor unbefugtem Zugriff, Veränderung, Kopieren oder Löschung geschützt sind. Aspekte der Weitergabe personenbezogener Daten sind zu regeln.

- Elektronische Übertragung, Datentransport, sowie deren Kontrolle.
- Einsatz von verschlüsselten Verbindungen (z.B. VPN, TLS)
- Sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Shredder für die sichere Vernichtung von Daten
- Datenschutzboxen für die Entsorgung von vertraulichen Papierdokumenten

Eingabekontrolle

Die Eingabekontrolle stellt sicher, dass nachvollzogen werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder gelöscht wurden. Die Dokumentation und Nachvollziehbarkeit der Datenverwaltung und -pflege sind zu gewährleisten.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Folgende Aktivitäten werden protokolliert: Hoch- und Herunterfahren von zentralen Rechnern (v.a. Servern und Firewalls)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

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

Verfügbarkeitskontrolle und Belastbarkeit

Die Verfügbarkeitskontrolle stellt sicher, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind. Systeme müssen in der Lage sein, mit risikobedingten Veränderungen umzugehen und eine hohe Toleranz sowie Ausgleichsfähigkeit gegenüber Störungen aufzuweisen.

- Feuerlöschgeräte in Serverräumen
- Testen von Datenwiederherstellung
- Schutzsteckdosenleisten in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Backup- & Recoverykonzept
- Unterbrechungsfreie Stromversorgung (USV)
- Aufbewahrung von Datensicherung an einem sicheren, separaten Ort
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen/IT-Räumen

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

Kontrollverfahren

Im Rahmen der Kontrollverfahren gewährleistet der Auftragnehmer, dass personenbezogene Daten nur gemäß den Weisungen des Auftraggebers verarbeitet werden. Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen ist zu implementieren.

- Unternehmensrichtlinien (Code of Conduct) vorhanden
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzkoordinator und -beauftragten
- Datenschutz-Management vorhanden
- Datenschutz-Konzept vorhanden

Technische und Organisatorische Maßnahmen beim mobilen Arbeiten

Die Gedys Intraware ermöglicht ihren Mitarbeitenden, anfallende Arbeiten via Remote-Zugang durchzuführen. Hierfür wurden Maßnahmen ergriffen, um dem Sicherheitsstandard des allgemeinen Sicherheitskonzeptes zu entsprechen. Dieses gilt, soweit anwendbar und wird um die folgenden Maßnahmen ergänzt.

Die Maßnahmen unterteilen sich in technische Maßnahmen, die den Zugang zum System betreffen sowie in organisatorische Maßnahmen, die den Umgang des jeweiligen Mitarbeiters mit Daten an seinem Heimarbeitsplatz betreffen.

Technische Maßnahmen

Die nachfolgenden Maßnahmen stellen die zusätzlich ergriffenen Maßnahmen dar. Für den Zugriff auf das System hat Gedys Intraware/Proalpha folgende Maßnahmen getroffen:

- Zugang ausschließlich über dienstliche Endgeräte
- Endgeräte werden IT-seitig regelmäßigen Updates unterzogen
- Applikationen dürfen ausschließlich nach Konsultation der hierfür vorliegenden Whitelist installiert werden. IT-seitig nicht zugelassene Applikationen dürfen nicht installiert werden.
- Ein Zugriff erfolgt ausschließlich durch eine verschlüsselte VPN-Verbindung
- Windows Clients
  - Endpoint Security
  - Antivirus Software
  - Systemverschlüsselung
- iOS Clients
  - verwaltet durch Intune Mobile Device Management (MDM)
    - Kontrolle über das Gerät mit Möglichkeit zum remote „wipe" bzw. „lock"
  - komplette Verschlüsselung des Gerätes
  - geschützt durch sechsstelligen Pass Code

- Restriction policy
  - nicht vertrauenswürdige Zertifikate können nicht manuell akzeptiert werden
  - keine Diagnosedaten an Apple
  - Benutzer kann keinen 3rd-Party Apps manuell vertrauen

Organisatorische Maßnahmen

In organisatorischer Hinsicht wurden in Ergänzung zu den Maßnahmen der allgemeinen TOM verschiedene Zusatzvereinbarungen sowie interne Richtlinien erlassen. Dies umfasst unter anderem Folgende Regelungen und Verpflichtungen:

- Zutritts- und Kontrollrecht des Arbeitsplatzes durch interne beauftragte Prüfer (z.B. Fachkraft für Arbeitssicherheit oder betrieblicher Datenschutzkoordinator/-beauftragter)
- Verpflichtung auf interne Richtlinie zur Nutzung technischer Einrichtungen
- Verpflichtung zum Schutz des Zugriffs unbefugter Dritter auf Arbeitsmittel
- Untersagung der Verwendung eigener technischer Einrichtungen (Ausgenommen WLAN, Peripheriegeräten wie Tastatur und Maus ohne Treiberinstallation)
- Verpflichtung, vertrauliche dienstliche Dokumente unter Verschluss zu halten (Cleandesk)
- Verpflichtung auf Vertraulichkeit/zur Geheimhaltung
- Verpflichtung, Wohnortswechsel mitzuteilen