Anlage zum Servicevertrag - Datenschutz

1. Allgemeines

Diese Vereinbarung wird als Ergänzung zur Einhaltung der datenschutzrechtlichen Regelungen des Art. 28 DS-GVO getroffen.

INNEO führt im Auftrag des Auftraggebers Service-, Wartungs- und/oder Pflegeleistungen durch. In diesem Zusammenhang ist es nicht ausgeschlossen, dass INNEO personenbezogene Daten verarbeitet, um die Leistungen durchzuführen oder durchführen zu können.

Zwischen INNEO und dem Auftraggeber besteht diesbezüglich ein Vertragsverhältnis (Servicevertrag).

2. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags ist die Durchführung der im Servicevertrag beschriebenen Leistungen wie beispielsweise technischer Support.

(2) Dauer

Die Dauer dieser Vereinbarung gilt für die Laufzeit des Servicevertrages.

Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten können folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien) sein:

- ☒ Personenstammdaten
- ☒ Kommunikationsdaten (z.B. Telefon, E-Mail)
- ☒ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- ☒ Kundenhistorie
- ☒ Vertragsabrechnungs- und Zahlungsdaten
- ☒ Planungs- und Steuerungsdaten
- ☒ CAD Daten, Produktdaten, Stücklisten, Zeichnungen, Dokumente mit Hinweisen zum Bearbeiter und anderen Versionierungsinformationen
- ☒ Zugangsdaten
- ☒ Backupdaten
- ☒ Logfiles

(3) Kategorien betroffener Personen können sein:

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Beschäftigte des Auftraggebers
- ☒ Ansprechpartner
- ☒ Geschäftspartner des Auftraggebers

3. Technisch-organisatorische Maßnahmen

(1) INNEO wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. INNEO verpflichtet sich, für die zu verarbeitenden Daten angemessene und dem Stand der Technik entsprechende technische und organsatorische Sicherheitsmaßnahmen nach den für den Auftraggeber einschlägigen deutschen und europäischen Datenschutzgesetzen zu treffen.

(2) INNEO verpflichtet sich zur Einhaltung der INNEO Standard TOMs. Der Auftraggeber kann diese jederzeit unter datenschutzbeauftragter@inneo.com anfordern. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es INNEO gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) INNEO darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an INNEO wendet, wird INNEO dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft sind durch den Auftraggeber sicherzustellen. INNEO unterstützt jedoch den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der

INNEO hierdurch entstehenden nachzuweisenden Aufwände und Kosten bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen gemäß Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

5. Qualitätssicherung und sonstige Pflichten INNEOs

INNEO hat zusätzlich zu der Einhaltung der Regelungen dieser Vereinbarung gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet INNEO insbesondere die Einhaltung folgender Vorgaben:

(a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt.

Der Datenschutzbeauftragte von INNEO ist unter folgenden Kontaktdaten erreichbar:

INNEO Solutions GmbH
Datenschutzbeauftragter
IT-Campus 1
73479 Ellwangen

Tel.: ***07961/890 137***

E-Mail: ***datenschutzbeauftragter@inneo.com***

(b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. INNEO setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. INNEO und jede INNEO unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten siehe INNEO Standard TOMs].

(d) Der Auftraggeber und INNEO arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung bei INNEO ermittelt.

(f) INNEO kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach dieser Vereinbarung.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung gemäß dem Servicevertrag beziehen. Nicht hierzu gehören Nebenleistungen, die INNEO z. B. als Telekommunikationsleistungen, 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 von Datenverarbeitungsanlagen in Anspruch nimmt. INNEO 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 Auftraggeber stimmt der Beauftragung derjenigen Softwarehersteller als Unterauftragnehmer zu, deren Software Gegenstand des bestehenden Servicevertrages mit INNEO ist.

(3) INNEO darf weitere Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. INNEO hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu überprüfen, dass dieser die zwischen Auftraggeber und INNEO getroffenen Vereinbarungen einhalten kann. Die Verpflichtung des Unterauftragnehmers muss den Anforderungen von Art. 28 Abs. 4 DS-GVO entsprechen.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt INNEO die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit INNEO Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer, die nicht in einem Wettbewerbsverhältnis zu INNEO stehen, durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch INNEO in dessen Geschäftsbetrieb zu überzeugen. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe von INNEO dabei nicht unverhältnismäßig stören.

(2) INNEO stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten überzeugen kann. INNEO verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. INNEO weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach. Der Nachweis der Umsetzung geeigneter Maßnahmen kann auch durch eine Selbstauditierung

bzw. die Vorlage aktueller Testate, Berichte oder Berichtsauszüge unabhängiger Prüfer (Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, etc.) erbracht werden.

(3) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen von INNEO hat der Auftraggeber INNEO die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann INNEO eine Erstattung der INNEO hierdurch entstehenden nachzuweisenden Aufwände und Kosten geltend machen.

8. Mitteilung bei Verstößen

(1) INNEO unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

(a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

(b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

(c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

(d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

(e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Servicevertrages enthalten oder nicht auf ein Fehlverhalten INNEOs zurückzuführen sind, kann INNEO eine Erstattung der INNEO hierdurch entstehenden nachzuweisenden Aufwände und Kosten beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechtes, insbesondere für die Rechtmäßigkeit der Datenverarbeitung sowie für die Wahrung der Betroffenenrechte, allein verantwortlich.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) INNEO hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. INNEO ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Servicevertrages – hat INNEO sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch INNEO entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. INNEO kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.