Hamburg, 09.09.2024

Auftragsverarbeitungsvertrag

Uniberry GmbH
Eimsbütteler Str. 53-55
22769 Hamburg

Ansprechpartner: Felix Ueckermann
info@comydo.com
+49 (0)40 228656650

Der Auftraggeber (für die Verarbeitung verantwortlich) und Comydo schließen den folgenden Vertrag zur Auftragsverarbeitung gemäß Art. 28 der europäischen Datenschutz-Grundverordnung (DSGVO). Dieser Auftragsverarbeitungsvertrag (im Folgenden „AVV“) bildet als Anhang zu den Allgemeinen Geschäftsbedingungen (im Folgenden „AGB“) von Comydo einen integralen Bestandteil des Vertragsverhältnisses zwischen den Vertragsparteien und wird gemeinsam mit diesen Vertragsgegenstand. Auf Grundlage dieses Vertragsverhältnisses verarbeitet Comydo personenbezogene Daten für den Auftraggeber. Die sich daraus ergebenden datenschutzrechtlichen Rechte und Verpflichtungen der Parteien werden durch diesen Auftragsverarbeitungsvertrag konkretisiert. Die Anlagen zu diesem Vertrag sind ebenfalls Bestandteil der Vereinbarung. Die getroffenen Regelungen finden Anwendung auf alle Leistungen welche Comydo für den Auftraggeber erbringt und sämtliche damit verbundenen Tätigkeiten, welche eine Verarbeitung personenbezogener Daten zur Folge haben und zur Folge haben können.

§ 1 Gegenstand und Dauer der Verarbeitung

a) Gegenstand des Vertrages ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch Comydo für den Auftraggeber in dessen Auftrag und nach dessen Weisung. Der Gegenstand und die Dauer des Vertrages richten sich nach dem Hauptvertrag.

b) Der Auftraggeber kann diesen Vertrag sowie den Hauptvertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von Comydo gegen die Bestimmungen dieser Vereinbarung vorlieget, ein solcher schwerwiegender Verstoß liegt insbesondere dann vor, wenn Comydo die Daten des Auftraggebers für andere als die nach dieser Vereinbarung bestimmten Zwecke verwendet oder gegen eine wesentliche Pflicht aus dieser Vereinbarung verstößt.

c) Auch bei Nichtvorliegen der zuvor genannten Voraussetzungen ist der Auftraggeber berechtigt, diese Vereinbarung und den Hauptvertrag fristlos zu kündigen, wenn Comydo wiederholt gegen diese Vereinbarung verstößt. Ein vorheriger schriftlicher Hinweis oder ein Hinweis in Textform des Auftraggebers ist hierfür Voraussetzung.

§ 2 Umfang, Art und Zweck der Verarbeitung

Umfang, Art und Zweck der Verarbeitung personenbezogener Daten ergeben sich aus dem zwischen den Parteien geschlossenen Dienstleistungsvertrag. Comydo führt dabei insbesondere folgende Verarbeitungen für den Auftraggeber durch:

- Kontaktdaten des Kunden, um den Geräteversand und die Inbetriebnahme zu koordinieren.
- Anlegen eines Nutzerkontos, über das sich sämtliche Funktionen des Systems steuern lassen. Dies umfasst Informationen zum Gebäudebestand und Zutrittsberechtigungen.
- Zutrittsberechtigungen können mit persönlichen Daten des Zutrittsuchenden verknüpft werden.
- Im operativen Betrieb werden Zutrittsberechtigungen geprüft.
- Erstellung von Log-Files.

§ 3 Art der personenbezogenen Daten

Comydo erhält Zugriff auf folgende personenbezogene Daten (dadurch, dass der Auftraggeber ihm die Daten bereitstellt oder ihm einen Zugriff auf die Daten ermöglicht), bzw. der Auftraggeber erlaubt Comydo folgende personenbezogene Daten zu erheben:

- Personenstammdaten (z.B. Vorname, Nachname)
- Kontaktdaten (z.B. E-Mail-Adresse)
- Vertragsdaten (z.B. Kundennummer)
- User-Account-Informationen

§ 4 Kreis der betroffenen Personen

Bei den betroffenen Personen der oben aufgelisteten Daten handelt es sich um:

- Kunden
- Auftraggeber/ Dienstleister

§ 5 Rechte und Pflichten des Auftraggebers; Kontrollrechte

a) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie zur Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich und somit Verantwortlicher im Sinne des Art. 4 Abs. 7 DSGVO.

b) Der Auftraggeber erteilt Comydo Weisungen über die Art und den Umfang der Verarbeitung der personenbezogenen Daten. Die Weisungen erfolgen grundsätzlich in Textform und sind von den Parteien zu dokumentieren.

c) Vor Beginn des Auftrages und der damit verbundenen Datenverarbeitung sowie im Anschluss ist der Auftraggeber in regelmäßigen Abständen berechtigt, sich nach rechtzeitiger vorheriger Anmeldung zu den üblichen Geschäftszeiten, von der Einhaltung der bei Comydo getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen.

d) Comydo erklärt sich damit einverstanden, dass sich der Auftraggeber jederzeit nach vorheriger Ankündigung von der Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang (in der Regel maximal einmal im Kalenderjahr) selbst oder durch Dritte überzeugen kann, dies insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Systeme sowie sonstige Kontrollen vor Ort.

e) Comydo hat eventuelle Kontrollmaßnahmen der Datenschutzaufsichtsbehörde gem. Art. 58 DSGVO zu dulden. Er wird den Auftraggeber unverzüglich nach Ankündigung oder Kenntniserlangung über die Durchführung der Kontrollmaßnahme sowie bei anderweitigen Anfragen, Ermittlungen oder

Erkundigungen der Datenschutzaufsichtsbehörde, insbesondere auch, wenn diese im Rahmen einer vorherigen Konsultation gem. Art. 36 DSGVO erfolgen, informieren, soweit die Maßnahmen oder Anfragen Datenverarbeitungen betreffen können, die Comydo für den Auftraggeber erbringt.

Auf Verlangen des Auftraggebers weist Comydo die Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis durch die Vorlage eines aktuellen Testats oder Berichts (wie z.B. Wirtschaftsprüfer, externer Datenschutzbeauftragter, Revisor oder einem externen Datenschutzauditor) und gegebenenfalls einer geeigneten Zertifizierung (z.B. nach BSI-Grundschutz, ISO27001 oder nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO) oder die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO erbracht werden. Die Kontrollrechte des Auftraggebers bleiben hiervon unberührt.

§ 6 Pflichten von Comydo

a) Comydo ist verpflichtet, personenbezogene Daten ausschließlich weisungsgemäß und nach den Vorgaben dieses Vertrages zu verarbeiten.

b) Bei der Gewährung der Rechte der Betroffenen gemäß Art. 15 ff. DSGVO (Berichtigung, Einschränkung der Verarbeitung, Löschung, Benachrichtigung und Auskunftserteilung) wird Comydo den Auftraggeber auf erstes Anfordern im Rahmen seiner Möglichkeiten unterstützen. Comydo wird hierfür geeignete technische und organisatorische Maßnahmen treffen. Comydo hat auf Weisung die personenbezogenen Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder die Verarbeitung einzuschränken.

c) Sollte die im Auftrag des Auftraggebers erhobenen Daten Gegenstand eines Verlangens auf Datenportabilität gemäß Art. 20 DSGVO sein, wird Comydo dem Auftraggeber den betreffenden Datensatz unverzüglich auf Anforderung in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen.

d) Sofern sich eine betroffene Person unmittelbar an Comydo mit der Wahrnehmung ihrer Betroffenenrechte wendet, hat dieser dieses Ersuchen unverzüglich an den Auftraggeber weiterzuleiten.

e) Comydo wird den Auftraggeber unverzüglich darauf hinweisen, wenn dieser der Meinung ist, dass eine erteilte Weisung gegen gesetzliche Vorschriften verstößt. Die Durchführung der entsprechenden Weisung kann dieser so lange aussetzen, bis sie durch den Auftraggeber bestätigt oder abgeändert wird.

f) Nach Beendigung des Hauptvertrages ist Comydo verpflichtet, sämtliche in seinen Besitz gelangten personenbezogenen Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen sowie datenschutz- und datensicherheitskonform und gemäß den Weisungen zu löschen. Dies betrifft auch etwaige Datensicherungen bei Comydo. Die datenschutz- und datensicherheitskonforme Löschung ist zu dokumentieren mit Datumsangabe dem Auftraggeber schriftlich zu bestätigen.

g) Comydo stellt sicher, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und andere für Comydo tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet Comydo, dass sich die zur Verarbeitung der

personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht erstreckt sich ebenfalls auf Home- und Telearbeit und besteht nach Beendigung des Auftrages fort.

h) Die/der Auftragnehmer:in stellt sicher, dass im Falle einer Verletzung personenbezogener Daten der Auftraggeberin bzw. des Auftraggebers, sie/er unverzüglich diese/n informiert und bei deren/dessen Pflichten gemäß Art. 33 – 36 DSGVO entsprechend unterstützt.

i) Comydo bestätigt, dass er, einen Datenschutzbeauftragten bestellt hat und die Einhaltung der Vorschriften zum Datenschutz und zur Datensicherheit unter Einbeziehung des Datenschutzbeauftragten überwacht.

Datenschutzbeauftragter von Comydo ist:

RA Philipp Heindorff
ph@freshcompliance.de
Fresh Compliance GmbH
Schönhauser Allee 43a
10435 Berlin

§ 7 Leistungsort

a) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung durch den Auftraggeber und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

b) Sofern die Verarbeitung personenbezogener Daten außerhalb der EU erfolgt, garantiert Comydo, dass die nach den jeweils geltenden Datenschutzvorschriften anwendbaren Voraussetzungen für das Eingreifen eines Erlaubnistatbestandes für die Verarbeitung personenbezogener Daten außerhalb der EU erfüllt sind ("datenschutzrechtliche Rechtfertigung"). Dies ist zum einen gegeben, sofern und soweit die EU-Kommission diesem bzw. dieser ein angemessenes Schutzniveau bescheinigt hat. Außerdem, wenn die Verarbeitung aufgrund geeigneter Garantien im Sinne von Art. 46 Abs. 1 lit. c) (EU-Standardvertragsklauseln) mit weiteren Sicherheitsvorkehrungen durch die/den Auftragnehmer:in erfolgt. Weiterhin wenn die Verarbeitung der personenbezogenen Daten außerhalb der EU ausschließlich im Rahmen eines Programms erfolgt, dem von der EU-Kommission ein angemessenes Schutzniveau bescheinigt wurde (gegenwärtig z.B. das EU-US Dara Privacy Framework), und er die für die Teilnahme an dem Programm erforderlichen formellen und inhaltlichen Voraussetzung erfüllt, er sich hierfür qualifiziert hat und während der Laufzeit des Auftrages ununterbrochen für das Programm qualifiziert bleibt.

§ 8 Unterauftragsverhältnisse

a) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber im Einzelfall.

b) Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

c) Bei Einschaltung eines weiteren Auftragsverarbeiter muss stets ein Schutzniveau, welches mit demjenigen dieser Vereinbarung vergleichbar ist, gewährleistet werden. Comydo bleibt jedoch zu jeder Zeit verantwortlich für jegliche Handlung oder Unterlassung der von ihm beauftragten weiteren Auftragsverarbeiter, in selber Weise wie er für die eigenen Handlungen und Unterlassungen verantwortlich ist.

d) Comydo hat die Einhaltung der Pflichten des weiteren Auftragsverarbeiters regelmäßig zu überprüfen. Comydo hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der weitere Auftragsverarbeiter die zugesicherten und erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.

e) Comydo arbeitet derzeit bei der Erfüllung des Auftrags mit den folgenden weiteren Auftragsverarbeitern zusammen, mit deren Beauftragung sich der Auftraggeber einverstanden erklärt:

Name und Anschrift des Subunternehmers	Beschreibung der Leistungen
Google Ireland Limited Gordon House Barrow Street Dublin 4 Ireland (Serverstandort ausschließlich Frankfurt/Deutschland)	Bereitstellung von Server-Infrastruktur für: Geräte-Kommunikation • Geräte-Monitoring • Prüfung von Zutrittsanfragen • Auswertung von Protokolldaten Verarbeitung von Kundendaten lediglich in pseudonymisierter Form.
Hetzner Online GmbH Industriestr. 25 91710 Gunzenhausen	• Hosting der Web-Anwendung • Verwaltung der Zutrittscodes • Datenhaltung
Uberspace Kaiserstraße 15 55116 Mainz	• Mailserver • Automatischer Versand von System-Mails und Key-Mails
Raidboxes GmbH Hafenstraße 32 48153 Münster	• Hosting der statischen Homepage (Infoseite) • Kontaktformular

Pipedrive OÜ Kompanii 2 Tartu 51004, Estonia	• Verwaltung von Kundenleads
Haufe-Lexware GmbH & Co. KG Ein Unternehmen der Haufe Group Munzinger Straße 9 79111 Freiburg	• Lexoffice, Abrechnung
sipgate GmbH Gladbacher Straße 74 40219 Düsseldorf	• Telefondienste für Supportanfragen über Telefon

§ 9 Technische und organisatorische Maßnahmen

a) Comydo ist verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung gem. Art 32 i.V.m Art. 5 Abs. 1 DSGVO einzuhalten. Er wird alle erforderlichen Maßnahmen zur Sicherung der Daten bzw. der Sicherheit der Verarbeitung, insbesondere auch unter Berücksichtigung des Standes der Technik, sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. Die zu treffenden Maßnahmen umfassen insbesondere Maßnahmen, mit denen eine angemessene Pseudonymisierung und Verschlüsselung gewährleistet werden kann sowie Maßnahmen zum Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Maßnahmen, die die Kontinuität der Verarbeitung nach Zwischenfällen gewährleisten.

b) Die von Comydo getroffenen technischen und organisatorischen Maßnahmen sind ausführlich in der Anlage zu diesem Vertrag dargestellt und sind Vertragsbestandteil.

§ 10 Haftung

a) Comydo haftet gegenüber dem Auftraggeber gemäß der gesetzlichen Regelungen für sämtliche Schäden durch schuldhafte Verstöße gegen diesen Vertrag, sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen, die Comydo, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten bei der Erbringung der vertraglichen Leistung verursachen.

b) Für den Ersatz von Schäden, die ein Betroffener aufgrund einer nach der DSGVO oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses geltend macht, der Auftraggeber bzw. Comydo gem. Art. 82 DSGVO gegenüber dem Betroffenen verantwortlich. Comydo stellt den Auftraggeber im Innenverhältnis von allen Schadensersatzansprüchen frei, die aufgrund einer schuldhaften Verletzung der Verpflichtungen aus diesem Vertrag durch Comydo gegen den Auftraggeber geltend gemacht werden.

§ 11 Löschung und Rückgabe personenbezogener Daten

a) Die/der Auftragnehmer:in darf ohne Kenntnis und Zustimmung der Auftraggeberin bzw. des Auftraggebers keine Kopien oder Duplikate der Daten erstellen, außer zur Datensicherung oder Erstellung technischer Kopien für folgende Zwecke:

- Zur Durchführung der Verarbeitungstätigkeiten im Rahmen dieses AVV;

- zur Bereitstellung von Nachweisen für die ordnungsgemäße Datenverarbeitung; oder
- zur Erfüllung gesetzlicher Aufbewahrungspflichten.

b) Nach Beendigung der vertragsgemäßen Auftragsverarbeitung oder auf Verlangen der Auftraggeberin bzw. des Auftraggebers früher, spätestens jedoch bei Beendigung des Vertrags, gibt die/der Auftragnehmer:in der/dem Auftraggeber:in alle Dokumente, Verarbeitungs- und Nutzungsergebnisse und Datensätze, soweit sich diese auf diesen Vertrag beziehen, zurück oder – nach erteilter Einwilligung – löscht bzw. zerstört diese auf eine mit dem Datenschutzrecht vereinbare Weise. Das gleiche gilt für alle damit in Zusammenhang stehenden Test-, Ausschuss-, redundanten und ausrangierten Materialien. Das Protokoll des Löschvorgangs bzw. der Zerstörung ist auf Anfrage zur Verfügung zu stellen.

c) Jede Dokumentation, die dem Nachweis einer ordnungsgemäßen Datenverarbeitung nach diesem Vertrag dient, kann von der Auftragnehmerin bzw. vom Auftragnehmer über die Vertragsdauer hinaus nach Maßgabe der jeweils geltenden Aufbewahrungsfristen gespeichert werden. Am Ende der Vertragsdauer kann die/der Auftragnehmer:in solche Dokumentation der/dem Auftraggeber:in aushändigen, so dass sie/er damit von dieser vertraglichen Verpflichtung entbunden ist.

d) Die Einrede des Zurückbehaltungsrechts (§ 273 BGB) wird hinsichtlich der für die/den Auftraggeber:in verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

§ 12 Schlussbestimmungen

a) Im Falle von Widersprüchen zwischen den Bestimmungen in dieser Vereinbarung und den Regelungen des Hauptvertrages gehen die Bestimmungen dieser Vereinbarung vor.

b) Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich erfolgen und bedürfen der ausdrücklichen Angabe, dass damit die vorliegenden Bestimmungen geändert und/oder ergänzt werden. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

c) Sollte eine Bestimmung dieser Vereinbarung unwirksam oder nicht durchsetzbar sein oder werden, so bleiben die übrigen Bestimmungen dieser Vereinbarung hiervon unberührt. Die unwirksame oder nicht durchsetzbare Bestimmung ist durch eine wirksame und durchsetzbare Bestimmung zu ersetzen, welche dem Zweck der ersetzenden Bestimmung am nächsten kommt.

d) Diese Vereinbarung unterliegt deutschem Recht.

e) Sofern der Zugriff auf die Daten durch Maßnahmen Dritter (z.B. Maßnahmen eines Insolvenzverwalters, Beschlagnahme durch Finanzbehörden, etc.) gefährdet wird, hat Comydo den Auftraggeber unverzüglich hierüber zu benachrichtigen.

ANLAGE - Technische und organisatorische Maßnahmen

Alle kritischen und relevanten Bereiche der IT-Infrastruktur, die für den Betrieb der von uns angebotenen Dienstleistungen notwendig sind, werden von zertifizierten Hosting-Partnern zur Verfügung gestellt. Die von Google und Hetzner garantierten TOMs sind maßgeblich für die Beurteilung des von Comydo gebotenen Sicherheitsniveaus. Darüber hinaus versichert Comydo die folgenden technischen und organisatorischen Maßnahmen in den eigenen Räumlichkeiten getroffen zu haben, um Arbeitsplatzrechner, Datenträger und NAS-Laufwerke zu schützen:

1. Maßnahmen zur Sicherung der Vertraulichkeit

a) Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren.

Beschreibung des Zutrittskontrollsystems:

- Chipkartenleser, kontrollierte Schlüsselvergabe
- Protokollierung der Zugänge
- Türsicherung (elektronischer Türöffner, etc.)
- Überwachungseinrichtung (Alarmanlagen, Video)
- Gesicherte Aktenschränke

b) Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Beschreibung des Zugangskontrollsystems:

- Kennwortverfahren, d.h. persönlicher und individueller User Log-In bei Anmeldung am System (u.a. Sonderzeichen, Mindestlänge)
- Einrichtung eines Benutzerstammsatzes pro User
- Begrenzung der Zahl der berechtigten Mitarbeiter
- Verschlüsselung von Datenträgern
- Abkapselung von sensiblen Systemen durch getrennte Nutzerkreise
- Authentifizierungsverfahren
- Einrichten von regelmäßigen aktualisierten Antiviren- und Spywarefiltern

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

- Berechtigungskonzepte (Profile, Rollen, etc.) und deren Dokumentation

- Verschlüsselung von unterschiedlichen Datenträgern
- Archivierungskonzept
- Protokollierung von Missbrauchsversuchen

d) Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Berechtigungskonzepte
- verschlüsselte Speicherung von personenbezogenen Daten
- Softwareseitige Kundentrennung
- Trennung von Test- und Produktivsystemen

e) Pseudonymisierung

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung des Pseudonymisierungsverfahrens:

- Hashwertverfahren (SHA-2; SHA-3)
- Zufällig generierte QR-Code-Inhalte
- Kundeneigene Pseudonyme statt Klartext-Informationen im Produktivsystem

2. Maßnahmen zur Sicherung der Integrität

a) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Beschreibung der Weitergabekontrolle:

- Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen
- Verschlüsselungsverfahren die Datenveränderungen während des Transports aufdecken
- sicherer Transportbehälter für Datenträger
- umfassende Protokollierungsverfahren

b) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Beschreibung des Eingabekontrollvorgangs:

- Protokollierung der Systemaktivitäten
- Protokollauswertungssysteme
- Archivierungssysteme

3. Maßnahmen zur Sicherung der Verfügbarkeit und Belastbarkeit

a) Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beschreibung des Verfügbarkeitskontrollsystems:

- Datensicherungsverfahren
- Spiegeln von Festplatten
- Brandmeldeanlage
- Alarmanlage
- Notfallplan

b) rasche Widerherstellbarkeit

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen:

- Datensicherungsverfahren
- regelmäßige Tests der Datenwiederherstellung

4. Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

Maßnahmen, die die datenschutzkonforme und sichere Verarbeitung sicherstellen.

Beschreibung der Überprüfungsverfahren:

- Datenschutzmanagement
- Formalisierte Prozesse für Datenschutzvorfälle
- Weisungen des Auftraggebers werden dokumentiert
- formalisiertes Auftragsmanagement