Datenschutz- und Datensicherheitskonzept – Technische und organisatorische Maßnahmen (TOM)

HCV Data Management GmbH
Am Eichelgarten 1
D-65396 Walluf

vorgelegt von
atarax
Dr.-Dassler-Str. 57
D-91074 Herzogenaurach

Bearbeiter:
Carolin Keller, Norbert Rauch

Version 1.0
24.05.2018

1. Vorwort

Das Dokument beschreibt die als verbindlich festgelegten technischen und organisatorischen Maßnahmen im Zusammenhang mit durchgeführten Auftragsverarbeitungsvorgängen zwischen Verantwortlichem/Auftraggeber und Auftragsverarbeiter/Auftragnehmer. Die dargestellten Maßnahmen stellen somit ein Abbild des gelebten Datenschutz- und Datensicherheitskonzept der HCV Data Management GmbH dar.

1.1. Geltungsbereich

Die beschriebenen technischen und organisatorischen Maßnahmen gelten für die HCV Data Management GmbH.

1.2. Dokumentenhistorie

Version	Datum	Bearbeiter	Kapitel	Änderung
1.0	24.05.2018	Carolin Keller, Norbert Rauch	6	Erstellung

2. Datenschutz- und Datensicherheitskonzept

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung zu treffenden technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 EU-DS-GVO.

Die EU-DS-GVO verpflichtet Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu anonymisieren oder zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen.

Diese Anforderungen erfüllt der Auftragnehmer durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Insbesondere die Schutzwerte: Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit.

Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- **Vertraulichkeit:**
  Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.

- **Integrität:**
  Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.

- **Verfügbarkeit:**
  Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.

- **Belastbarkeit:**
  Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst Widerstandsfähig ausgestaltet sein müssen.

3. Vertraulichkeit

Geeignete technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit werden, unter Berücksichtigung des Stands der Technik, der Art, des Umfangs, der Umstände, der Zwecke der Verarbeitung, der Implementierungskosten und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen getroffen. Hiermit wird ein dem Risiko angemessenes Schutzniveau gewährleistet.

3.1. Zutrittskontrolle

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

3.1.1. Objektsicherung

- Gebäudekomplex ist mit Einbruchmeldesystem u.a. Alarmanlage gesichert
- Rechenzentrum ist eigener abgesicherter Bereich
- Zugänge zu Stockwerken und Außentüren sind gesichert
- Außentüren, Stockwerkszugangstüren werden mit einem Schließsystem gesichert
- Schächte (Klimaanlage, Umluftanlage, Aufzug usw.) sind gesichert
- Fenstersicherung im Erdgeschoss
- Kameraüberwachung

3.1.2. Sicherheitszonen

- Rechenzentrum ist getrennter Bereich mit strikter Zutrittsbeschränkung und Überwachung
- Rechenzentrum wird als Closed-Shop betrieben
- Zutritte zum Rechenzentrum werden protokolliert
- Weitere Sicherheitszonen mit restriktiven Zutrittsberechtigungen sind definiert
- Sicherheitszonen sind durch getrennte Schließsysteme abgegrenzt

3.1.3. Art der Zutrittskontrolle
- Türsicherungen sind verbaut
- Schlüsselregelung getroffen
- Ausgabe unter Wahrung des 4-Augen-Prinzips
- Während der Kernzeiten ist der Empfang besetzt und empfängt Besucher
- Anweisungen für das Verschließen von Bürotüren und Fenstern
- Kontrollgänge nach Ende der Bürozeiten

3.1.4. Regelung der Zutrittsberechtigungen
- Zutrittsberechtigungen sind restriktiv ausgestaltet
- Zutrittsregelungen für bestimmte Personengruppen (Mitarbeiter, Führungskräfte, Firmenfremde, Besucher, Wartungs-, Reinigungspersonal, Lieferanten, Boten usw.)
- Festlegung befugter Personen mit Bezug auf Sicherheitszonen (z. B. Rechenzentrum)
- Besucher müssen sich am Empfang anmelden und werden abgeholt und begleitet
- Regelungen für das Ausscheiden von Mitarbeitern oder den internen Stellen- bzw. Berechtigungswechsel
- Regelungen / Folgemaßnahmen bei Verlust von Ausweisen, Schlüsseln usw.
- Aufsicht des Wartungs-, Reparatur- und Reinigungspersonals im Rechenzentrum

3.1.5. Alarmanlage/Videoüberwachung
- Scharfschaltung erfolgt automatisch und läuft außerhalb der Geschäftszeiten
- Bei betreten der Überwachungszonen außerhalb der Kernzeiten Alarmmeldung bei Wachdienst
- Bei betreten der Überwachungszonen außerhalb der Kernzeiten lösen Aktivitäten Aufzeichnung aus
- Aufzeichnungen werden 4 Monate gespeichert
- Meldelinien für Sabotagealarm, Fehlfunktion, etc. standardmäßig vorhanden
- Wartungsvertrag

3.2. Zugangskontrolle
Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

3.2.1. Regelung der Zugangsberechtigungen
- Fixierte Regelungen für die Vergabe von Zugangsberechtigungen getroffen
- Vergabe nach dem 4-Augen- und dem Need-to-know-Prinzip
- Zutrittsberechtigte weisen sich durch Benutzernamen und Passwort aus
- Regelungen für die Verwendung von Passwörtern, deren Länge, Komplexität und Aufbewahrung
- Regelungen für Fälle von Verlust oder Kompromittierung der Passwörter etabliert
- Vertretungsregelungen definiert und berechtigungskonform ausgestaltet
- Passwörter von Administratoren unterliegen höheren Anforderungen an Komplexität
- Administratoren-Konten werden ausschließlich für eng begrenzte Tätigkeiten genutzt
- Regelungen für das Ausscheiden bzw. den Stellenwechsel von Berechtigten
- Getrennte Infrastruktur für Besucher
- Trennung der Verbindung bei wiederholten Fehlversuchen oder Zeitüberschreitungen
- Regelungen zum Deaktivieren nicht genutzter Accounts

3.2.2. Zusätzliche Maßnahmen beim Fernzugang
- Regelungen für die Benutzung des Anschlusses, insbesondere bei Benutzung durch Dritte
- Personen die zur Anmeldung von außerhalb befugt sind, werden festgelegt
- Netzzugangssicherung durch Hard- und Softwaremaßnahmen
- Unberechtigter Zugriff aus dem Internet wird durch den Einsatz von Firewalls verhindert
- Regelungen bei Fernadministration und Fernwartung (Fernwartungskonzept, allgemeine Technikerrichtlinie)

3.2.3. Protokollierung von Zugängen
- Benutzung der Datenverarbeitungssysteme nachweisbar (Protokollierung der Zugänge)
- Protokollierung der Remotezugänge am (SSL) VPN-Gateway; (Handhabung über Bechtle, etoken)
- Protokollierung der Vergabe / Änderung von Zugangsberechtigungen
- Protokollierung fehlgeschlagener Zugangsversuche
- Regelmäßige Überprüfung der Protokolle auf sicherheitsrelevante Aktionen oder Vorgänge

3.3. Zugriffskontrolle / Benutzerkontrolle

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

3.3.1. Berechtigungskonzept

- Individuelle Zugriffsrechte, Benutzergruppen gebildet
- Regelungen für Vergabe und die Verwaltung von Zugriffsberechtigungen
- Regelungen für Dateihaltung organisatorischer Dokumente (z. B. Verfallsdatum, Aufbewahrungsfristen)
- Verwaltung der Benutzergruppen erfolgt in einem zentralen Verzeichnisdienst
- Vergebene Berechtigungen werden regelmäßig überprüft

3.3.2. Zugriffsschutz

- Einsatz von Verschlüsselungsroutinen, sowie die Möglichkeit zur Dateiverschlüsselung (speziell auch bei Passwortdateien) ist gegeben
- Verschlüsselung von mobilen Endgeräten
- Netzzugriffssicherungen eingerichtet
- Verwendung nur freigegebener Hard- und Software
- Netzkomponenten sind gesichert
- Netzwerk segmentiert
- Trennung von Test und Produktivumgebung
- Kritische Dienste unterliegen einem Monitoring
- Beschränkung der freien Abfragemöglichkeiten (SQL-Query) von Datenbanken
- Sichere Löschung von Informationen

3.3.3. Aufbewahrung bei Verwendung von Datenträgern

- Aufbewahrung von Datenträgern ist geregelt (sichere Orte)
- Festlegung der zur Datenträgerentnahme befugten Personen (Schlüsselverwaltung)
- Verschlüsselte Datenträger stehen zur Verfügung
- Festlegung der zur Datenträgerentnahme befugten Personen
- Sichere Löschung/Vernichtung von Datenträgern ist

3.3.4. Protokollierung von Zugriffen

- Protokollierung von Netzzugriffen
- Protokolle unterliegen definierter Auswertung

3.4. Trennungskontrolle

Es ist zu gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.

Maßnahmen

- Eingesetzte Software und Ablagestruktur ist mandantenfähig
- Logische Trennung der Daten
- Trennung von Test- und Produktivdaten; Produktivdaten werden nicht für Tests verwendet
- Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet
- Dokumentation der Trennung der Datenverarbeitungen (Mandantenfähigkeit, Buchungskreistrennung, etc.)

3.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne weitere Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen den entsprechenden technischen und organisatorischen Maßnahmen.

Maßnahmen

Pseudonymisierungen werden vom Auftragnehmer weisungsgebunden im Einzelfall realisiert.

4. Integrität

Die Richtigkeit der verarbeiteten personenbezogenen Daten ist zu gewährleisten. Unzulässige Änderungen müssen identifiziert und korrigiert werden können.

4.1. Weitergabekontrolle / Übertragungskontrolle
Es darf kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich sein.

4.1.1. Regelung der elektronischen Übertragung
- Festlegung der Stellen (Dritte), an die Daten übermittelt werden dürfen
- Möglichkeit Daten verschlüsselt zu übertragen (z. B. SSL, S-MIME, PGP)

4.1.2. Regelung bei der Speicherung auf Wechseldatenträgern
Eine Speicherung von personenbezogenen Daten auf Wechseldatenträgern ist grundsätzlich nicht vorgesehen. Im Ausnahmefall werden ausschließlich verschlüsselte mobile Datenträger verwendet.

4.1.3. Regelungen des Transports von Datenträgern
- Transport von Datenträgern mit personenbezogenen Daten ausschließlich durch betriebszugehörige Boten, gesicherte Transportverhältnisse oder eine sonstige sichere Versandform
- Datenträger sind stets verschlüsselt

4.2. Eingabekontrolle / Datenträgerkontrolle / Speicherkontrolle
Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:
- Zuständigkeiten für Dateneingabe, einschließlich Vertretungsregelungen sind durch Berechtigungsvergabe festgelegt
- Protokollierung aller Eingaben, Veränderungen oder Löschungen personenbezogener Daten werden

5. Verfügbarkeit und Belastbarkeit / Wiederherstellbarkeit
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust abgesichert sind.

5.1. Erstellung und Verwahrung von Sicherheitskopien
- Dokumentiertes Datensicherungskonzept
- Kontrollierte und regelmäßige Sicherung der Dateien und Datenbanken
- Protokollierung der Datensicherungen
- Tests der Datensicherung werden regelmäßig durchgeführt und dokumentiert
- Namenskonventionen für Sicherungsdateien
- Kennzeichnung der Datensicherungsträger
- Schreibschutz für Datensicherungsträger
- Datensicherung ist geschützt vor unberechtigten Zutritt, Zugang und Zugriff
- Datensicherungsträger werden sicher an besonders geschützten Orten gelagert

5.2. Gewährleistung des laufenden Betriebes
Der laufende Betrieb ist durch technische und organisatorische Maßnahmen sichergestellt.

5.2.1. Unterbrechungsfreie Stromversorgung (UPS)
- Unterbrechungsfreie Stromversorgung ist Rechenzentrum vorgeschaltet
- Ordnungsgemäße Funktionsfähigkeit wird durch regelmäßige Tests sichergestellt
- Dokumentation der Tests
- Wartungsvertrag abgeschlossen

5.2.2. Brandschutz
- Benachrichtigung der verantwortlichen Mitarbeiter bei Auslösung
- Optische und akustische Meldung im Rechenzentrum bei Auslösung
- Handlöscher im Rechenzentrum vorhanden
- Auf Brandlastreduzierung wird geachtet

5.2.3. Klimatisierung
- Zwei getrennte Klimatisierungssysteme mit getrennten Leitungswegen
- Benachrichtigung der verantwortlichen Mitarbeiter bei Auslösung
- Temperaturüberwachung an mehreren Messpunkten mit Einbindung in das Operating und Störungsmanagement
- Wartungsvertrag vorhanden

5.2.4. Anbindung Internet
- Redundante Internetanbindung mit getrennter Wegeführung und getrennter Hauseinführung
- Anbindung über unterschiedliche Provider

5.3. Maßnahmen zum betrieblichen Katastrophenschutz
- Notfallplan (inkl. Zuständigkeiten, Wiederanlaufkonzept und Rufbereitschaften) vorhanden
- Notfallhandbuch (mit Zuständigkeiten) erstellt und gepflegt
- Notfallorganisation ist etabliert
- Brandschutzmaßnahmen
- Schutz vor Wassereinbruch

5.4. Organisatorische Maßnahmen
- Datenschutzrichtlinien sowie sicherheitsspezifische Arbeitsanweisungen existieren, wurden verkündet und werden kontrolliert
- Geordnetes Change-Management
- Vorgaben für Verfahrens- und Programmdokumentation
- Vorhandensein ausreichender Personalressourcen
- Eingesetzte Hard- und Software wird regelmäßig überprüft
- Anwender werden geschult
- Bestellung eines IT-Sicherheitsbeauftragten
- Organisatorische Regelungen zur Datenträgeraufbewahrung (Kennzeichnung, Aufbewahrungsfristen)

6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

6.1. Datenschutz-Management
Die umfangreichen Pflichten und Anforderungen der EU-DS-GVO erfordern eine ganzheitliche Strategie nach einem strukturierten Ansatz und ein entsprechendes Managementsystem. Alle Elemente, die für die Sicherstellung des Datenschutzes erforderlich sind, unterliegen der systematischen Koordination des Datenschutz-Managements.

Maßnahmen
- Datenschutzorganisation etabliert
- Über Datenschutzstrategie wird ein strukturierter Ansatz verfolgt
- Etablierte Prozesse sehen die Einbindung des Datenschutzbeauftragten vor
- Datenschutzrelevante Richtlinien und Arbeitsanweisungen werden verkündet und die Einhaltung kontrolliert
- Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren

6.2. Incident-Response-Management
Um im Bedarfsfall eines Vorfalls reagieren zu können, sind einschlägige Meldewege zu definieren und Verantwortlichkeiten festzulegen.

Maßnahmen
- Mitarbeiter sind entsprechend geschult
- Meldestellen und Meldewege für Vorfälle- und Sicherheitsvorfälle sind definiert
- Geordnete Behandlung ist sichergestellt
- Dokumentation wird gepflegt

6.3. Datenschutzfreundliche Voreinstellungen
Durch Voreinstellungen ist sicherzustellen, dass personenbezogene Daten nur nach den jeweiligen bestimmten Verarbeitungszweck verarbeitet werden. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Speicherfrist und die Zugänglichkeit).

Maßnahmen
- Für sensible Bereiche stehen eigene Drucker zur Verfügung
- Durch kontinuierlichen Sensibilisierungs- und Schulungsprozess im Rahmen des Datenschutzmanagements sind die Mitarbeiter behutsam im Umgang mit personenbezogenen Daten

6.4. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Es erfolgt keine Auftragsverarbeitung im Sinne von Art. 28 EU-DS-GVO ohne entsprechende Weisung des Auftraggebers.

Maßnahmen
- Interner Prozess stellt sicher, dass notwendige Verträge zur Auftragsdatenverarbeitung abgeschlossen werden
- Schriftlicher Vertrag zwischen Auftraggeber und Auftragnehmer
- Auftraggeber erteilt Auftragnehmer Weisungen in Schriftform
- Auftragnehmer hat ausreichende betriebsinterne Anweisungen aufgrund des Auftrags und der damit verbundenen Weisungen des Auftraggebers
- Ausreichende Maßnahmen zur Einhaltung des Datenschutzes durch einen möglichen Unterauftragnehmer können auch durch den Auftraggeber geprüft werden
- Wenn beim Auftragnehmer eine Prüfung durch die Aufsichtsbehörde stattgefunden hat, so kann der Auftraggeber den Prüfbericht verlangen; Gleiches gilt für Prüfungen bei möglichen Unterauftragnehmern