Aufstellung für Auftraggeber der medicomp Gesellschaft für neue Medien und Computer mbH zu den bei der medicomp Gesellschaft für neue Medien und Computer mbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz gem. Art 32 DSGVO

Diese Auflistung der bei der medicomp Gesellschaft für neue Medien und Computer mbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz (TOMs) orientiert sich an den Vorgaben des § 9 BDSG (alt) und der Anlage zu § 9 Satz 1 BDSG (alt), diese Dokumentation ermöglicht eine strukturierte Dokumentation der TOMs, da es weder in der EU-Datenschutzgrundverordnung (DSGVO) noch im neuen Bundesdatenschutzgesetz (BDSG-Neu) dazu Vorgaben für nicht öffentliche Stellen gibt (§ 64 BDSG-Neu findet bei nicht öffentlichen Stellen keine Anwendung). Diese Angaben dokumentieren auch die Forderungen des Art. 32 der DSGVO und § 78a SGB X. Es soll Verantwortlichen (Auftraggebern) dazu dienen, ihren Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Art. 28 und 29 DSGVO und 80 SGB X zu erleichtern.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Art. 28, 29 DSGVO konformen, Dienstleistungsvertrag gedacht und kann jedem Verantwortlichen (Auftraggeber) auf Anforderung zur Verfügung gestellt werden. Die getroffenen Maßnahmen unterliegen den technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhanden Sicherheitsniveau nicht unterschritten wird.

Die Daten, die bei der medicomp Gesellschaft für neue Medien und Computer mbH im Auftrag verarbeitet werden, sind als besonders sensibel eingestuft. Es handelt sich um personenbezogene Daten gemäß Art. 4 Nr. 1 und um Sozialdaten gemäß § 67 Abs. 1 SGB X in Verbindung mit besonderen Daten gemäß Art. 4 Nr. 15 DSGVO (Gesundheitsdaten).

Ergänzend sei noch erwähnt, dass es bei der medicomp Gesellschaft für neue Medien und Computer mbH IT-Notfallpläne, Datensicherungs- und Berechtigungs-konzepte und dokumentierte Prozessabläufe gibt.

Allgemeiner Teil:

Name und Anschrift des Unternehmens:

medicomp Gesellschaft für neue Medien und Computer mbH
Hoheloogstr. 14
67065 Ludwigshafen am Rhein

Ansprechpartner mit Telefon, Fax und E-Mail:

Herr Gerhard Greiner, Geschäftsführer
Tel.: +49 621 6717820
Fax: +49 621 67178295
E-Mail: gerhard.greiner@medicomp.de

Name der Geschäftsführer:

Wolfgang Schunck
Gerhard Greiner
Angelo Mauceri

Name und Kontaktdaten der Datenschutzbeauftragten:

Joachim Kramer

Kramer Datenschutz OHG
Elsternweg 24
42555 Velbert
Tel.: +49 2052 / 92897 -66
Fax: +49 2052 / 92897 -67
E-Mail: j.kramer@datenschutz-kramer.de

Datenschutzbeauftragter:

Bestellung:

- *externe Datenschutzbeauftragte gem. Art.37 DSGVO und § 38 BDSG-Neu*
- *schriftliche Bestellung vom 24.02.2018 liegt vor*

Qualifikation:

- *Datenschutz-Auditor (TÜV) Zertifizierungsstelle für Personal TAR-ZERT der TÜV Akademie Rheinland Nr. 19553*
- *regelmäßige Fortbildungen*
- *Mitglied im Erfa-MEO für Datenschutzbeauftragte*
- *GDD Mitglied*
- *Firma Kramer & Partner besitzt über 30 Jahre Erfahrung im Datenschutz*

Mitarbeiter der medicomp Gesellschaft für neue Medien und Computer mbH:

- *alle Mitarbeiter sind schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht nach § 203 StGB, der Vertraulichkeit nach DSGVO, BDSG-Neu und auf das Sozialgeheimnis nach § 35SGB I verpflichtet worden*
- *die Verpflichtung erfolgte auf einem extra Formular*
- *die der Verpflichtung zugrundeliegenden Gesetzestexte wurden allen Mitarbeitern gegen Unterschrift ausgehändigt*
- *die Verpflichtung wird bei Einstellung durch Herrn Gerhard Greiner vorgenommen*
- *Arbeitsanweisungen über die private Nutzung von E-Mail, Internet und Telefon*
- *alle Mitarbeiter werden in regelmäßigen Abständen durch den bDSB geschult*

Verzeichnis der Verarbeitungstätigkeiten:

- *das „Verzeichnis der Verarbeitungstätigkeiten“ liegt vor*

Anlage zum Vertrag Auftragsverarbeitung:
Technische und organisatorische Maßnahmen

Präambel
Die in dieser Anlage aufgeführten technischen und organisatorischen Maßnahmen werden allgemein aufgeführt. Es versteht sich von selbst, dass die Firma medicomp GmbH entsprechende detaillierte Maßnahmen ergreift die Daten des Auftraggebers im Rahmen des Hauptauftrages sowie des Vertrages zur Auftragsverarbeitung besonders sorgfältig durch geeignete Maßnahmen zu schützen. Hierzu zählt insbesondere, dass wir in dieser Anlage nicht alle Details in der Form offenlegen, da diese sicherheitsrelevant sind. Die Firma medicomp GmbH hält detaillierte technische und organisatorische Maßnahmen bereit und wird diese im Rahmen von Audits, Prüfungen und Zertifizierungen den entsprechenden Institutionen zur Verfügung stellen.

Vertraulichkeit (Art. 32 Abs. 1b DSGVO)

In unserem Haus ist die räumliche **Zutrittskontrolle** folgendermaßen sichergestellt:

Die Gebäude der medicomp sind an den systemkritischen Punkten über Zutrittskontrollfunktionen nur den autorisierten Personen zugänglich. Es sind Schlüssellisten und Schlüsselquittungen vorhanden.

Eingangsbereiche und Fenster sind außerhalb der Geschäftszeiten fest verschlossen und zusätzlich gesichert. Sowohl die Rechenzentren, als auch das Unternehmen ist durch eine Alarmanlage gesichert.

Der Serverraum im Unternehmen ist durch eine elektronische Zugangskontrolle gesichert. Es findet sowohl im Unternehmen als auch in den Rechenzentren eine Protokollierung der Zugänge statt.

Unter Berücksichtigung der geltenden Besucherregelung der medicomp können sich Besucher, Gäste und Schulungsteilnehmer nur im Bereich des baulich getrennten medicomp Schulungszentrums frei bewegen. Der Zutritt zu den Büros ist nur in Begleitung von Mitarbeitern von medicomp gestattet. Der Zutritt zu dem Serverraum und den Rechenzentren ist diesem Personenkreis untersagt.

Der Zutritt zu den Rechenzentren unserer Serverfarmen ist durch elektronische Zugangskontrollen, bestehend aus Zutrittskarte und Code, sowie individuellen Angaben für den Zugang durch die Personenvereinzelungsanlage gesichert, und ist sowohl zeitlich als auch personell genau festgelegt.

Der Zutritt ist nur solchen Mitarbeitern gestattet, deren Aufgabengebiet sich auf die Betreuung des Rechenzentrumsbetriebes erstreckt. Nur diesen Mitarbeitern wird der Zutritt nach vorheriger Anmeldung freigeschaltet.

Die Rechenzentren werden zudem von einem Sicherheitsdienst per Video überwacht. Jeder Zugang wird registriert.

Die Rechenzentren unserer Serverfarmen sind zudem örtlich vom Unternehmen getrennt. Ein Zugang zum Unternehmen führt somit nicht automatisch zu einem Zugang zu den Rechenzentren.

Um das unbefugte Eindringen in unsere Systeme und Datenverarbeitungssysteme zu verhindern, verwenden wir folgende **Zugangskontrollen**:

Alle Systeme der medicomp werden ständig aktualisiert und regelmäßig gesichert. Systeme zur Datenverarbeitung unterliegen nochmals besonderen Sicherheitsmechanismen und werden entsprechend protokolliert, um bei Bedarf entsprechende Auswertungen vornehmen zu können.

Die Netzwerke der medicomp sind sowohl im Unternehmen, als auch in den Rechenzentren gegen externe Zugriffe durch ein mehrstufiges Firewall-System abgeschirmt. Aus fremden Netzen kann und darf nur unter bestimmten Voraussetzungen zugegriffen werden.

Server, die eine Verbindung zum Internet haben befinden sich in einer DMZ und werden ständig überwacht mit entsprechender Protokollierung von Ereignissen.

Alle Server sind nur über Useranmeldung mit persönlichem Passwort zugänglich. Die Anmeldungen werden protokolliert und können im Bedarfsfall ausgewertet werden.

Ein externer Zugriff auf die Datenbankserver, die für die Speicherung der sensiblen Daten verwendet werden, ist durch entsprechende Zugangsberechtigungen, das mehrstufige Firewall-System und die anwendungsbezogene Segmentierung der Netzwerke ausgeschlossen.

Die Datenbankserver werden von der EDV-Leitung und dem Administrator betreut und sind durch eine Benutzerkennung und ein Kennwort geschützt.

Kennwörter werden ausschließlich durch den Benutzer erstellt und müssen den definierten Kennwortrichtlinien der medicomp entsprechen.

Wie wird der Zugriff (**Zugriffkontrolle**) auf verschiedene Daten bzw. Systeme geregelt:

Jeder Nutzer unserer Anwendungen besitzt eigene Zugangsdaten bestehend aus einer Benutzerkennung und einem persönlichen Kennwort. Die Kennwörter und die Benutzerdaten werden verschlüsselt gespeichert. Ein Zugriff auf das Kennwort ist nur dem Benutzer selbst möglich. Interne Zugriffe innerhalb unserer Anwendungen sind durch die eindeutigen Zugangsdaten ebenfalls kontrollierbar. Die Nutzer können lediglich auftragsbezogene Daten einsehen. Die Einsicht ist nur über die für den Nutzer zugänglichen Anwendungen möglich. Das Rollenkonzept unserer Anwendungen gestattet eine abgestufte Zugangsberechtigung zu den Daten.

Sämtliche Zugriffe, sowohl lesend als auch schreibend, werden protokolliert. Auffällige Zugriffe werden automatisiert von Überwachungssystemen an berechtigte Mitarbeiter der medicomp gemeldet und können bei Bedarf ausgewertet werden.

Sämtliche Zugriffe auf die Datenverarbeitungssysteme sind ebenfalls über Zugangsdaten geschützt. Mitarbeiter verfügen lediglich über die Zugangsdaten, die für die jeweilige Aufgabenbewältigung erforderlich sind.

Es ist verboten, Kennwörter an andere Personen weiter zu geben.

Innerhalb der medicomp werden die Zugriffsmöglichkeiten auf das "Need to Know"-Prinzip beschränkt.

Es finden regelmäßig Schulungen zum Datenschutz und zur Datensicherheit statt.

Um Daten, die zu unterschiedlichen Zwecken erhoben wurden oder um die Daten von Mandanten voneinander zu trennen (**Trennungskontrolle**), haben wir folgende Maßnahmen ergriffen:

Unserer Anwendungen verarbeiten ausschließlich Daten, die für die Anwendung erforderlich sind. Es werden keine zu unterschiedlichen Zwecken erhobenen Daten verknüpft und verwendet.

Die Datenspeicherung erfolgt für die verschiedenen Kunden auf vollständig getrennten Datenbanken und somit logisch getrennt.

Integrität (Art. 32 Abs. 1b DSGVO)

Wir kontrollieren die Weitergabe (**Weitergabekontrolle**) personenbezogener Daten bei Übermittlung bzw. Übertragung oder bei Transport mit folgenden Maßnahmen:

Personenbezogene Daten werden im Online Verfahren ausschließlich über VPN-Verbindungen bzw. über SSL/TLS verschlüsselte Verbindungen übertragen.

Im Einsatz findet grundsätzlich kein Transport der Daten statt. Lediglich bei der Erstellung externen Datensicherungen werden zusätzliche Datenträger von den Rechenzentren in die Bank transportiert und im Tresor eingelagert. Der Transport der externen Datensicherungen wird nur von dazu autorisierten Personen durchgeführt. Die für den Transport verwendeten Datenträger sind hardwareseitig verschlüsselt.

Für ausgehende Übermittlungen werden der Empfänger und die Art der übermittelten Daten festgehalten. Eingehende Übermittlungen entsprechen Eingaben in unseren Anwendungen und sind dadurch bereits durch die Anwendung festgehalten und protokolliert. In den Zugriffsprotokollen ist zudem auch erkennbar, welche Daten zu welchem Zeitpunkt an Anwender übertragen wurden.

Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind schriftlich zur Verschwiegenheit verpflichtet.

Nicht mehr benötigte Daten in Papierform bzw. nicht mehr gebrauchte oder defekte Datenträger, werden bei uns wie folgt entsorgt:

Daten in Papierform werden mit einem Aktenvernichter nach DIN 66399 P4 datenschutzgerecht entsorgt. Elektronische und optische Datenträger werden gesammelt und durch die IT-Administration nach DIN 66399 O3 T4 H4 entsorgt (quittiert).

Wir gewähren die Nachvollziehbarkeit bzw. Dokumentation der Wartungsarbeiten bzw. Systemzugriffe mit folgenden Maßnahmen (**Eingabekontrolle**). Dadurch kann nachvollzogen werden, wer auf ein System bzw. Daten zugegriffen hat und wann:

Um Datenmanipulationen und Dateneinsichten im Bedarfsfall nachvollziehen zu können, werden sämtliche Datenzugriffe auf Sozialdaten protokolliert. Dabei werden Anwender, Zeitpunkt und Ort gespeichert. Die Protokolle werden auf den Datenbankservern direkt aufbewahrt und werden regelmäßig mitgesichert. Der Zugriff auf die Protokolle ist nur den Mitarbeitern gewährt, die auch Zugriff auf die Datenbankserver haben und somit autorisiert sind. Die Protokolldaten sind im direkten Zugriff maximal 12 Monate verfügbar.

Die Aufträge (**Auftragskontrolle**) unserer Kunden kontrollieren wir anhand folgender Möglichkeiten:

Es ist sichergestellt, dass die gespeicherten Daten, die in unseren Anwendungen verarbeitet werden, auch im Bezug zum Auftrag stehen. Der genaue Auftrag ist in der Vereinbarung zur Auftragsverarbeitung gem. Art. 28 und 29 DSGVO sowie § 80 SGB X definiert. Eine interne Qualitätssicherung findet regelmäßig statt.

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

Folgende Sicherheitsmaßnahmen (**Verfügbarkeitskontrolle**) haben wir gegen zufällige oder mutwillige Zerstörung und gegen Verlust bzw. Sabotage von Daten ergriffen:

Die Sicherheit der Daten und deren Verfügbarkeit wird durch ein mehrstufiges Backup- und Recovery-Konzept gewährleistet, sowie die redundante Auslegung aller Systeme und ihrer Komponenten.

Die Rechenzentren unserer Serverfarmen sind durch mehrstufige Notstromversorgungen und intelligente USV-Systeme gegen einen plötzlichen Ausfall der Stromversorgung geschützt.

Unserer Serverfarmen werden in zwei Rechenzentren an unterschiedlichen Standorten aktiv-aktiv betrieben. Sämtliche eingesetzte Hardware wie Server, SAN-Systeme, Switche etc. sind in jedem Rechenzentrum redundant vorhanden. Ein Totalausfall ist dadurch ausgeschlossen.

Es werden täglich automatisiert Sicherungskopien aller Daten in beiden Rechenzentren erstellt, um eine größtmögliche Verfügbarkeit im Rahmen der vereinbarten Leistungserbringung zu gewährleisten. Die Sicherungskopien werden derzeit maximal 12 Monate im Direktzugriff aufbewahrt. Ältere Sicherungen werden in ein Bankschließfach ausgelagert. Die Datenwiederherstellung bei Ausfällen erfolgt innerhalb von maximal 24 Stunden.

Die Backup-Server in jedem Rechenzentrum verfügen derzeit über eine Speicherkapazität die es ermöglicht, tägliche Sicherungskopien aller Daten maximal 12 Monate im Direktzugriff aufbewahren zu können. Die Speicherkapazität kann bei Bedarf unterbrechungsfrei vergrößert werden. Ein vollständiger Verlust der Daten ist ausgeschlossen.

Überprüfung, und Evaluierung der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1d DSGVO)

Folgende Maßnahmen treffen wir (**Organisationskontrolle**) um den Datenschutzanforderungen gerecht zu werden

Die Verarbeitung der sensiblen Daten erfolgt lediglich im Produktionsbetrieb.

Mitarbeitern ist der Zugriff auf die Daten grundsätzlich verweigert, sofern der Zugriff nicht für die Aufgabenbewältigung erforderlich ist.

Mitarbeiter werden regelmäßig zum Thema Datenschutz geschult. Durch den externen bDSB finden regelmäßige Kontrollen statt.

Unsere Auftraggeber prüfen regelmäßig die medicomp Gesellschaft für neue Medien und Computer mbH. Unsere Auftraggeber beauftragen unabhängige Prüfunternehmen mit der Prüfung. Die Prüfberichte liegen vor.

Velbert, 22.05.2018 

Joachim Kramer (betrieblicher Datenschutzbeauftragter)

Ludwigshafen, 23.05.2018 

Gerhard Greiner, Geschäftsführer