Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO („TOM“)

der

FIBU-doc Praxismanagement GmbH

Am Südhang 28

65510 Hünstetten

- nachstehend „FDPM“ genannt -

Stand 23. Februar 2019

Einleitung

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. FDPM ist sich über die besondere Verantwortung für die Daten ihrer Kunden bewusst und erfüllt diesen Anspruch durch folgende Maßnahmen (Gliederung richtet sich nach dem Aufbau des Art. 32 Abs. 1 DSGVO):

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

1.1 Zutrittskontrolle

1.1.1 Zutrittskontrolle am Firmensitz

Der unbefugte Zutritt zu den Firmenräumen wird u.a. dadurch verhindert, dass der Zutritt zu den Büros durch ein manuelles Schließsystem geregelt ist. Die Eingangstüren sind dabei auch tagsüber geschlossen und nur per Schlüssel zu öffnen (Knauf an der Türaußenseite). Alle Mitarbeiter sind per Dienstanweisung dazu angehalten, die Diensträume geschlossen zu halten und diese bei Verlassen zu verschließen. Die Schlüsselvergabe an die Mitarbeiter ist dokumentiert.

Der Zutritt von betriebsfremden Personen wird durch die Mitarbeiter kontrolliert. Besucher müssen klingeln und werden durch einen Mitarbeiter am Eingang in Empfang genommen. Innerhalb des Firmenbereichs werden die Besucher geführt. Dabei liegt es in der Verantwortung des empfangenden Mitarbeiters, die Besucher zu den jeweiligen Mitarbeitern zu führen. Jeder Mitarbeiter ist dann für seine Besucher verantwortlich. Alle Mitarbeiter sind per Dienstanweisung über dieses Vorgehen informiert.

Nebenausgänge, Fluchttüren und sonstige Notausgänge können von außen nicht geöffnet werden.

Der Server sowie die Netzwerktechnik ist in einem verschließbaren Kellerraum und einem verschließbaren Serverschrank untergebracht.

Die Auswahl des Reinigungspersonals erfolgt mit großer Sorgfalt. Das Reinigungspersonal verfügt nicht über eigene Schlüssel, sondern wird vor der Reinigung in die Räume gelassen und bei der Reinigung beaufsichtigt.

1.1.2 Zutrittskontrolle zu den Servern der Test- und Entwicklungsumgebungen

Der Zutritt zu Servern der Test- und Entwicklungsumgebungen wird durch die Firmen ito consult GmbH, Dresden (ito), und die Firma BuchhaltungsButler GmbH, Unterspreewald (BHB) kontrolliert, in deren Räumen die Test- und Entwicklungsumgebungen betrieben werden. Zwischen FDPM und ito bzw. BHB besteht jeweils ein Vertrag zur Verarbeitung von Daten im Auftrag, in dem ito bzw. BHB der FDPM ein adäquates Sicherheitsniveau zusagt, welches dem Sicherheitsniveau entspricht, das FDPM in den eigenen Räumen sicherstellt.

1.1.3 Zutrittskontrolle zu den Servern der Produktivumgebungen bei der Hetzner Online GmbH, Gunzenhausen (Hetzner) und Amazon Web Services EMEA SARL, Luxemburg (AWS)

Der Zutritt zu unseren Servern der Produktivumgebungen wird durch Hetzner und AWS kontrolliert. Die Server unserer Produktivumgebungen werden von ito in einem Hetzner Rechenzentrum in Falkenstein sowie von BHB in einem AWS Rechenzentrum in Frankfurt am Main betrieben. Für das Rechenzentrum von Hetzner liegt ein DIN ISO/IEC 27001 Zertifizierung vor. Für das Rechenzentrum und die Leistungen von AWS liegen Zertifizierungen nach DIN ISO/IEC 9001, 27001, 27017 und 27018 vor. Diese Zertifizierungen können auf den Websites von Hetzner und AWS eingesehen und heruntergeladen werden.

1.2 Zugangskontrolle

Zugang zu den Datenverarbeitungsanlagen erhalten ausschließlich berechtigte Personen. Die Zugangskontrolle verhindert, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können.

Die Server im Rechenzentrum werden ausschließlich von namentlich benannten Mitarbeitern der ito administriert und verfügen hierzu über entsprechende Benutzerkonten und IP-basierte Beschränkungen. Die Administration erfolgt über das Internet mittels verschlüsselter Verbindungen („Site-to-Site IPsec Tunnel“ mit AES 256-bit PFS Verschlüsselung). Mitarbeiter des Rechenzentrumbetreibers haben keinen Zugang zu Kundendaten oder der Datenverarbeitungssoftware. Um nicht autorisierten Zugang über das Internet zu verhindern sind die Server durch eine hardwarebasierte Firewall mit Web Applikation Firewall geschützt.

Der Zugang zu Rechnern in den Büroräumen der FDPM wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter auf seinem Rechner ein eigenes Benutzerkonto. Der Zugriff auf das bürointerne Netzwerk von außerhalb der Büroräume ist ausschließlich über eine VPN-Verbindung (Virtual Private Network) möglich, für die aktuell nur die Geschäftsleitung freigeschaltet ist. Das bürointerne Netzwerk wird ebenfalls von einer hardwarebasierten Firewall und einem „Intrusion Prevention & Detection System“ geschützt.

Der Zugang zu den Datenverarbeitungssystemen ist mit Benutzerkennung und einem sicheren Authentifizierungsverfahren geschützt. Benutzerkennungen können nur von der Geschäftsleitung verwaltet oder erstellt werden. Es sind Regeln zur Bildung sicherer Passwörter festgelegt und Passwörter dürfen nicht mehrfach verwendet werden. Zur Absicherung der Passwörter und um die Einhaltung der Regeln zur Bildung sicherer Passwörter zu unterstützen, verwenden die Mitarbeiter der FDPM eine Software für die Erstellung und verschlüsselte Aufbewahrung sicherer Passwörter.

Die Datenträger aller mobilen Einsatzgeräte (z.B. Laptops) der FDPM sind verschlüsselt. Auf allen Rechnern und Servern kommt Anti-Virus-Software sowie spezielle Software für „Endpoint Security“ zum Einsatz.

Eventuell physisch vorliegende personenbezogene Daten lagern in zusätzlich verschließbaren Schränken, zu denen nur berechtigte Personen Zugang haben. Das Reinigungspersonal hat dabei grundsätzlich nie Zugang zu den verschließbaren Schränken oder Serverschränken.

Alle Mitarbeiter sind bei längerer Abwesenheit per Dienstanweisung zu einem „clean desk“ verpflichtet.

1.3 Zugriffskontrolle

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

In den vom Auftragnehmer genutzten Datenverarbeitungssystemen sind Berechtigungsprofile hinterlegt, in denen die zugriffsberechtigten Personen festgelegt sind. Die Rechte werden in einem geregelten Verfahren vergeben, und die Notwendigkeit der bestehenden Rechte wird regelmäßig kontrolliert. Die Einrichtung und Freigabe werden dokumentiert.

FDPM hat die technischen und organisatorischen Maßnahmen getroffen, die sicherstellen, dass ausscheidenden Mitarbeitern sämtliche Unterlagen, Zugangsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht werden, um einen unberechtigten Zugriff auf die Daten des Auftraggebers zu verhindern.

Der Zugang zu Daten über Kunden für den Kundenservice ist auf folgende Daten beschränkt, sofern der Kunde dies nicht selbst in den Einstellungen aufgehoben hat: Praxis / Firma, Name, Vorname, Benutzername, E-

Mail-Adresse und Adresse des Kunden bzw. der Benutzer der Kundeninstanz, gebuchte Module und Anwendungen, letzter Login, letzte Datenaktualisierung / Import, Anzahl der Benutzer und Abrechnungsdaten.

Der Zugriff auf technischer Ebene auf Kundendaten, z.B. über die Datenbank des Kunden, ist ausschließlich eigens dafür benannten Mitarbeitern der FDPM und der ito möglich. In diesem Fall verwenden besagte Mitarbeiter jeweils eigene Benutzerkonten. Der Zugriff ist nur gestattet, wenn eine Supportaufgabe vorliegt, die nicht durch den Kunden oder den Support alleine gelöst werden kann und der Auftraggeber seine Einwilligung zum Zugriff erteilt hat. Diese wird im Ticketsystem protokolliert. Sollte die Aufgabe auch durch direkten Zugriff auf die Daten nicht lösbar sein, kann eine lokale Kopie der Daten z.B. für Debuggingzwecke erstellt und dem verantwortlichen Entwickler zugänglich gemacht werden. Nach Abschluss der Arbeiten werden lokale Kopien gelöscht.

Eventuell physisch vorliegende personenbezogene Daten werden nach Abschluss der Arbeiten mittels eines Aktenschredders (mind. Stufe 3) oder einen externen Aktenvernichter mit entsprechender Zertifizierung vernichtet. Alle Mitarbeiter sind hierzu per Dienstanweisung verpflichtet.

1.4 Trennungskontrolle

Daten die zu unterschiedlichen Zwecken erhoben werden, werden ausschließlich getrennt verarbeitet. Es werden Daten mehrerer Kunden und Anwendungen auf den gleichen Servern und Datenbanken verarbeitet. Die Trennung der Daten einzelner Kunden und Benutzer voneinander wird teilweise durch getrennte Datenbanken und immer auch durch getrennte Benutzerkonten mitentsprechenden Zugriffsrechten geregelt. Ein Zugriff auf die Datenbank und Daten eines bestimmten Kunden durch Benutzer eines anderen Kunden ist somit faktisch ausgeschlossen.

Test- und Produktivumgebung sind physisch getrennt auf unterschiedlichen Servern.

1.5 Pseudonymisierung / Anonymisierung (Art. 32 Abs. 1 lit. a, Art. 25 Abs. 1 DSGVO)

Werden Daten zu statistischen Zwecken verwendet, so sind alle Mitarbeiter per Dienstanweisung verpflichte, dies ausschließlich in aggregierter und / oder vollständig anonymisierter Form ohne Nennung des Auftraggebers zu tun. Alle personenbezogenen Daten werden ebenfalls im Falle einer Weitergabe oder beauftragten Löschung anonymisiert.

2. Integrität (Art. 32 Abs. 1 Ziff. b DSGVO)

2.1 Weitergabekontrolle

Die Weitergabekontrolle gewährleistet, 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.

Die Weitergabekontrolle wird durch verschiedene Maßnahmen gewährleistet. Zum einen werden Daten nicht außerhalb der Server am Firmensitz oder des Rechenzentrums gespeichert, mit Ausnahme der in diesen TOM genannten Speicherung für Debuggingzwecke. Die Mitarbeiter des Rechenzentrumbetreibers haben grundsätzlich keinen Zugriff oder Zugang zu den auf den Datenträgern gespeicherten Daten und können diese Daten weder lesen noch verändern.

Zum anderen werden Daten grundsätzlich nur über verschlüsselte Verbindungen zwischen dem Server und dem Client des Kunden außerhalb des Rechenzentrums übertragen. Hierbei kommt das SSL verschlüsselte HTTP Protokoll (HTTPS) zum Einsatz. Sollte für besondere Supportaufgaben eine Übertragung von Daten in die Büroräume der FDPM notwendig sein, findet diese durch FDPM ebenfalls ausschließlich verschlüsselt statt. Werden Daten für Sicherungszwecke auf einen anderen Server übertragen, so erfolgt dies ebenfalls ausschließlich verschlüsselt und / oder über Tunnelverbindungen.

Eine Übertragung außerhalb Deutschlands findet nur dann statt, wenn der Auftraggeber oder seine Mitarbeiter die Anwendungen der FDPM im Ausland verwendet.

Werden personenbezogene Daten per E-Mail versendet, so erfolgt dies ebenfalls ausschließlich verschlüsselter. Beim geplanten Empfang von personenbezogenen Daten werden die Versender ebenfalls gebeten dies in verschlüsselter Form vorzunehmen.

2.2 Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Die Eingabekontrolle wird dabei über getrennte Benutzerkonten und entsprechende Protokolleinträge und Serverprotokollierungen umgesetzt. Die Rechte der einzelnen Benutzerkonten für die Eingabe, Änderung und Löschung von Daten werden dabei auf Basis eines Berechtigungskonzeptes vergeben. Für die Löschung von Daten (sowie über die Erteilung von Weisungen hierüber) ist ausschließlich die Geschäftsleitung zuständig.

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

Die Verfügbarkeit und Funktion der für die Datenverarbeitung erforderlichen Systeme werden rund um die Uhr überwacht. Fehlfunktionen werden schnellstmöglich gemeldet und behoben.

Ein mehrstufiges Sicherheitskonzept stellt die Verfügbarkeit der Daten sicher. Alle physikalischen Datenträger (Festplatten) sind als RAID-Verbund ausfallsicher angelegt. Der Status der Datenträger wird laufend automatisch überwacht und defekte Festplatten werden unverzüglich ausgetauscht.

Zum anderen werden die Kundendaten regelmäßig auf physikalisch getrennten Servern (off-site) gesichert und gespeichert. Es existiert ein Notfallplan, um die Sicherungen bei Verlust oder Zerstörung der physikalischen Datenträger auf andere Datenträger zurückzuspielen.

Das verwendete Rechenzentrum bietet durch vollklimatisierte Sicherheitsräume, ein modernes Brandfrühesterkennungssystem mit direkter Verbindung zur örtlichen Feuerwehr, eine redundante USV-Anlagen, einen Notstromdiesel für autonomen Betrieb sowie multiredundante Netzanbindungen an wichtige Knotenpunkte sehr guten Schutz vor Schäden durch äußere Einflüsse und höchste Ausfallsicherheit. Ferner kommt ein spezielles, hardwarebasiertes System zur Abwehr von sogenannten DDoS-Angriffen zum Einsatz.

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

4.1 Datenschutzmanagement

FDPM ist sich seiner Verantwortung in Bezug auf Datenschutz sehr bewusst. Deshalb wird dem Datenschutzmanagement eine besondere Stellung in unserem Haus zuteil. Wir haben uns im Rahmen von Leitlinien und Anweisungen zu einem verantwortungsbewussten Umgang mit dem Thema Datenschutz verpflichtet. Für das Datenschutz-Management kommt ferner eine spezielle Software-Lösung zum Einsatz, in der die Leitlinien und Anweisungen sowie alle sonstigen Regelungen dokumentiert und regelmäßig überprüft werden.

Unsere Mitarbeiter sind durch Schulungen und andere Sensibilisierungsmaßnahmen umfassend mit dem Thema Datenschutz und den besonderen Anforderungen an die Verschwiegenheit nach § 203 StGB vertraut gemacht worden. Eine erneute Sensibilisierung und Schulung der Mitarbeiter erfolgt mindestens jährlich. Alle relevanten Dokumentationen, Verfahrensanweisungen und Regelungen zum Datenschutz sind den Mitarbeiter jederzeit über unseren Fileserver zugänglich.

Eine Überprüfung der Wirksamkeit der technischen und organisatorischen Schutzmaßnahmen wird mindestens jährlich durchgeführt.

Ein externer Datenschutzbeauftragter wurde bestellt. Die Kontaktdaten sind auf unserer Website leicht zugänglich einsehbar.

Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt.

4.2 Incident-Reponse-Management

Um die Wahrscheinlichkeit des Auftretens von Vorfällen mit Betriebsunterbrechung zu vermindern und uns gegen diese zu schützen, kommt eine Reihe von Maßnahmen zum Einsatz. Hierzu gehören hardwarebasierte Firewalls vor allen Netzwerken, ein SPAM-Filter für alle eingehenden E-Mails, die Verwendung von Virenscannern auf allen Rechnern und die Verwendung eines „Intrusion Prevention & Detection Systems". Alle genannten Systeme entsprechen dabei dem Stand der Technik, werden regelmäßig überprüft und ständig aktualisiert.

Es existiert ferner ein dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen und Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde). Alle Sicherheitsvorfälle und Datenpannen werden ferner dokumentiert, schnellstmöglich behoben und im Nachgang analysiert, um geeignete Maßnahmen zu ergreifen, die ein erneutes Vorkommen nach Möglichkeit verhindern. Alle Mitarbeiter, die mit der Entwicklung, der Bereitstellung und der Unterstützung unserer Anwendungen in Kontakt kommen, wurden geschult und haben sich mit ihren Aufgaben in diesem Zusammenhang vertraut gemacht.

4.3 Datenschutzfreundliche Voreinstellungen

Die Art der Daten, die vom Auftraggeber erfasst und verarbeitet werden, liegen rein in der Verantwortung des Auftraggebers. So hat der Auftraggeber das dem Verarbeitungsrisiko angemessene Schutzniveau zu ermitteln und die diesbezügliche Schutzbedarfsklassifizierung zu dokumentieren.

Die Voreinstellungen unserer Anwendungen unterstützen den Auftraggeber soweit es geht dabei, nach Möglichkeit nur solche personenbezogenen Daten zu verarbeitet, die für den jeweiligen Verarbeitungszweck erforderlich sind. Eine Verarbeitung von personenbezogenen Daten durch den Auftraggeber zu einem anderen als dem jeweils zulässigen Verarbeitungszweck können wir aber nicht vollständig verhindern.

Unsere Anwendungen unterstützen den Auftraggeber ferner dabei sicherzustellen, dass nur Personen Zugang zu personenbezogenen Daten haben, die hierzu berechtigt sind (z.B. mit dem Rollen- und Berechtigungssystem).

Soweit vorhanden, sind die Voreinstellungen unserer Anwendungen so eingestellt, dass personenbezogene Daten nur dem Auftraggeber bzw. einem möglichst kleinen Kreis an Anwendern beim Auftraggeber zugänglich sind.

4.4 Auftragskontrolle

Bei der Auswahl geeigneter Unterauftragsverarbeiter wird FDPM die gebotene Sorgfalt, gerade auch in Bezug auf Datenschutz und Datensicherheit, walten lassen. Vor Vergabe der Datenverarbeitung im Auftrag durch FDPM an Unterauftragsverarbeiter, stellt ferner FDPM sicher, dass beim Unterauftragsverarbeiter eine Kontrolle in Bezug auf die Einhaltung der Anforderungen nach Art. 28 DSGVO durch Auftraggeber und/oder FDPM durchgeführt werden kann. Diese Kontrolle stellt sicher, dass beim Unterauftragsverarbeiter die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen zur Sicherung des Datenschutzes nach Maßgabe dieser Vereinbarung eingerichtet sind.

Über jeden Unterauftrag wird ein Vertrag unter Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und der DSGVO abgeschlossen. Dies gilt insbesondere auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und über Softwarepflege sowie sonstige IT-Unterstützungsverträge, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Bei längerer Zusammenarbeit wird FDPM ferner laufend das Schutzniveau des Unterauftragsverarbeiter überprüfen.

Sonstige Angaben

Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich zu festzuhalten und dem Auftraggeber bekanntzugeben.