

## Datenschutzhinweise zum Einsatz von indicda medicalONE\*

Stand: September 2022

\*) indicda medicalONE ist eine Software zur Online-Spracherkennung, bereitgestellt als Dienst/Service/Anwendung über eine in Deutschland ansässige und durch DFC-SYSTEMS administrierte Rechenzentrums-Infrastruktur (RZI).

Für DFC-SYSTEMS hat der Schutz personenbezogener Daten seiner Kunden oberste Priorität. Daher verpflichtet sich DFC-SYSTEMS, alle deutschen und europäischen Vorschriften sowie die in der Bundesrepublik Deutschland geltenden Richtlinien und Verordnungen zum Schutz personenbezogener Daten einzuhalten.

Folgende Datenschutzrichtlinien zum Schutz von personenbezogenen Daten seiner Kunden werden von DFC-SYSTEMS kontinuierlich umgesetzt:

- Jeder Kunde verfügt alleinig über seine Daten. DFC-SYSTEMS kann diese Daten nur zu den im Folgenden aufgeführten Zwecken verarbeiten.
- Die Verarbeitung der Daten erfolgt ausschließlich in Deutschland, nachvollziehbar, vertraulich und nach hohen Sicherheitsstandards.
- DFC-SYSTEMS verpflichtet sich gemäß den Bestimmungen und Vorgaben der Europäischen Datenschutzgrundverordnung (EU DSGVO) zu einer kontinuierlichen Kontrolle und Verbesserung der bestehenden Datenschutz-Maßnahmen.
- DFC-SYSTEMS garantiert über eigene und externe Kompetenzen im Bereich Datenschutz und IT-Sicherheit, das bereits bestehende Sicherheitsniveau nicht nur zu halten, sondern stetig weiter zu verbessern.
- Die Verarbeitung der Daten erfolgt ausschließlich in deutschen Rechenzentren, die über die erforderlichen Datenschutz-, Sicherheits- und Compliance-Zertifizierungen verfügen.

### Gegenstand der Datenschutzbestimmungen

DFC-SYSTEMS möchte seine Nutzer durch die Datenschutzbestimmungen darüber informieren, wie die personenbezogenen Daten verarbeitet und geschützt werden, die bei der Registrierung und Anwendung von indicda medicalONE zum Einsatz kommen.

### Identität und Kontaktdaten der verantwortlichen Stellen

Rechtliche Erklärung: Die für die Verarbeitung von personenbezogenen Daten verantwortliche Stelle ist, laut Gesetz, die Person (Nutzer), die die Mittel und Zwecke der Verarbeitung bestimmt. Der Auftragsverarbeiter ist die Person, die im Namen und im Auftrag der verantwortlichen Stelle personenbezogene Daten verarbeitet. Der Auftragsverarbeiter handelt ausschließlich unter der Aufsicht und gemäß den Weisungen der verantwortlichen Stelle. Verantwortliche Stelle für die Verarbeitung der personenbezogenen Daten ist:

1. Für die personenbezogenen Daten, die durch den Nutzer (Abonnenten) bei der Registrierung und Anwendung von indicda medicalONE erfasst werden: jeder Nutzer selbst. DFC-SYSTEMS ist Auftragsverarbeiter und handelt nach der Weisung der verantwortlichen Stelle.
2. Für die Daten, die vom Nutzer bei der Registrierung und Anwendung von indicda medicalONE auf der durch DFC-SYSTEMS administrierten Rechenzentrums-Infrastruktur (RZI) verarbeitet werden: DFC-SYSTEMS GmbH, Claudius-Keller-Straße 3c, D-81669 München.

DFC-SYSTEMS ergreift die geeigneten technischen und organisatorischen Maßnahmen, um die Sicherheit und die Geheimhaltung sämtlicher Daten, über die DFC-SYSTEMS verfügt oder die DFC-SYSTEMS unter Einhaltung des BDSG und der DSGVO verarbeitet, sicherzustellen.

## Erhebung und Herkunft der Daten

Alle Daten, die Nutzer betreffen, werden nur direkt von diesen erhoben. In jedem Falle werden die Nutzer über die Zwecke informiert, zu denen ihre Daten von DFC-SYSTEMS über die verschiedenen Online-Datenerfassungsformulare oder über eingesetzte Cookies erhoben werden.

## Zweck der Datenverarbeitung

### 1. Notwendigkeit der Erhebung und Verarbeitung von personenbezogenen Daten

Für die Registrierung bei indicda medicalONE und zur Anlegung eines Nutzeraccounts ist die Erhebung von personenbezogenen Daten des Nutzers erforderlich. Zur Anlage eines Nutzeraccounts werden folgende Daten erhoben: E-Mail-Adresse, Telefonnummer, Passwort, Name, Vorname, Geschlecht, Geburtsdatum, Adresse.

### 2. Rechtsgrundlage für die Erhebung und Verarbeitung von personenbezogenen Daten

Die Rechtsgrundlage für die Erhebung der Benutzerdaten ist:

- Erbringung unserer Services für Nutzer/Abonnent, Identifizierung, Kontrolle der Berechtigung zum Abruf des Angebots bzw. Nutzung des Dienstes/Services zur Online-Spracherkennung (Art. 6 Abs. 1 lit. b) DSGVO).
- unser berechtigtes Interesse an der Sicherstellung der besten Qualität unserer Services/Dienste zur Online-Spracherkennung sowie an der Verbesserung des Betriebs unserer Website und unserer Anwendung (Art. 6 Abs. 1 lit. f) DSGVO).

## Arten der verarbeiteten personenbezogenen Daten

DFC-SYSTEMS kann als Auftragsverarbeiter nach Art. 28 DSGVO für die Bereitstellung des Dienstes/Services indicda medicalONE zur Online-Spracherkennung ganz oder teilweise folgende Daten für den verantwortlichen Nutzer/Abonnenten verarbeiten:

- Nachname, Vorname, Geburtsdatum, Geschlecht des Nutzers
- Telefonnummer, E-Mail-Adresse, Postanschrift des Nutzers
- Benutzername und Kennwort des Nutzers
- Medizinische Fachdisziplin des Nutzers

DFC-SYSTEMS kann als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO im Rahmen der Nutzung der indicda medicalONE Online-Spracherkennung durch den Nutzer/Abonnenten ganz oder teilweise folgende Daten erheben:

- Informationen zur Nutzung der Anwendung durch den Nutzer/Abonnenten (Nutzungszeit, Nutzungsdauer)
- Informationen zur Verhinderung und Bekämpfung von Computerbetrug: IP-Adresse, Endgerät
- Informationen, um die Navigation für den Benutzer innerhalb der Anwendung oder die Nutzung der Anwendung selbst zu verbessern: Login- und Nutzungsdaten, Anwendungsprofil

## Keine Weitergabe der personenbezogenen Daten

Personenbezogene Daten werden unter keinen Umständen an Dritte ohne in dieser Erklärung beschriebene Rechtsgrundlage weitergeleitet. Die personenbezogenen Daten dürfen von DFC-SYSTEMS und Unterauftragnehmern (Dienstleister) nur zur Erfüllung und unter strenger Beachtung der oben genannten Zwecke unter Einhaltung der Datenschutzbestimmungen verwendet werden. Im Rahmen ihres jeweiligen Verantwortungsbereichs und der oben genannten Zweckerfüllung sind die Personen, die Zugang zu den durch DFC-SYSTEMS verarbeiteten Daten erhalten können, Angestellte des DFC-SYSTEMS Kundenservice. DFC-SYSTEMS setzt nur Rechenzentrum-Provider in Deutschland ein. Es werden diesen keine personenbezogenen Daten mitgeteilt.

## Dauer der Speicherung

Daten werden nur so lange gespeichert, wie es in Übereinstimmung mit dem anwendbaren Recht für die Erfüllung des jeweiligen Zwecks erforderlich ist.

DFC-SYSTEMS erhebt und verarbeitet die IP-Adresse des Nutzers auf Grundlage seines berechtigten Interesses während einer Dauer von 12 Monaten ab dem Zeitpunkt der Datenerhebung. Diese Verarbeitung ist für die folgenden Zwecke erforderlich:

- Gewährleistung der Sicherheit und Robustheit der Plattform
- Identifizierung von unnormalen Verbindungsdaten zur Abwehr von Attacken
- Beweisführung im Fall von Streitigkeiten
- Sicherstellung der Nutzung des Dienstes/Services indicda medicalONE

## Rechte der Nutzer

DFC-SYSTEMS trifft alle erforderlichen Maßnahmen, um die Genauigkeit und Relevanz der Datenverarbeitung gemäß dem Zweck, für den sie erfasst werden, zu gewährleisten. Gemäß der DSGVO stehen dem Nutzer folgende Rechte zu:

- Recht auf Zugang, Auskunft, (Artikel 15 DSGVO), Berichtigung (Artikel 16 DSGVO), Aktualisierung und Vollständigkeit der Nutzerdaten
- Recht auf Sperrung oder Löschung der personenbezogenen Daten (Artikel 17 DSGVO), falls diese ungenau, unvollständig oder nicht mehr valide sind oder deren Erhebung, Benutzung, Mitteilung oder Speicherung unerlaubt ist
- Recht auf jederzeitiges Widerrufen der Einwilligung (Artikel 13-2 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO)
- Recht auf Widerspruch gegen die Verarbeitung (Artikel 21 DSGVO)
- Recht auf Datenübertragbarkeit der vom Nutzer eingegebenen Daten, soweit diese aufgrund eines Vertrages oder einer Einwilligung automatisiert verarbeitet werden (Artikel 20 DSGVO)

Der Nutzer/Abonnent hat das Recht zu erfahren, wie DFC-SYSTEMS seine personenbezogenen Daten einsetzt, das Recht auf Einspruch (Widerspruch, Löschung, Sperrung, Einschränkung, Aktualisierung) gegen die Verarbeitung oder darauf, eine erklärte Einwilligung zur Verarbeitung personenbezogener Daten durch DFC-SYSTEMS zu widerrufen, sowie das Recht auf Berichtigung. Der Nutzer/Abonnent kann DFC-SYSTEMS schriftlich unter folgender Adresse kontaktieren: DFC-SYSTEMS GmbH, Claudius-Keller-Straße 3c, D-81669 München oder per E-Mail an [datenschutz@dfcsystems.de](mailto:datenschutz@dfcsystems.de). Für die Anträge auf Löschung von personenbezogenen Daten sind die gesetzlichen Verpflichtungen von DFC-SYSTEMS zur Aufbewahrung oder Archivierung der betroffenen Dokumente zu berücksichtigen. Der Nutzer/Abonnent hat zudem das Recht, sich bei einer Datenschutz-Aufsichtsbehörde über die Verarbeitung seiner personenbezogenen Daten durch DFC-SYSTEMS zu beschweren.

## Sicherheit

DFC-SYSTEMS richtet alle technischen und organisatorischen Maßnahmen darauf aus, die sichere und geschützte Verarbeitung der personenbezogenen Daten zu gewährleisten. In diesem Zusammenhang trifft DFC-SYSTEMS alle notwendigen Vorkehrungen hinsichtlich der Art der Daten und der mit der Verarbeitung verbundenen Risiken, um die Sicherheit der Daten zu gewährleisten und insbesondere zu verhindern, dass sie verfälscht, beschädigt oder unbefugten Dritten zugänglich gemacht werden (physischer Schutz der Einrichtungen, Authentifizierungsprozess mit persönlichem und sicherem Zugang durch Benutzernamen und vertrauliche Kennwörter, Protokollierung der Verbindungsdaten, Verschlüsselung bestimmter Daten, etc.).

## **Anlage 1: Technische und organisatorische Maßnahmen (TOM) zu Datenschutz und Datensicherheit der DFC-SYSTEMS GmbH am Firmensitz München und im Rechenzentrum Frankfurt**

### **1. Vertraulichkeit**

#### **Zutrittskontrolle**

##### **Sicherungsmaßnahmen für Gebäude, Büroräume, Tiefgarage am Firmensitz München**

Das Gebäude und die Büroräume werden überwacht durch Bewegungsmelder und eine Alarmanlage mit akustischem Alarm und automatischer Alarmierung des Wachdienstes.

Der Zutritt in das Bürogebäude ist nur zwischen Montag und Freitag von 07:00 bis 19:00 Uhr möglich, außerhalb dieser Zeiten nur über eine Schlüssel-Token. Der Zutritt zu den Büroräumen ist ausschließlich über ein Schlüssel-Token möglich. Alle Besucher werden im Empfangsbereich durch das entsprechende Personal abgeholt und begleitet. Alle Besuche werden im Sekretariat protokolliert. Der Zugang zur Tiefgarage ist nur mit entsprechendem Tiefgaragen-Schlüssel möglich. Der Zugang von der Tiefgarage in das Bürogebäude ist nur mit Schlüssel-Token möglich. Gebäude, Büroräume und Tiefgarage verfügen über ein elektronisches Schließsystem; verlorene Schlüssel- oder Schlüssel-Token können zentral gesperrt werden. Weitere Zugänge zu Gebäude, Tiefgarage und Büroräumen sind nicht vorhanden. Geschäftsräume sind alle mit Isolierverglasung versehen. Räume mit Datenverarbeitungsanlagen besitzen keine Fenster.

##### **Sicherungsmaßnahmen für datenverarbeitende Systeme**

Der Zugang zu zentralen DV- und TK-Systemen ist nur autorisierten Mitarbeitern der DFC-SYSTEMS gestattet. Der Zutritt zu den Räumlichkeiten (Serverraum) ist zusätzlich durch ein Code-System gesichert (2-Faktor-Autorisierung). Externe Wartungstechniker haben nur in Begleitung von DFC-Personal Zutritt zu diesen Räumlichkeiten.

#### **Verwaltung der Zutrittsmittel**

Zur Verwaltung der und dem Umgang mit Zutrittsmitteln (Schlüssel, Schlüssel-Token, Zugangs-Code) existiert eine Dienstanweisung. Diese regelt auch die Dokumentation der Zutrittsmittel im Schlüsselbuch. Maßnahmen/Regelungen bei Verlust eines Zutrittsmittels sind ebenfalls in der Dienstanweisung festgeschrieben.

##### **Sicherungsmaßnahmen für Gebäude und Betriebsgelände Rechenzentrum Frankfurt**

Für das Betriebsgelände und das Gebäude des Rechenzentrums in Frankfurt bestehen folgende Sicherungsmaßnahmen. Überwachung des Gebäudes durch:

- Alarmanlage, Gebäudeüberwachung, Videoüberwachung
- Überwachung des Betriebsgeländes durch:
  - Sicherheitsdienst (24/7)
  - Durchgängig besetzter Empfang im Verwaltungsgebäude

Das gesamte Gelände ist von einem Sicherheitszaun umgeben. Die Zufahrt zum Gelände ist nur über eine beschränkte Pforte möglich. Das Rechenzentrum/die Serverräume befinden sich in einem separat gesicherten und überwachten Gebäude. Zutritt haben nur die Mitarbeiter (abgestufte Zutrittsregelungen). Der Zutritt muss unabhängig von den vorhandenen Ausweisen im Vorfeld angemeldet werden. Es werden Anwesenheitsaufzeichnungen im Sicherheitsbereich geführt. Es bestehen schriftliche Zutrittsregelungen. Der Zutritt für grundsätzlich nicht zugriffsberechtigte Mitarbeiter und unternehmensfremde Personen (z. B. Wartungstechniker, Reinigungskräfte, Besucher) ist durch Begleitung geregelt. Die Datenverarbeitungstechnik ist auf dem Betriebsgelände in dedizierten Räumen untergebracht. Das Rechenzentrum ist permanent mit einbruchs- und feuerhemmenden Türen verschlossen. Zutritt ist nur über autorisierte Personen mittels 2-Faktor-Autorisierung (Berechtigungsausweis + biometrische Prüfung) möglich. Der Zugang zum Rechenzentrum wird permanent mit Kameras überwacht.

## **Zugangskontrolle zu Datenverarbeitungsanlagen**

Mit der Zugangskontrolle soll die Benutzung der Datenverarbeitungsanlage(n) gesichert werden. Dies betrifft den lokalen Zugangsschutz, wie z. B. passwortgesicherter Zugang auf Betriebssystemebene sowie bei vernetzten Systemen der Zugriff/Zugang über das Netzwerk.

## **Identifikation und Authentifikation von Benutzern**

Identifikation und Authentifikation von Benutzern erfolgt mit User-ID (Benutzername) und Passwort am Client sowie an der Anwendung/Host (abhängig von der Applikation). Nach 5 Minuten Inaktivität des Benutzers wird die Bildschirmsperre des Arbeitsplatzrechners erzwungen. Die Bildschirmsperre ist nur durch Eingabe des Passwortes aufhebbar.

## **Passwortrichtlinien**

Es existieren Vorgaben für die Mindestlänge (8 Zeichen) und Komplexitätsanforderungen (Groß- und Kleinschreibung sowie mind. 1 Sonderzeichen) von Passwörtern.

Passwörter sind mit einer Gültigkeitsdauer von max. 6 Monaten versehen. Die dargestellten Passwortkonventionen werden durch Systemeinstellungen erzwungen.

## **Remotezugriff von Mitarbeitern**

Remotezugriff von Mitarbeitern erfolgt ausschließlich über Dienstrechner der Mitarbeiter sowie über verschlüsselte VPN-Verbindungen. Die Dienstrechner sind mit einem aktuellen Virenschutz versehen. Jeder Remotezugriff muss beantragt werden und unterliegen der Genehmigung.

## **Zugriffskontrolle zu Datenverarbeitungsanlagen**

Zu verstehen ist hierunter insbesondere die Kontrolle der Berechtigung zum Zugriff auf die jeweiligen Daten. Nur die Person, die den Zugriff auf jeweilige Daten für ihre jeweilige Tätigkeit benötigt, darf die Zugriffsrechte erhalten. Es wird gewährleistet, dass die Nutzungsberechtigten 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 können.

## **Systemadministration**

Die Administration der Datenverarbeitungssysteme wird von internen Mitarbeitern der DFC-SYSTEMS durchgeführt. Administratoren identifizieren sich mit User-ID und Passwort gegenüber dem Client und ggf. der Anwendung/Host. Für die Differenzierung zwischen der User- und Administrationstätigkeit werden doppelte User-ID / Passwörter pro Person eingesetzt.

## **Trennungskontrolle**

Es wird gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden, und zwar durch eine logische und physikalische Trennung.

## **2. Integrität**

### **Weitergabekontrolle/Aufbewahrung/Vernichtung**

Ziel ist die Gewährleistung, 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 und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Datenweitergabe und -transport beruhen auf einheitlichen Systemen zur Authentifizierung von Benutzern durch Benutzererkennung, Zertifikat und Passwort. Alle Kanäle über unsichere Medien (z. B. Internet) werden mittels kryptographischer Verschlüsselung (VPN) gesichert. Datenträger, die aus Gründen der Betriebssicherheit angefertigt werden, werden an zentralen Stellen unter Verschluss gehalten. Betriebsrelevante Daten werden, in verschlüsselter Form, aus Gründen der Betriebssicherheit zusätzlich an einen externen Standort ausgelagert.

Es existieren Regelungen über die Vernichtung von Datenträgern/Festplatten etc. (z. B. Anzahl der Löschvorgänge). Nicht mehr benötigte Dokumente in Papierform werden in den Bereichen geschreddert. Die Entsorgung von größeren Mengen an Dokumenten erfolgt über ein zertifiziertes Drittunternehmen.

### **Eingabekontrolle**

Je nach Verhältnismäßigkeit wird die revisionssichere automatische Protokollierung der

Eingaben in Logfiles oder Tabellen erzwungen. Elemente der Protokollierung sind:

- betroffener Datensatz
- Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes)
- Zeitpunkt der Aktivität bzw. des Ereignisses
- ausführende Person (Benutzerkennzeichen)

Je nach Notwendigkeit und unter Berücksichtigung der geltenden Datenschutzbestimmungen wird eine Auswertungsmöglichkeit dieses Protokolls zur Verfügung gestellt.

## **3. Verfügbarkeit und Belastbarkeit**

### Verfügbarkeitskontrolle

#### **Betriebsbereitschaft**

Der Betrieb wird durch Personal vor Ort von 08:00 Uhr bis 18:00 Uhr, Montag bis Freitag, sichergestellt. Die IT-Systeme werden rund um die Uhr mittels einer Überwachungslösung überwacht. Alle zentralen Server- und Storage-Systeme sind redundant ausgelegt. Es existiert ein Alarmierungsplan bei Ausfall der zentralen Server- und Storage-Systeme an 24/7.

#### **Datensicherung**

- Es findet eine tägliche automatisierte Sicherung der Daten statt.
- Es werden zusätzlich verschlüsselte Kopien der Datensicherungen ausgelagert.
- Es erfolgt eine wöchentliche Prüfung der Protokollierung der Datensicherung.
- Pro Quartal wird ein Einleseversuch der Datensicherung unternommen.
- Jedes Jahr wird eine Wiederherstellung durchgeführt.

#### **Unterbrechungsfreie Stromversorgung / Notstromaggregat**

Alle systemrelevanten Datenverarbeitungsanlagen sind mit einer ausreichend dimensionierten USV versehen. Das Rechenzentrum in Frankfurt verfügt über ein Notstromaggregat sowie über einen ÜberspannungsfILTER und Temperatur-/Feuchtigkeitsüberwachung.

### Wiederherstellbarkeit

- Das Qualitätsmanagement von DFC-SYSTEMS umfasst u. a. Prozesse und Definitionen zu:
- Zeitplanung, Art u. Umfang von regelmäßigen Recovery Tests
- Verwendete interne und externe Schnittstellen mit Verantwortlichkeiten
- Risikobewertung der eingesetzten Prozesse
- Beschreibung Eskalationsprozess und Maßnahmenplan

**Vorliegende Richtlinien und Anweisungen bestehen in Bezug auf die Datensicherheit:**

- Geeignete IT-Sicherheitsmaßnahmen (Datensicherungskonzept)
- Sicherheit- und Notfallkonzept
- Förderung des Sicherheitsbewusstseins (Mitarbeiter)
- Langzeit-Archivierung
- Nutzung von E-Mail
- Nutzung von Internet
- Schutz, Bekanntgabe und Vernichtung von Daten
- Sicherheitsleitlinien für Mitarbeiter

**Regelmäßige Aktivitäten**

- Administrativer Support von Sicherheitseinrichtungen
- Reaktion auf sicherheitsrelevante Ereignisse
- Fortlaufende Überwachung der IT-Systeme
- Change-Management
- Mitarbeiterschulungen

**Weitergehende Maßnahmen**

- Basis-Benutzerpasswort
- Mehrfach-Log-ons und -Passwörter
- Virtual Private Network (VPN) für Datenverschlüsselung
- Secure Sockets Layer (SSL)
- Spam-Filter
- Paket-Filter
- Content-Filter
- Desktop-Antiviren-Software
- Antiviren-Software
- Personal-Firewalls
- Anwendungs-Firewalls
- Netzwerk-Firewalls
- VPN-Lösung für Homeoffice-Anbindung

#### 4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

##### Datenschutzmanagement

DFC-SYSTEMS führt bereits seit 2009 ein Datenschutz-Managementsystem zur Einhaltung der Datenschutzbestimmungen. Aufgaben und Pflichten des Datenschutzbeauftragten sind in einer Verfahrensanweisung definiert. Die Bestellung erfolgt formal.

Der Beauftragte für den Datenschutz als internes fachlich weisungsunabhängiges Organ überwacht die Einhaltung der Datenschutzvorschriften. Er ist verantwortlich für die Richtlinien auf dem Gebiet des Datenschutzes und überwacht deren Einhaltung. Er führt Datenschutz-Kontrollen und -Audits durch. Der Beauftragte für den Datenschutz wird von der Geschäftsführung der DFC-SYSTEMS bestellt.

Das Qualitätsmanagement definiert verfahrensbezogene technische und organisatorische Maßnahmen (Verfahrensanweisungen) betreffend:

- Informationspflichten des Unternehmens
- Gewährung der Rechte der Betroffenen
- Umgang mit Kunden und Patientendaten (inkl. Fernwartung und Datenimporte)
- Datenschutz-Folgenabschätzung
- AV-Verträge
- Datenpannen

Neben den verpflichtenden Datenschutzregelungen wurden bestimmte Prozesse bei DFC-SYSTEMS zentral durch Prozesse geregelt. Dazu gehören:

- Verpflichtung aller Mitarbeiter auf Datengeheimnis nach DS-GVO sowie auf die Schweigepflicht nach §203 StGB (Verpflichtung sind als Anlagen in die Arbeitsverträge integriert, jeder neue Mitarbeiter wird somit vor dem Beginn der Tätigkeit verpflichtet)
- Schulung neuer Mitarbeiter auf Datenschutz zeitnah nach der Einstellung
- Datenschutz-Prüfung neuer Software/Module bereits während der Planungsphase

## Auftragskontrolle

### **Auftragskontrolle Fernwartung**

Den Kunden wird grundsätzlich empfohlen, die Fernwartungs-Zugänge geschlossen zu halten und nur bei Bedarf und nach telefonischer Anfrage den Zugang frei zu schalten. Dieses Vorgehen liegt im Ermessen des Kunden. Beim Zugriff auf Kundensysteme ausgehend von mobilen Arbeitsplätzen oder von Home-Offices ist es verboten, gleichzeitig Verbindung zu unsicheren, unbekanntem Netzwerken aufgebaut zu haben. Die Verbindung zu Kunden darf immer erst nach dem erfolgreichen Aufbau des Zugriffs zur Zentrale durch den VPN Client erstellt werden. Der VPN Client lässt in der standardmäßigen Einstellung keine weiteren Verbindungen zu. Diese Einstellungen dürfen nicht geändert oder kompromittiert werden. Besondere Tätigkeiten, welche das Produktivsystem verändern und/oder ein Risiko oder eine hohe Auswirkung auf die Prozesse beim Kunden haben, werden durch das 4-Augenprinzip über eine qualifizierte Person abgesichert.

Es werden Fernwartungs-Werkzeuge verwendet, bei welchen der Kunde aktiv den Zugang freigeben muss und die Aktivitäten mitverfolgen kann (z. B. TeamViewer). Wenn die eingesetzte Fernwartungssoftware diese aktive Freigabe nicht voraussetzt, wird der Kunde über die Notwendigkeit des Zugriffs informiert und seine Zustimmung dafür angefordert.

Diese Zustimmung (wer und wann) wird schriftlich dokumentiert. Die Dokumentation des Fernwartungszugriffes und dessen Inhalt erfolgt immer in einem CRM-System (Service Ticket-System). Es ist nicht erlaubt, undokumentierte Fernwartungszugriffe durchzuführen. Sämtliche Aktivitäten auf dem Kundensystem sind nachvollziehbar für Dritte sachlich beschrieben.

Hierbei wird immer dokumentiert:

- der ausführende Mitarbeiter
- der Zeitpunkt (Datum/Uhrzeit) und die Dauer
- das Zielsystem (Test oder Produktiv bzw. Rechnername oder IP-Adresse)
- die Tätigkeit sachlich in Kurzform, insbesondere wenn Prozesse gestoppt/gestartet, Änderungen in Datenbanken, Änderungen in Konfigurationstabellen, Uploads und Downloads durchgeführt wurden

Mit Kunden, die per Fernwartung betreut werden, müssen einmalig schriftliche Datenschutzvereinbarungen, sog. AV-Verträge (AVV), abgeschlossen werden. Diese Vereinbarungen regeln die Fernwartungszugriffe sowie Datenverarbeitung auf den Kundensystemen.

### Incident Management

Das DFC IT-Service Team stellt sicher, dass angemessen auf jegliche aktuellen oder zu erwartenden Vorfälle bezüglich der internen oder in der Betreuung befindlichen Informationssysteme reagiert werden kann. Hierzu wurden entsprechende Maßnahmen definiert, die sicherstellen, dass:

- Sicherheitsvorfälle frühzeitig erkannt werden und deren Auswirkungen minimiert oder begrenzt werden können
- Bei Eintreten eines Vorfalls strukturierte und zeitsparende Vorgehensmodelle in Verbindung mit Verantwortlichkeiten existieren, wie Maßnahmen und Vorgehensweisen
- Vorfälle nachvollziehbar dokumentiert und analysiert werden können
- Die Wiederholung des Vorfalls durch Ergreifen nachhaltiger Maßnahmen vermieden werden kann

### Privacy by Default

Es gibt ein einheitliches Konzept zu Datenschutz-relevanten und IT-sicherheitstechnischen Voreinstellungen und Standards für die zu administrierenden IT-Systeme, wie:

- Voreinstellungen des Betriebssystems für Client PCs und der automatischen Bereitstellung von sicherheitsrelevanten Updates und Verteilung von Software-Applikationen
- Voreinstellungen des Betriebssystems für aus Vorlagen bereitgestellten virtuellen Servern

### Zertifizierungen Rechenzentrum Frankfurt

Das Rechenzentrum in Frankfurt wird betrieben durch die Microsoft Deutschland GmbH und verfügt über folgende Zertifizierungen:

- Information Security Management System ISO/IEC 27001:2013 (TÜV NORD CERT GmbH)
- Code of practice for protection of personally identifiable information (PII) in public clouds ISO/IEC 27018 (TÜV NORD CERT GmbH)