KVB

KASSENÄRZTLICHE
VEREINIGUNG BAYERNS
Körperschaft des öffentlichen Rechts

IT- ERC

KVB-Dienststelle

Geschäftszeichen:	10724252
Vertrags-Nummer (EVB-IT):	

Verpflichtung

zur Befolgung der nachfolgend dargestellten technischen und organisatorischen Maßnahmen beim Zugriff auf das Netzwerk der KVB zu Wartungs- und Entwicklungszwecken aus ungemanagten Netzwerken (z.B. dem Homeoffice)

bei der Durchführung der Leistungen nach dem/den zwischen der Fa. FREIHAFEN IT GmbH und der Kassenärztlichen Vereinigung Bayerns bestehenden Vertrages/Verträge.

Der Person (nachfolgend Dienstleister genannt), welche tatsächlich den Zugriff auf Systeme und Daten der KVB durchführt, verpflichtet sich die nachfolgenden Technischen und Organisatorische Maßnahmen zu befolgen.

Der Zugriff auf das Netzwerk der KVB erfolgt bevorzugt über den von der KVB zur Verfügung gestellten Hardware Client. Dieser wird ausschließlich vom Dienstleister verwendet.

Erfolgt der Zugriff auf das Netzwerk der KVB über einen Hardware Client, der von der o. g. Firma zur Verfügung gestellt wird, so wird sichergestellt dass der Hardware Client entsprechend den Empfehlungen des BSI Grundschutzes gemanagt wird (https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html).

Der Hardwareclient wird bei Nichtbenutzung so aufbewahrt, dass eine Manipulation oder Benutzung durch unbefugte Dritte hinreichend sicher ausgeschlossen werden kann (z.B. abgeschlossener Schrank, abgeschlossenes Büro).

Der Dienstleister unterlässt alle Handlungen die die voreingestellten Sicherheitsmaßnahmen am Hardwareclient deaktivieren oder schwächen. Bei Entdeckung einer Schwachstelle muss umgehend der IT Support der KVB (bei KVB Client) oder der IT-Support der oben genannten Firma (bei Hardware dieser Firma) benachrichtigt werden.

Es werden keine drahtlosen Eingabegeräte (Maus, Tastatur, etc.) verwendet.

Es werden keine Abzüge des Bildschirminhaltes erstellt (z.B. Screenshots oder Fotografien). Wird ein von der KVB gemanagter Hardware Client eingesetzt gilt: Es werden keine Abzüge des Bildschirminhaltes erstellt (z.B. Screenshots oder Fotografien), die den Hardwareclient verlassen.

Der Hardwareclient wird so positioniert, dass kein unbefugter Einblick in die dargestellten Bildschirminhalte möglich ist (z.B. durch ein Fenster zur Straße oder mit Fernrohr aus Nachbargebäude). Maßnahmen können Sichtschutzfolien, Vorhänge, Stellwende etc. sein.

Bei Verlust oder Diebstahl des Hardwareclients oder der Authentisierungsmittel (Tokengenerator, Passwort) wird umgehend der KVB IT Support benachrichtigt (ggf. auch der IT Support der Eigentümerfirma).

Die Zugangsmittel (Hardwareclient, Tokengenerator etc.) werden nach Aufforderung durch die KVB, spätestens bei Beendigung des Vertragsverhältnisses, an die KVB zurückgegeben.

Der Dienstleister erklärt sich damit einverstanden, dass alle seine Tätigkeiten in der KVB aufgezeichnet werden.

Dieses Dokument ist vom Dienstleister persönlich zu unterzeichnen.

Brunsbüttel 19.04.23
Ort, Datum

Unterschrift Kandidat/in

Name (Kandidat/in) in Druckschrift:

Oliver Perschke

KVB

KASSENÄRZTLICHE
VEREINIGUNG BAYERNS
Körperschaft des öffentlichen Rechts

IT- ERC
KVB-Dienststelle

Geschäftszeichen:	**10724252**
10724252 Vergabe-Nummer:	**10724252**

Verpflichtung

auf die Vertraulichkeit nach DSGVO und zur Wahrung, das Datengeheimnisses nach Art. 11 BayDSG und des Sozial- und Patientengeheimnisses

bei der Durchführung der Leistungen nach dem/den zwischen der Fa. FREIHAFEN IT GmbH und der Kassenärztlichen Vereinigung Bayerns bestehenden Vertrages/Verträge.

Bei der Kassenärztlichen Vereinigung Bayerns werden im Rahmen ihrer Aufgabenerfüllung überwiegend hochsensible medizinische Patientendaten, aber auch Arztdaten und Daten der Mitarbeiter der Kassenärztlichen Vereinigung Bayerns erhoben, verarbeitet und genutzt.

Der Gesetzgeber hat die Kassenärztliche Vereinigung Bayerns (gleichermaßen Krankenkassen, Rentenversicherungsträger etc.) durch strenge gesetzliche Vorschriften zur Wahrung dieser persönlichen Geheimnisse verpflichtet. Die wichtigsten gesetzlichen Vorschriften sind in der Anlage zu dieser Verpflichtung abgedruckt.

Die Durchführung von Arbeiten im Rahmen des/der o. g. Vertrages/Verträge kann in Einzelfällen erforderlich machen, dass der Unterzeichner nach den obigen Vorschriften geschützte Sozialdaten bzw. personenbezogene Daten zur Kenntnis nehmen kann. Nach dem zu dem/den o. g. Vertrag/Verträgen abgeschlossenen Datenschutzvertrag ist der Unterzeichner bei der Durchführung seiner Arbeiten in der Kassenärztlichen Vereinigung Bayerns in gleichem Maße wie Mitarbeiter der Kassenärztlichen Vereinigung Bayerns verpflichtet, die obigen Geheimnisse zu wahren. Die Verpflichtung gilt auch über das Ende des/der o.g. Vertrages/Verträge hinaus und wirkt auch nach einer ggf. eintretenden Beendigung des Beschäftigungsverhältnisses des Unterzeichners mit der Fa. **FREIHAFEN IT GmbH.**

Belehrung und Verpflichtung

Ich bestätige, dass ich die für die Kassenärztliche Vereinigung Bayerns geltenden gesetzlichen Verschwiegenheitspflichten und die gesetzlichen Datenschutz- und Strafvorschriften zur Kenntnis genommen habe. Ich verpflichte mich zur uneingeschränkten Beachtung dieser Verschwiegenheitspflichten. Mir ist bekannt, dass ein Verstoß gegen diese Pflichten strafrechtliche und haftungsrechtliche, aber auch arbeitsrechtliche Maßnahmen zur Folge haben kann.

Brunsbüttel, 19.04.23
Ort, Datum

Unterschrift Kandidat/in

Name (Kandidat/in) in Druckschrift: Oliver Perschke

Funktion in der Fa. **Seniorberater / Consultant**

Anlage zur Verpflichtung auf die Vertraulichkeit

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim betrieblichen Datenschutzbeauftragten.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „**Personenbezogene Daten**" [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Art. 4 Nr. 2 DS-GVO: „**Verarbeitung**" [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] auf **rechtmäßige Weise**, nach Treu und Glauben und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz").
Art. 5 Abs. 1 lit. f DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").
Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten **ausschließlich auf Weisung** des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.
Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch **Vernichtung**, **Verlust** oder **Veränderung**, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte **Offenlegung** von beziehungsweise unbefugten **Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer **Verletzung** des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...] zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftung

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf **Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.
Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von **Geldbußen** gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
§ 42 BDSG
(1) Mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.
(2) Mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.
§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit **Freiheitsstrafe** bis zu drei Jahren oder mit **Geldstrafe** bestraft.
§ 303a Abs. 1 StGB: Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit **Freiheitsstrafe** bis zu zwei Jahren oder mit **Geldstrafe** bestraft.

Optional – Fernmeldegeheimnis

§ 88 TKG

(1) [1]Dem Fernmeldegeheimnis unterliegen der **Inhalt der Telekommunikation und ihre näheren Umstände**, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. [2]Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) [1]Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. [2]Die Pflicht zur Geheimhaltung besteht **auch nach dem Ende der Tätigkeit** fort, durch die sie begründet worden ist.

(3) [1]Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. [2]Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. [3]Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. [4]Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. […]

Optional – Sozialgeheimnis

§ 35 Abs. 1 Satz 1, Abs. 4 SGB I: Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs 2 SGB X) von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis). Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.

§ 67 Abs. 2 SGB X: Sozialdaten sind personenbezogene Daten (Art. 4 Nr. 1 DSGVO), die von einer in § 35 des SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Datgen, auch von juristischen Personen, die Geheimnischarakter haben.

§ 78 Abs. 1 Satz 2 & 3 SGB X: […] [2]Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. [3]Die Dritten haben die Daten **in demselben Umfang geheim zu halten** wie die in § 35 [SGB I] genannten Stellen.

§ 85 Abs. 1 SGB X: Für Sozialdaten gelten die Strafvorschriften des § 42 Abs. 1 und 2 des BDSG entsprechend.