KVN-Portal

Das Onlineportal der KVN

KVN
Kassenärztliche Vereinigung
Niedersachsen

IT- Rahmen- und Sicherheitsrichtlinien

Informationen zum Datenschutz bei Nutzung des KVN-Portals

Der Zugang zum KVN-Portal ist mit einem starken Authentisierungsverfahren gegen Missbrauch geschützt. Für die Nutzung des KVN-Portals über KV-FlexNet benötigen Sie Ihre Benutzerdaten und eine persönlich auf Sie registrierte KVN-PINCard.

Der sehr hohe Sicherheitsstandard des KVN-Portals sichert ausschließlich den Zugriff auf die zur KVN übertragenen bzw. bei der KVN hinterlegten Daten.

Der Zugriff auf Ihre mit dem Internet verbundenen PC‘s durch unbefugte Dritte über das Internet ist nicht automatisch geschützt.

Für die **Absicherung** Ihrer mit dem Internet verbundenen PC‘s bzw. Ihres Praxisnetzes gegen unbefugte Zugriffe von Dritten sowie etwa gegen Trojaner und Viren **sind Sie selbst verantwortlich!**

Hierfür übernimmt die KVN **keine** Haftung.

Praktische Sicherheitshinweise geben Ihnen dazu unsere nachstehenden Informationen sowie die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

IT-Grundschutzprofile des BSI für kleine Institutionen (z.B. Arztpraxen):

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/it-grundschutz_profil_klein.pdf

Vorgaben zum Datenschutz von der KBV

http://www.kbv.de/html/7237.php

Zugangsdaten

Die Zugangsdaten zum KVN-Portal sind persönlich auf Sie ausgestellt. Eine Weitergabe und/oder die Kenntlichmachung Ihrer persönlichen Zugangsdaten an unbefugte Dritte erfolgt in Ihrer Verantwortung.

Bei Weitergabe der Zugangsdaten besteht die Gefahr des Missbrauchs sensibler Daten (arztbezogene-, persönliche- sowie Patientendaten etc.).

KVN-PINCard Personal

Der durch Sie aktivierte Benutzer der KVN-PINCard Personal hat die Berechtigung in Ihrem Namen und Ihrer Verantwortung im KVN-Portal tätig zu werden.

Für Schäden, die durch Missachtung des Datenschutzes entstehen, haften Sie als Passwortinhaber.

Bei Missbrauch übernimmt die KVN **keine** Haftung!

Aktuelle Programmversionen

Achten Sie darauf, dass auf Ihrem Computer stets die aktuellsten Updates/Patch-Level für Betriebssystem, Internet-Browser und Internet Security installiert sind, um so die Gefahr programmseitiger Sicherheitslücken zu reduzieren.

Sorgen Sie daher auch für eine automatische Aktualisierung.

Firewall

Eine Firewall ist ein Sicherungssystem, das einen Computer oder ein Rechnernetz vor unerwünschten Netzwerkzugriffen schützt und sollte ein Teil Ihres Sicherheitskonzepts sein.

Setzen Sie eine Firewall auf lokaler Rechnerebene und/oder auf Netzwerkebene ein und konfigurieren Sie die Firewall so, dass nur der benötigte Datenverkehr zugelassen wird.

Setzen Sie eine **Firewall von einem Drittanbieter** ein, kann die **KVN** im Fehlerfall **keine Unterstützung** leisten

Virenschutz

Setzen Sie eine aktuelle Antiviren-Software ein und sorgen Sie regelmäßig für Updates der Virensignaturen, damit Ihr Computer auch vor neuen Viren geschützt ist.

Schutz vor Phishing und Spyware

Unter Phishing versteht man den Versuch des Identitätsdiebstahls (Username, Passwort) und kann über E-Mails oder über eingeschleuste Spionageprogramme erfolgen um an persönliche Daten eines Benutzers zu gelangen.

Setzen Sie eine Anti-Spyware-Spezialsoftware ein, falls Ihr Antiviren-Programm diese Funktion nicht schon beinhaltet, und aktivieren Sie diese.

Bei Problemen mit solcher Art Software, wenden Sie sich bitte an den IT-Administrator Ihrer Praxis.

Verzicht auf Internet-Dienste

Deaktivieren Sie alle nicht benötigten Internet-Dienste auf Ihrem PC, soweit darauf sensible Daten (z.B. Patientendaten) gespeichert sind. Nehmen Sie auf diesem Rechner keine Datei-Downloads aus dem Internet vor (Ausnahme ggf. die Aktualisierung von Virensignaturen und neue Patches für Betriebssystem und Browser, sofern diese abgesichert von einer kontrollierten Adresse aus erfolgen; vgl. Firewall). Verzichten Sie auf die Nutzung von E-Mail-Programmen auf einem PC, der sensible Daten enthält, bzw. lassen Sie besondere Vorsicht vor verdächtigen E-Mails walten. Öffnen Sie keine unbekannten Dateianhänge und klicken Sie nicht auf in verdächtigen E-Mails enthaltene Links. Beachten Sie bitte immer die o.g. Sicherheitshinweise.

Zugang

Das KVN-Portal erreichen Sie entweder über KV-FlexNet mit KVN-PINCard (Software-VPN), über KV-SafeNet oder über das Netz der Telematikinfrastruktur (TI) mittels Konnektor (Hardware-VPN).

Systemanforderungen

Nachfolgende Mindestanforderungen muss Ihr Computer erfüllen.

Betriebssystem:*

- Windows 8.1 und Windows 10
- MAC OS X (Version 10.12.x - 10.15.x)

Internet Browser:*

- Internet Explorer ab Version 11.0
- Edge ab Version 42.0
- Google Chrome ab Version 64.x
- Mozilla Firefox ab Version 58.x
- Safari ab Version 10.x

* Änderungen dazu entnehmen Sie bitte von der Webseite der KVN

Internetanbindung:

- DSL
- UMTS

Sonstiges:

Installiertes Java Runtime Environment (JRE) Version 7

Sofern Sie in Ihrer Arztpraxis einen Terminalserver einsetzen, ist ein Zugang über KV-FlexNet nicht, oder nur eingeschränkt möglich.

Im Fehlerfall wenden Sie sich bitte an Ihren IT Betreuer.

Alternativ wählen Sie bitte den Zugang über KV-SafeNet bzw. über das Netz der Telematikinfrastruktur.

Kontakt

Unsere gebührenfreie IT-Servicehotline:

0800 5 101025

Unsere Servicezeiten:

Montag bis Donnerstag: 8 - 18 Uhr

Freitag: 8 - 16 Uhr

Gerne nehmen wir Ihre Anfrage auch via E-Mail entgegen:

it-service@kvn.de