

---

## Informationsblatt zum Datenschutz bei Nutzung von KV-Ident Plus

Stand April 2018

KV-Ident Plus ist ein so genanntes starkes Authentisierungsverfahren und bietet den KVB-Mitgliedern Zugang zu den webbasierten Informationsangeboten und Dienstleistungen der KVB sowie zum Sicheren Netz der KVen (SNK). Der Besitz eines persönlichen KV-Ident Plus Tokens und das Wissen des Kennworts der persönlichen KVB-Benutzererkennung realisieren eine Zwei-Faktor-Authentisierung für die sichere Anmeldung zum Mitgliederportal „Meine KVB“ bzw. den darin enthaltenen Online-Anwendungen sowie zum SNK.

Bei der Nutzung dieser webbasierten Informationsangebote und Dienstleistungen werden alle Daten über eine Tunnelverbindung über das Internet per TLS-Verschlüsselung übermittelt. Um eine Tunnelverbindung herstellen zu können, muss der Teilnehmer einmalig zu Beginn der Nutzung von KV-Ident Plus eine spezielle, von der KVB bereit gestellte VPN-Software installieren. Die Installation muss auf jedem Rechner erfolgen, mit dem KV-Ident Plus genutzt wird.

Für die Nutzung von KV-Ident Plus wird ein Rechner mit aktuellem Betriebssystem (Microsoft Windows 7 und höher oder Apple MAC OS 10.9 und höher) und Internetzugang sowie einem aktuellen Internet-Browser (Internet Explorer Version 8 und höher; Firefox Version 24 und höher; Google Chrome Version 21 und höher; Apple Safari Version 7 und höher) benötigt. Zusätzlich muss auf dem Rechner die von der KVB zur Verfügung gestellte VPN-Software installiert sein.

KV-Ident Plus gewährleistet die Sicherheit des Daten- und Informationsaustausches erst ab dem Zeitpunkt, ab dem der Tunnel aufgebaut ist. Bis zum Aufbau des Tunnels und der Authentisierung mit KV-Ident Plus bewegt sich der Teilnehmer im öffentlichen Internet. Hierfür und für eventuelle Auswirkungen von Schadprogrammen auf dem Rechner (z.B. Mitlesen von Tastatureingaben und Bildschirminhalten) kann die KVB keine Haftung übernehmen.

Für die Absicherung seines Rechners gegen unbefugte Zugriffe von Dritten ist der Teilnehmer selbst verantwortlich. In diesem Zusammenhang ist auf die Einhaltung der Empfehlungen der Kassenärztlichen Bundesvereinigung und Bundesärztekammer zu Datenschutz und Datenverarbeitung in der Arztpraxis<sup>1</sup> zu achten.

---

<sup>1</sup> Bundesärztekammer, Kassenärztliche Bundesvereinigung: Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis; Deutsches Ärzteblatt v. 09. März 2018  
Direktlink: [http://www.kbv.de/media/sp/Empfehlungen\\_aerztliche\\_Schweigepflicht\\_Datenschutz.pdf](http://www.kbv.de/media/sp/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf)  
Erweiterte Informationen: <http://www.kbv.de/html/datensicherheit.php>

## **Informationsblatt zum Datenschutz bei Nutzung von KV-Ident Plus**

---

### **Gemäß dieser Empfehlungen sind vom Teilnehmer u.a. folgende IT-Sicherheitsmaßnahmen zu tätigen:**

- Einsatz von aktuellen Viren-Schutzprogrammen und regelmäßige Aktualisierungen der eingesetzten Viren-Schutzprogramme.
- Einsatz einer Firewall. Eine Firewall ist eine Netzwerk-Sicherheitskomponente, die entscheidet, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren (öffentlichen) Netzes, wie z. B. dem Internet, aus dem privaten Netz heraus nutzbar sind. Sie gewährleistet somit die Einhaltung von Sicherheitsrichtlinien zwischen einem privaten und einem öffentlichen (nicht sicheren) Netz.

Bei der Teilnahme am KV-Ident Plus Verfahren der KVB obliegt es der Sorgfaltspflicht der Teilnehmer, für die eigene Rechtersicherheit zu sorgen. Die KVB weist ausdrücklich auf diese Sorgfaltspflicht hin. Bei Verwendung eines Rechners, der über einen direkten Zugriff auf Patientendaten oder einen anderen vernetzten Rechner mit Patientendaten verfügt, ist dieser nach gängigem Stand der Technik vom Internet zu schützen. Auf den Seiten des Bundesamts für Sicherheit in der Informationstechnik ([www.bsi.de](http://www.bsi.de)) werden die entsprechenden Empfehlungen dazu in aktueller Form vorgehalten und zur allgemeinen Nutzung zur Verfügung gestellt.

KV-Ident Plus bietet sehr hohe Sicherheitsstandards durch die Kombination der Benutzerkennung und des Tokens bei der Authentisierung. Um den Datenverkehr wirksam zu schützen, ist ein sorgfältiger Umgang mit beiden Faktoren unbedingt notwendig. Aus diesem Grund ist es wichtig, ein sicheres Kennwort auszuwählen und dieses sicher aufzubewahren.

### **Folgende Sicherheitsregeln sind zur Auswahl eines sicheren Kennworts und zum Umgang mit der KVB-Benutzerkennung zu beachten:**

- Ein sicheres Kennwort muss aus mindestens 8 Zeichen bestehen und mindestens eine Zahl und einen Buchstaben enthalten und darf nicht identisch mit dem alten Passwort sein.
- Dasselbe Kennwort nicht für mehrere unterschiedliche Online-Dienstleistungen benutzen.
- Das Kennwort ist geheim zu halten. Es darf nicht aufgeschrieben werden und unter keinen Umständen auf dem Rechner gespeichert werden.
- Das Kennwort darf keinem unbefugten Dritten überlassen werden.
- Das Kennwort ist regelmäßig, mindestens monatlich, zu ändern.
- Bei einem Verlassen des Arbeitsplatzes, melden Sie sich mittels dem Button „Abmelden“ (oben rechts) von der jeweiligen Anwendung ab.

Bei der Vermutung, dass jemand Zugang zum Kennwort hat, ist die persönliche KVB-Benutzerkennung unverzüglich sperren zu lassen.

Eine Sperrung der KVB-Benutzerkennung kann telefonisch veranlasst werden. Sie erreichen die Sperrhotline der KVB 24 Stunden am Tag unter 0 89 / 5 70 93 – 8 80 10.

## Informationsblatt zum Datenschutz bei Nutzung von KV-Ident Plus

---

### **Folgende Sicherheitsregeln sind zudem für den Umgang mit dem KV-Ident Plus Token zu beachten:**

- Die KVB-Benutzerkennung muss immer getrennt von dem KV-Ident Plus Token aufbewahrt werden.
- Der KV-Ident Plus Token darf nicht zugänglich für unbefugte Dritte aufbewahrt werden.
- Beim Verlassen des Arbeitsplatzes ist die bestehende Verbindung mit dem Button „Abmelden“ zu beenden.
- Der KV-Ident Plus Token darf keinem unbefugten Dritten überlassen werden.
- Den abgefragten Code des KV-Ident Plus Tokens niemals am Telefon nennen, noch auf Anfrage bei sogenannten Phishing E-Mails eingeben.
- Bei Verlust des KV-Ident Plus Tokens diesen unverzüglich sperren oder beenden lassen.

Über das Online Service-Portal kann der Teilnehmer jederzeit seine(n) KV-Ident Plus Token temporär sperren oder auch endgültig beenden.

Eine Sperrung des KV-Ident Plus Tokens kann telefonisch veranlasst werden. Sie erreichen die Sperrhotline der KVB 24 Stunden am Tag unter 0 89 / 5 70 93 – 8 80 10.

Weitergehende Informationen zum Thema Datenschutz sowie die Erläuterung Ihrer Rechte entnehmen Sie bitte der KVB-Internetseite unter: <https://www.kvb.de/datenschutz/>