Datenschutzschulung

für die APH, das psib und das JRI

Dirk Krebs

08.10.2025

Wie schützen wir personenbezogene Daten und was machen wir, wenn dies uns nicht gelingt?

1. Technischer Schutz und organisatorischer Schutz
2. Wie ist bei einem Datenschutzvorfall vorzugehen?

Wie schützen wir personenbezogene Daten in unserer Praxis?

- Technische Maßnahmen und organisatorische Maßnahmen (TOMS) zum Schutz der personenbezogenen Daten

Einstellungen

Einstellung suchen

Dirk Krebs
Lokales Konto

- Startseite
- System
- Bluetooth und Geräte
- Netzwerk und Internet
- Personalisierung
- Apps
- Konten
- Zeit und Sprache
- Spielen
- Barrierefreiheit
- Datenschutz und Sicherheit
- Windows Update

Konten

DIRK KREBS
Lokales Konto

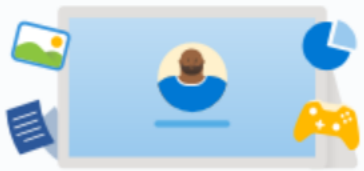
Prämien
• Anmelden

OneDrive
• Anmelden

Microsoft-Konto
Melden Sie sich an, um Windows optimal zu nutzen

Ein Konto für alles, was Microsoft ist

Greifen Sie mit nur einem Konto auf Ihre bevorzugten Microsoft-Produkte und -Dienste zu. Ihr Microsoft-Konto verbindet Sie mit den Dateien, Fotos, Personen und Inhalten, die Ihnen am wichtigsten sind.



Anmelden Weitere Informationen

Kontoeinstellungen

Ihre Infos
Profilbild

Suche

12:30
09.10.2025

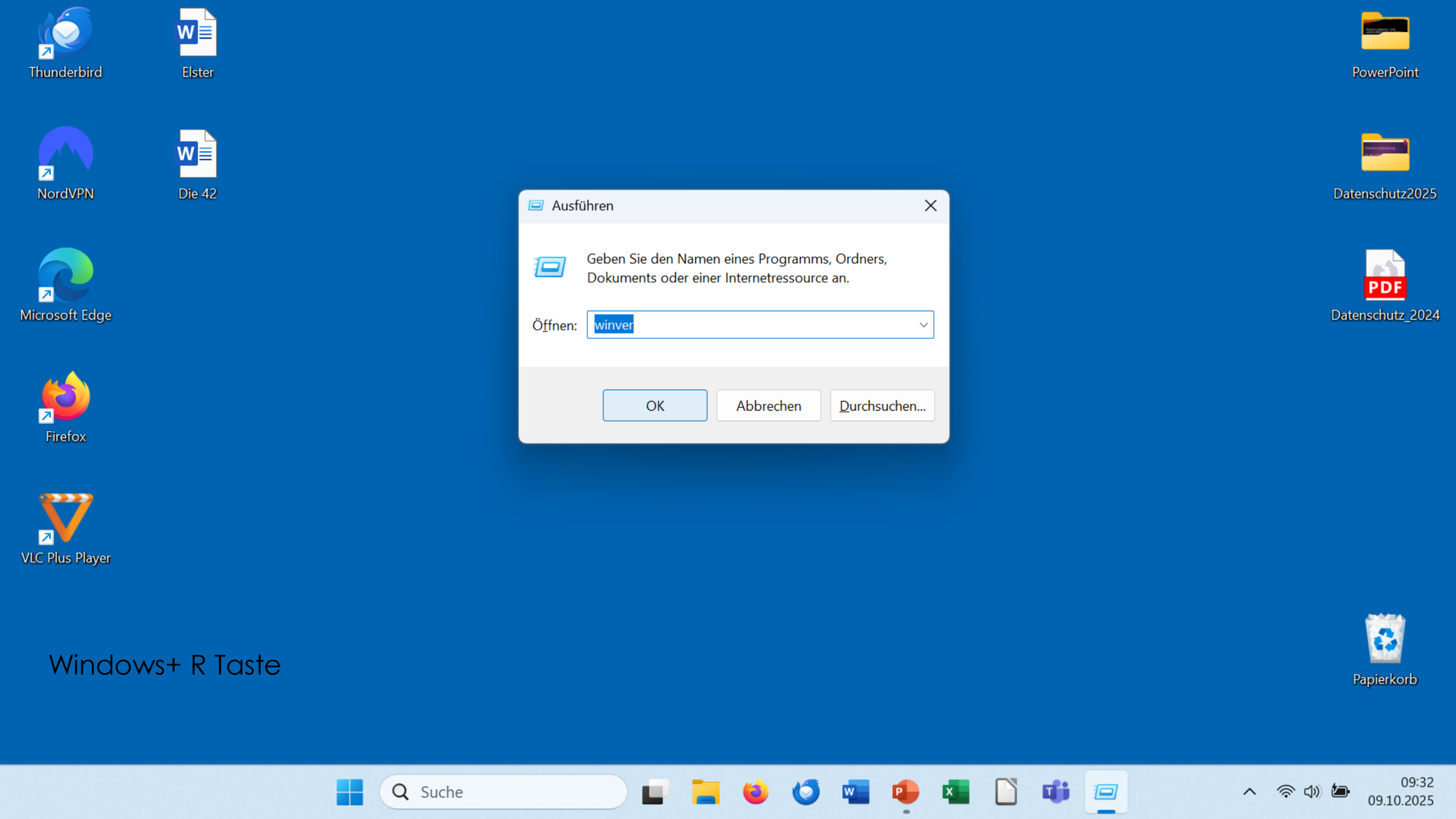
Windows Betriebssystem

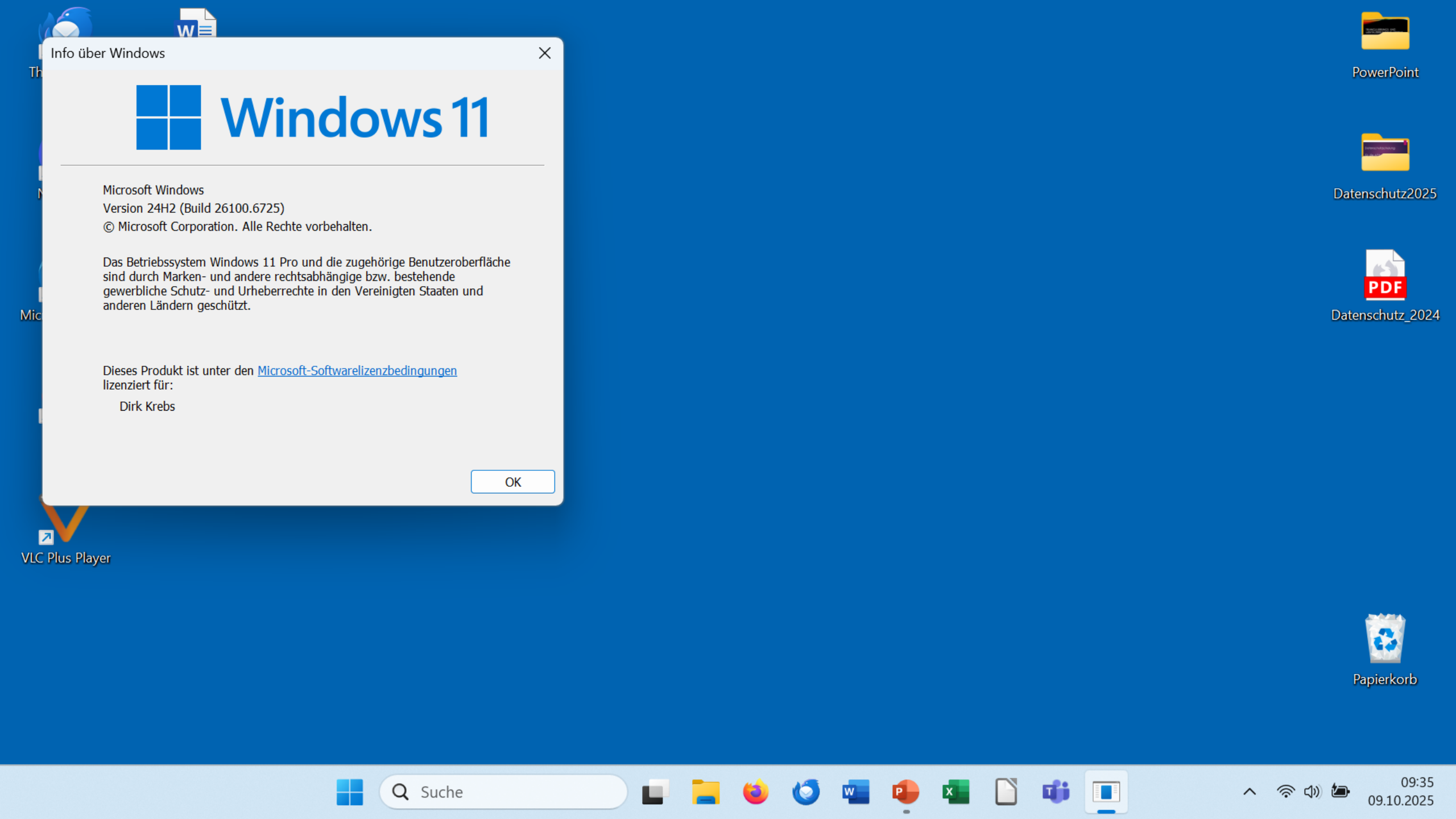
I

1. **Das Betriebssystem:**

   Windows 11 Home ist für Praxen nicht geeignet.

   Windows 11 Pro erfüllt alle Anforderungen der KBV IT-Sicherheitsrichtlinie (April 2025) – von der Verschlüsselung über das Update-Management bis hin zur sicheren Netzwerkanbindung und Dokumentation.


Thunderbird
Elster
PowerPoint
NordVPN
Die 42
Datenschutz2025
Microsoft Edge
Datenschutz_2024
Firefox
VLC Plus Player
Ausführen
Geben Sie den Namen eines Programms, Ordners, Dokuments oder einer Internetressource an.
Öffnen:
winver
OK
Abbrechen
Durchsuchen...
Windows+ R Taste
Papierkorb
Suche
09:32
09.10.2025

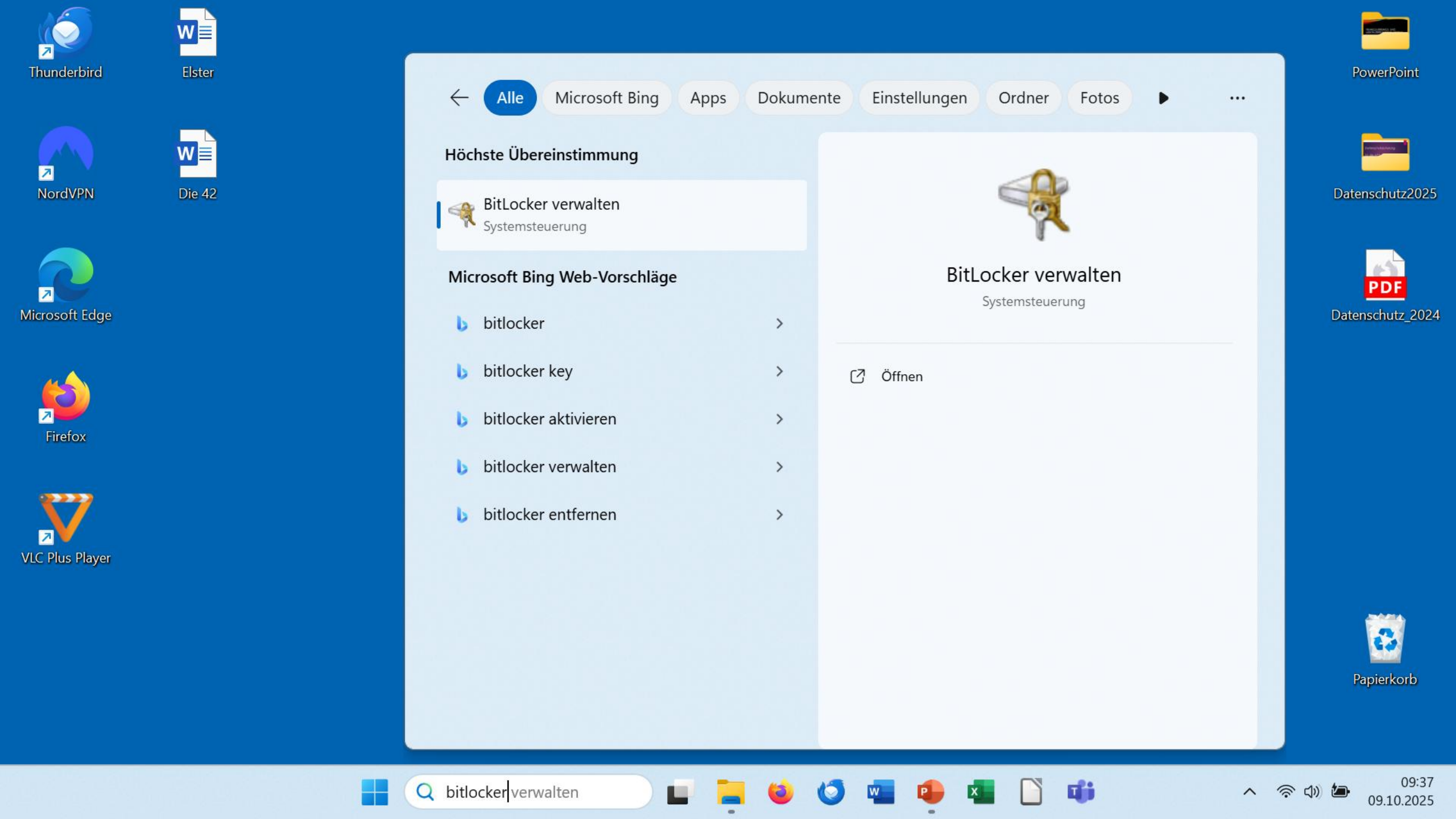

Info über Windows
Windows 11
Microsoft Windows
Version 24H2 (Build 26100.6725)
© Microsoft Corporation. Alle Rechte vorbehalten.
Das Betriebssystem Windows 11 Pro und die zugehörige Benutzeroberfläche sind durch Marken- und andere rechtsabhängige bzw. bestehende gewerbliche Schutz- und Urheberrechte in den Vereinigten Staaten und anderen Ländern geschützt.
Dieses Produkt ist unter den Microsoft-Softwarelizenzbedingungen lizenziert für:
Dirk Krebs
OK
PowerPoint
Datenschutz2025
Datenschutz_2024
VLC Plus Player
Papierkorb
Suche
09:35
09.10.2025

Windows 11 Pro

I

1. Kann die eigene Festplatte und die Wechseldatenträger (externen Festplatten) verschlüsseln (BitLocker)

2. Bietet eine erweiterte Steuerung um Updates gezielt und nachvollziehbar zu installieren


Thunderbird
Elster
PowerPoint
NordVPN
Die 42
Datenschutz2025
Microsoft Edge
Datenschutz_2024
Firefox
VLC Plus Player
Papierkorb
Alle
Microsoft Bing
Apps
Dokumente
Einstellungen
Ordner
Fotos
Höchste Übereinstimmung
BitLocker verwalten
Systemsteuerung
Microsoft Bing Web-Vorschläge
bitlocker
bitlocker key
bitlocker aktivieren
bitlocker verwalten
bitlocker entfernen
BitLocker verwalten
Systemsteuerung
Öffnen
bitlocker verwalten
09:37
09.10.2025

IT-Sicherheitsrichtlinie KBV (seit 2021)
I

- Virenschutzprogramm einsetzen
- Apps nur aus offiziellen App-Stores herunterladen, löschen, wenn nicht mehr benötigt.
- Keine Vertraulichen Daten über Apps versenden
- Computer, Smartphones, Tablets mit komplexen Gerätesperrcode schützen
- Nach Nutzung abmelden / Sperrbildschirm muss installiert sein
- Regelmäßige Datensicherung (Ein Plan muss festlegen, wie oft)
- In Ihrer Praxis werden verschlüsselte Internetanwendungen genutzt. (Achten Sie auf Internetseiten, die mit „https://“ beginnen)

Datensicherung

- Eine Datensicherung sollte, wenn möglich, automatisiert auf eine externe verschlüsselte Festplatte erfolgen
- Für den Fall von z.B. Bränden und Wasserschäden ist es idealerweise sinnvoll das Backup und den Computer nicht am gleichen Ort zu lagern.
- Zwei externe Festplatten, eine zur täglichen Datensicherung in der Praxis, tausch nach einer Woche

IT-Sicherheitsrichtlinie KBV (seit 2021) II

- Wechseldatenträger müssen bei jeder Verwendung auf Schadsoftware überprüft werden.
- Es werden nur Apps genutzt, die Dokumente verschlüsselt und lokal abspeichern.
- Die Administrationsdaten der Telematikinfrastruktur werden sicher aufbewahrt
- Bei Verlust des Diensthandys muss SIM Karte zeitnah gesperrt werden

IT-Sicherheitsrichtlinie KBV (seit 2025)

- Praxispersonal soll bzgl. IT eingewiesen, sensibilisiert, geschult werden.
- Eine Einarbeitung soll stattfinden.
- Endet die Beschäftigung, müssen Passwörter, Zugangsdaten verändert oder vernichtet werden.
- Externes Personal (IT-Dienstleister) muss verpflichtet werden, Gesetze, Vorschriften und interne Reglungen einzuhalten. Bei kurzen Einsatz muss es beaufsichtigt werden.
- Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden
- Es ist geregelt, dass Spam E-Mails ignoriert und gelöscht werden

Einstellung suchen

Dirk Krebs
Lokales Konto

Datenschutz und Sicherheit

App-Berechtigungen

Standort

Kamera

Mikrofon

Stimmaktivierung

Benachrichtigungen

Kontoinformationen

Kontakte

Einstellung suchen

Dirk Krebs
Lokales Konto

Datenschutz und Sicherheit

Sicherheit

Windows-Sicherheit
Antivirensoftware, Browser, Firewall und Netzwerkschutz für Ihr Gerät

Mein Gerät suchen
Verfolgen Sie Ihr Gerät, wenn Sie glauben, dass Sie es verloren haben.

Windows-Berechtigungen

Allgemein
Werbe-ID, lokale Inhalte, App-Starts, Einstellungsvorschläge, Produktivitätstools

Spracherkennung
Online-Spracherkennung für Diktate und andere sprachbasierte Interaktionen

Freihand- und Eingabeanpassung
Benutzerwörterbuch, Wörter in Ihrem Wörterbuch

Diagnose und Feedback
Diagnosedaten, Freihand- und Eingabedaten, maßgeschneiderte Erfahrungen, Feedback-Häufigkeit

Suche
Suchverlauf, Apps durchsuchen, Cloudinhaltssuche, Suchindizierung

Passwortrichtlinie

- Passwörter sind geheim zu halten (nicht in Dateien speichern oder in einer Weise vorhalten, die eine Kenntnisnahme Dritter möglich macht).
- Die Passwörter sind im Hinblick auf ihre Länge und ihre Komplexität entsprechend den Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik (BSI) zu wählen.
- Ein passwortgeschützter Bildschirmschoner ist zu aktivieren. Er muss so konfiguriert sein, dass er nach kurzer Zeit den Zugriff auf das angemeldete Endgerät verhindert. Der Bildschirmschoner ist ggf. manuell zu aktivieren.

Komplexer Code / Komplexes Passwort

In wenigen Schritten zum sicheren Passwort

Sie haben zwei Strategien zur Wahl

Langes und weniger komplexes Passwort

Nutzen Sie ein langes Passwort (mindestens 25 Zeichen), brauchen Sie nur zwei Zeichenarten, z.B. Groß- und Kleinbuchstaben.

Umsetzungsbeispiel: tisch_himmel_kenia_blau_pfannkuchenteig_lachen

Kürzeres und komplexes Passwort

Nutzen Sie ein kurzes Passwort (mindestens acht Zeichen), sollten Sie vier Zeichenarten kombinieren (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen).

Umsetzungsbeispiel: q7yPv8!x§B

www.bsi.bund.de

Organisatorische Maßnahmen zum Schutz der personenbezogenen Daten
Organisatorische Maßnahmen I

- Bewahren Sie Aufzeichnungen über Patienten oder sonstige im Behandlungskontext stehenden Materialien stets verschlossen auf (Zwei-Schranken-Prinzip).
- Patientendaten werden niemals unverschlüsselt über das Internet versendet, beispielsweise per E-Mail.
- Verwenden Sie für die Kommunikation über und mit Patienten nur sichere Kommunikationswege.
- Beachten Sie: öffentlicher W-LAN-Netze sind in der Regel unsicher und ein Einfallstor für Hackerangriffe.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Organisatorische Maßnahmen II

- Zugriffsberechtigungen sind vergeben. Somit ist klar geregelt, wer in der Praxis auf Dateien und Ordner zugreifen kann.
- In den Praxisräumlichkeiten wird auf Diskretion geachtet: Die Anmeldung ist getrennt vom Wartebereich.
- Patientenunterlagen werden so positioniert, dass andere Patienten diese nicht einsehen können. Wenn der Behandler nicht im Raum ist, werden Patientenakten generell unter Verschluss gehalten.

Technische und organisatorische Maßnahmen (TOMS)

zum Schutz der personenbezogenen Daten

Organisatorische Maßnahmen III

- Es ist festgelegt, wann und durch wen personenbezogene Daten gelöscht beziehungsweise vernichtet werden. Patientenakten werden nach DIN-Normen vernichtet.
- Es ist festgelegt, was bei Datenpannen und Datenschutzverstößen zu tun ist und wer die Meldung übernimmt (Meldung in der Regel an die zuständige Aufsichtsbehörde innerhalb von 72 Stunden).
- Die Mitarbeiter in der Praxis wurden über die Einhaltung von Schweigepflicht und Datenschutz informiert.

Wie schützen wir personenbezogene Daten und was machen wir, wenn dies uns nicht gelingt?

1. Wie ist bei einem Datenschutzvorfall vorzugehen?

Datenschutzvorfall

I

- Es besteht eine Meldepflicht innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde.
- Eine Meldepflicht wird indes nicht ausgelöst, wenn voraussichtlich kein Risiko für die Rechte und Freiheiten der betroffenen Patienten besteht, weil Maßnahmen zur Schadenseindämmung nachweisbar ergriffen worden sind.
- Sofern eine meldepflichtige „Datenpanne“ vorliegt, müssen auch die betroffenen Patienten unverzüglich in klarer und einfacher Sprache benachrichtigt werden, wenn ein Risiko für ihre persönlichen Rechte und Freiheiten wahrscheinlich erscheint.
- Eine Benachrichtigung ist entbehrlich, wenn geeignete technisch-organisatorische Maßnahmen (z. B. eine Verschlüsselung) ausschließen, dass ein Schaden für Patienten eintreten kann oder wenn wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden.

Datenschutzvorfall

I

- Eine Verletzung des Schutzes personenbezogener Daten liegt in jeder Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig,

  zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

- Informieren Sie unverzüglich die Person Ihres Ausbildungsinstitutes / Praxis, die für solche Fälle benannt wurde.

Bitte senden Sie dieses Formular umgehend und vollständig ausgefüllt in einer Kopie auch an den Datenschutzbeauftragten. Es dient dem Nachweis gegenüber der Aufsichtsbehörde und erleichtert das Ausfüllen des Meldebogens an die Aufsichtsbehörde

Dr. Thomas Pudelko,
datenschutz@tpudelko.de

1. Detaillierte Sachverhaltsschilderung

2. Wer ist Verantwortlicher?

3. Zeitraum oder Zeitpunkt des Vorfalls

4. Zeitpunkt der Feststellung des Vorfalls

5. Ursache des Vorfalls

6. Ort des Vorfalls

7. Art der Verletzung

8. Kategorien der betroffenen Personen

9. Anzahl der betroffenen Personen / betroffenen

10. Kategorien der personenbezogenen Daten

☐ Gesundheit
☐ Bank- oder Kreditbereich
☐ Religion
☐ Sexualität
☐ Weltanschauung
☐ E-Mail-Adressen
☐ Passwörter
☐ Berufsgeheimnis
☐ Adressen
☐ Biometrie
☐ Standort
☐ Fotos/Videos
☐ Sonstiges
☐ Straftaten oder Ordnungswidrigkeiten

11. Zu welchem Zweck wurden die in Ziffer 10 genannten Daten verarbeitet

12. Wann und wie wurden die betroffenen Personen über den Datenschutzvorfall unterrichtet?

13. Angaben zur Auftragsverarbeitung

Zur Durchführung der Verarbeitungstätigkeit werden Auftragsverarbeiter herangezogen:
☐ Ja ☐ Nein
Falls ja: Benennen Sie die Auftragsverarbeiter

14. Mögliche Folgen und Auswirkungen der Datenschutzverletzung für die betroffenen Personen

☐ Verlust der Kontrolle über ihre personenbezogenen Daten
☐ Einschränkung ihrer Rechte
☐ Diskriminierung,
☐ Identitätsdiebstahl oder -betrug
☐ finanzielle Verluste
☐ unbefugte Aufhebung der Pseudonymisierung
☐ Rufschädigung
☐ Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten
☐ andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person

Ausführliche Beschreibung der möglichen Auswirkungen für die betroffenen Personen:

15. Erläuterung zu eingeleiteten Sicherheitsmaßnahmen bzw. geplanten Sicherheitsmaßnahmen nach dem Datenschutzvorfall, um die betroffenen Personen zu schützen

16. Erläuterung, in wie weit, die eingeleiteten Maßnahmen zu einer Minderung der nachteiligen Folgen für die betroffenen Personen führen

17. Erläuterung zu vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen des Verantwortlichen

Die Daten sind verschlüsselt:
☐ Ja ☐ Nein
Falls ja: Welcher Verschlüsslungsalgorithmus wurde verwendet:

Falls nein: Nennen Sie andere technische und organisatorische Maßnahmen, die zum Schutz der in Ziffer 10 bis 14 genannten Daten ergriffen wurden:

Diesem Meldeformular sind folgende Anlagen beigefügt:
☐ Beschreibung der Verarbeitungstätigkeit aus Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO (Verantwortlicher)

☐ Beschreibung der Verarbeitungstätigkeit aus Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO (Auftragsverarbeiter)

☐ Dokumentation zur Datenschutz-Folgenabschätzung nach Art. 35 DSGVO

Ort, Datum

Vorname und Nachname Unterschrift

Vielen Dank für Ihre Aufmerksamkeit

Verarbeitung Personen-bezogenen Daten

Personen bezogene Daten, wie der Name, das Alter, der Familienstand, das Geburtsdatum, die Anschrift, die Telefonnummer, sowie Gesundheitsdaten*

*(Anamnesen, Diagnosen, Berichte, Befunde, mitbehandelnde Ärzte)

werden mit oder ohne Hilfe automatisierter Verfahren erhoben, erfasst, gespeichert, angepasst, verändert, ausgelesen, abgefragt, verknüpft, verwendet, bereitgestellt, gelöscht oder vernichtet.

Verbotsprinzip mit Erlaubnisvorbehalt

Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten,

… es sei denn, die Datenverarbeitung ist aufgrund einer gesetzlichen Vorschrift zulässig

… oder der Betroffene hat in diese eingewilligt.

Grundlage der Verarbeitung in der Praxis und im Institut

- Die Datenverarbeitung erfolgt aufgrund gesetzlicher Vorgaben, um den Behandlungsvertrag und die damit verbundenen Pflichten zu erfüllen.

- Die Erhebung von Gesundheitsdaten ist Voraussetzung für die Behandlung der Patienten. Werden die notwendigen Informationen nicht bereitgestellt, kann eine sorgfältige Behandlung nicht erfolgen.

Besonderheit
eines Aus- und Weiterbildungs-Instituts

Um die Qualität der Aus- und Weiterbildung
und damit der Therapie zu gewährleisten,

werden Informationen über die Therapiesitzungen
an die Ausbilder/Dozenten weitergegeben.

Dokumentation der Patienteninformation

- Der Patient ist über die Speicherung personenbezogener Daten zum Zwecke der Behandlung zu informieren.
- Ein Hinweis auf den Aushang „Patienteninformation“ genügt.
  Wenn der Patient einen Ausdruck wünscht, sollte dieser über das Sekretariat erhältlich sein.
- In der Patientenakte muss dokumentiert werden, dass der Patient auf die Patienteninformation zum Datenschutz hingewiesen worden ist.

PATIENTENINFORMATION ZUM DATENSCHUTZ

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach der EU-Datenschutz-Grundverordnung (DSGVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck unsere Praxis Daten erhebt, speichert oder weiterleitet. Der Information können Sie auch entnehmen, welche Rechte Sie in puncto Datenschutz haben.

1. VERANTWORTLICHKEIT FÜR DIE DATENVERARBEITUNG

Verantwortlich für die Datenverarbeitung ist das:

John-Rittmeister-Institut

Stresemannplatz 4

24103 Kiel

Telefon: 0431/8886295

sekretariat@john-rittmeister-institut.de

Sie erreichen den zuständigen Datenschutzbeauftragten unter:

Name: Dr. Thomas Pudelko

E-Mail: Datenschutz@t-pudelko.de

2. ZWECK DER DATENVERARBEITUNG

Die Datenverarbeitung erfolgt aufgrund gesetzlicher Vorgaben, um den Behandlungsvertrag zwischen Ihnen und Ihrem Therapeuten bzw. ihrer Therapeutin und die damit verbundenen Pflichten zu erfüllen.

Hierzu verarbeiten wir Ihre personenbezogenen Daten, insbesondere Ihre Gesundheitsdaten. Dazu zählen Anamnesen, Diagnosen, Therapievorschläge und Befunde, die wir oder andere Therapeuten erheben. Zu diesen Zwecken können uns auch andere Ärzte oder Psychotherapeuten, bei denen Sie in Behandlung sind, Daten zur Verfügung stellen (z.B. in Arztbriefen).

Die Erhebung von Gesundheitsdaten ist Voraussetzung für Ihre Behandlung. Werden die notwendigen Informationen nicht bereitgestellt, kann eine sorgfältige Behandlung nicht erfolgen.

In unserem Institut wird die Behandlung hauptsächlich durch Therapeuten in fortgeschrittener Ausbildung (Ausbildung von Psychotherapeuten oder Ärzten) durchgeführt. Um die Qualität von Ausbildung und Therapie zu gewährleisten, werden Informationen über die Therapiesitzungen an die entsprechenden Ausbilder/Dozenten weitergegeben.

3. EMPFÄNGER IHRER DATEN

Wir übermitteln Ihre personenbezogenen Daten nur dann an Dritte, wenn dies gesetzlich erlaubt ist oder Sie eingewilligt haben.

Empfänger Ihrer personenbezogenen Daten können vor allem andere Psychotherapeuten, Ärzte, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Kammern und privatärztliche Verrechnungsstellen sein.

Die Übermittlung erfolgt überwiegend zum Zwecke der Abrechnung der bei Ihnen erbrachten Leistungen, zur Klärung von therapeutischen und sich aus Ihrem Versicherungsverhältnis ergebenden Fragen. Im Einzelfall erfolgt die Übermittlung von Daten an weitere berechtigte Empfänger.

4. SPEICHERUNG IHRER DATEN

Wir bewahren Ihre personenbezogenen Daten nur solange auf, wie dies für die Durchführung der Behandlung erforderlich ist.

Aufgrund rechtlicher Vorgaben sind wir dazu verpflichtet, diese Daten mindestens 10 Jahre nach Abschluss der Behandlung aufzubewahren. Nach anderen Vorschriften können sich längere Aufbewahrungsfristen ergeben, zum Beispiel 30 Jahre.

5. IHRE RECHTE

Sie haben das Recht, über die Sie betreffenden personenbezogenen Daten Auskunft zu erhalten. Auch können Sie die Berichtigung unrichtiger Daten verlangen.

1. Grundlagen
2. Datenschutzziele der Institute / der Praxen
3. Wie schützen und verwahren Sie die Daten ihrer Patienten?
4. Wie ist bei einem Datenschutzvorfall vorzugehen?

Grundsätzliche Datenschutzziele der Institute / Praxen

- Unbedingte Einhaltung der Vorgaben der EU-Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes, institutseigenen Datenschutzvorschriften und des Telemediengesetzes

  durch alle Mitarbeiter, Funktionsträger, Praktikanten, Honorarkräfte, AWT´s, Dozenten, Supervisoren und Lehranalytiker sowie Mitglieder.

- Strikte Verpflichtung zur Geheimhaltung und Vertraulichkeit
- Unbedingter Schutz vor Dateneinsicht durch Unbefugte
- Datenschutzkonforme Arbeitsplatzgestaltung

Konkrete Schutzziele der Institute / Praxen
I

Vertraulichkeit und Datensicherheit sind zu gewährleisten!

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden

und

durch angemessene organisatorische und technische Maßnahmen (TOMs) geschützt werden.

Was soll verhindert werden?

…ein unberechtigten Zugriff,

…eine unrechtmäßige Verarbeitung,

…eine Weitergabe,

…ein versehentlicher Verlust,

…eine Veränderung oder Zerstörung

Konkrete Schutzziele der Institute / Praxen II

- **Rechtevergabe**
  Wo es angezeigt ist, werden Verschlüsselungen, Passwortschutz, Zugriffsrechtevergabe, Zugriffskontrollverfahren und eine Protokollierung administrativer Tätigkeiten durchgeführt.

- **Zeitliche Verfügbarkeit** (Gesicherter Zugriff auf Information innerhalb einer festgelegten Zeit)
  Daten werden immer nur den Mitarbeiter, Funktionsträger, Patienten, Praktikanten, Honorarkräfte, Ausbildungskandidaten, Dozenten, Supervisoren und Lehranalytiker oder Mitglieder zur Verfügung gestellt. Sie haben Zugriff auf diese, wenn die Bearbeitung dieser zu den zugewiesenen Aufgaben gehört. Die zuvor Genannten haben unmittelbar auf alle Prozesse und Daten Zugriff, die sie für die Erledigung ihrer Aufgaben benötigen.

Konkrete Schutzziele der Institute / Praxen III

- **Transparenz**
  Personenbezogene Verfahren sollen mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können. Die Quelle der Daten ist stets nachvollziehbar und jedem Dateninhaber kann innerhalb kurzer Zeit Auskunft über die sie betreffenden Daten gegeben werden.

  Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- die Identität der verantwortlichen Stelle
- den Zweck der Datenverarbeitung
- die hinterlegten Aufbewahrungsfristen
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

Konkrete Schutzziele der Institute / Praxen IV

- **Löschung und Speicherbegrenzung**

  Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden.

- **Nichtverkettbarkeit**

  Personenbezogene Verfahren müssen so eingerichtet sein, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. Die Zweckbindung wird über alle Prozesse eingehalten.

Konkrete Schutzziele der Institute / Praxen V

- **Intervenierbarkeit**
  Personenbezogene Verfahren benötigen Maßnahmen, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen. Neben der Auskunft über die sie betreffenden Daten ist gewährleistet, dass eine Korrektur einer angemahnten falschen Information unverzüglich an allen Stellen des Systems erfolgen kann.

- **Qualitätive Verfügbarkeit**
  Die Arbeit des John-Rittmeister-Instituts stützt sich auf eine reibungslos funktionierende Datenverfügbarkeit. Durch redundante Speichersysteme, Sicherheitskopien, Clustersysteme oder Ausweichzentren ist eine hohe Qualität der Verfügbarkeit gewährleistet.

Konkrete Schutzziele der Institute / Praxen VI

- **Fairness und Rechtmäßigkeit**
  Bei der Verarbeitung personenbezogener Daten muss das informationelle Selbstbestimmungsrecht des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

- **Zweckbindung**
  Daten werden nur für den Zweck ihrer Erhebung verarbeitet und gespeichert. Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

Konkrete Schutzziele der Institute / Praxen VII

- **Sachliche Richtigkeit und Datenaktualität**
  Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

- **Rechenschaftspflicht**
  Die oberste Leitung kann jederzeit die Einhaltung der hier beschriebenen Datenschutzziele nachweisen. Die oberste Leitung kann jederzeit über Datenverarbeitungszwecke, den Verbleib von Daten bei Weitergabe und Löschfristen einzelner Dateninhaber Auskunft geben.

Konkrete Schutzziele der Institute / Praxen VIII

- **Zuständigkeit**
  Im Institut / in der Praxis sind die Aufgaben und Zuständigkeiten hinsichtlich der Erreichung dieser Ziele klar geregelt.

- Es gibt es eine Datenschutzleitlinie die allgemein bekannt ist und deren Umsetzung wird durch Organisationsregeln gewährleistet.