IT-Sicherheit in Rechtsanwaltskanzleien

Handbuch

03.2018

INHALTSVERZEICHNIS

1. Grundsätzliches

Längst ist die Elektronische Datenverarbeitung (EDV) bzw Informationstechnik (IT) in Rechtsanwaltskanzleien zur Selbstverständlichkeit geworden. Mit eindeutig steigender Tendenz, denn die zukünftigen Möglichkeiten, Anforderungen und Wünsche von Klienten bedingen eine stärkere Vernetzung und damit auch einen vermehrten Austausch vertraulicher Daten. Der Elektronische Rechtsverkehr (ERV) ermöglicht eine gesicherte, papierlose Übermittlung von strukturierten und damit weiterverarbeitbaren Daten von Verfahrensbeteiligten zu Gerichten und zurück, aber auch von Rechtsanwälten untereinander. Der ERV ersetzt damit in vielen Bereichen die konventionelle Übermittlung von Dokumenten, verlangt jedoch auch ein erhöhtes Maß an IT-Sicherheitsbewusstsein.

Der sichere Umgang mit Klientendaten ist für Rechtsanwältinnen und Rechtsanwälte nicht nur eine ethische Verpflichtung, sondern auch gesetzlich gefordert. Die einschlägigen Gesetze verpflichten Anwender von Daten iSd § 36 Datenschutzgesetz (DSG 2018) bzw ab 25.5.2018 Art 4 Datenschutz-Grundverordnung (EU-DSGVO) zum Ergreifen wirksamer Maßnahmen zur Gewährleistung der Datensicherheit.

ACHTUNG: Archivium empfiehlt, alle Daten physisch ausschließlich in Österreich zu halten und zu speichern - nur dann ist sichergestellt, dass österreichisches Recht anwendbar ist. Online-Programme, wie zum Beispiel Windows 365 oder Google Docs, die ausschließlich in der Cloud arbeiten, sind nach berufsrechtlichen Vorschriften mangels Garantie, dass die Datenhaltung ausschließlich in Österreich erfolgt, nicht als kompatibel mit § 9 RAO einzustufen. Auch andere häufig verwendete Schreibprogramme und Mobilgeräte speichern in der Cloud. Erkundigen Sie sich auf den Hersteller-Websites, ob und allenfalls wie die Cloud-Speicherung bei diversen Programmen deaktiviert werden kann.

Der Rat der Anwaltschaften (CCBE) hat Richtlinien erstellt, die gegenüber an Cloud-Lösungen interessierten Rechtsanwälten Empfehlungen aussprechen, anhand welcher Kriterien ein geeigneter Cloud-Dienstleister ausgewählt werden kann. Die "CCBE Guidelines on the use of Cloud Computing Services by lawyers" finden Sie auf www.ccbe.eu unter Documents / Documents by theme / IT Law in der Registerkarte “Guides & Recommendations”.

§ 40 Abs 3 RL-BA 2015 normiert, dass ein Rechtsanwalt, der die Dienste eines externen Rechenzentrums in Anspruch nimmt, vertraglich sicherzustellen hat, dass die extern gespeicherten Daten dem gleichen Schutz (Beschlagnahmeschutz) unterliegen wie in der Kanzlei gespeicherte Daten.

Das vorliegende Handbuch behandelt wesentliche Aspekte der Datensicherheit. Mit einfachen Mitteln kann den wesentlichen Sicherheitsanforderungen entsprochen werden. Es ist jedoch ratsam, das Fachwissen eines IT-Dienstleisters hinzuzuziehen.

1.1. Was bedeutet „IT-Sicherheit“?

Die IT in einer Kanzlei ist ein wesentliches und unverzichtbares Werkzeug geworden. Wurde sie einmal eingeführt, ist ein Arbeiten ohne IT nahezu unmöglich, weil in der Regel keine anderen Aufzeichnungen mehr existieren. Informationssicherheit dient dem Schutz vor Gefahren bzw Bedrohungen, der Vermeidung von Schäden und der Minimierung von Risiken. Die wichtigsten Bereiche sind:

- **Betriebssicherheit (Verfügbarkeit)**
  Die IT muss immer funktionieren, sobald sie benötigt wird. Dieses Funktionieren erfordert jedoch Wartungen, Updates und gegebenenfalls Erneuerungen.

- **Datensicherheit (Integrität)**
  Die Daten, die in Ihrer Kanzlei erfasst werden, dürfen nicht verändert werden oder verlorengehen.

- **Vertraulichkeit**
  Ausschließlich jene Personen, die dazu berechtigt sind, dürfen Daten einsehen oder weitergeben.

1.2. Wer oder was beeinflusst die IT-Sicherheit?

- Gesetzliche Regelungen, vor allem die EU-DSGVO und das DSG 2018;

- Erwartungshaltung der Klienten: Werden die Daten in der Kanzlei vertraulich behandelt und aufbewahrt?

- Informationen aus Medien: Welche Trends gibt es? Was machen meine Kolleginnen und Kollegen?

- Angebote von Dienstleistern: Welche Leistungen soll ich einem Dienstleister übertragen? Wie kann ich die Ausführung kontrollieren?

Praxistipps: Was kann ich für die IT-Sicherheit tun?	
√	Informieren Sie sich – zB in diesem Handbuch
√	Besprechen Sie notwendige Schritte mit Ihrem IT-Dienstleister
√	Führen Sie eine IT-Dokumentation (IT-Sicherheitskonzept) und halten Sie diese aktuell

1.3. Rechtliche Grundlagen bezüglich Datensicherheit

Was ist Datenverarbeitung? Welche Informationen dürfen in welcher Form weitergegeben werden? Was verlangt der Gesetzgeber?

Die wesentlichen gesetzlichen Vorschriften zum Thema Datenschutz finden sich im DSG 2000 gültig bis zum 24.5.2018. Danach gelten die EU-DSGVO und das DSG 2018. Auch das Arbeitsrecht ist zu berücksichtigen, wenn es beispielsweise die Regelung der Benutzung des Internets oder der E-Mail-Infrastruktur in der Kanzlei betrifft.

Die Rechtsanwälte sind standesrechtlich zur Verschwiegenheit gemäß § 9 RAO verpflichtet und haben diese Verpflichtungen auf Mitarbeiter und Dienstleister zu überbinden.

1.4. Datenverarbeitung und Datenübermittlung

Die einschlägigen Gesetze verpflichten Anwender von Daten zum Ergreifen von Maßnahmen zur Gewährleistung der Datensicherheit.

Dabei ist sicherzustellen, dass
- die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind,
- ihre Verwendung ordnungsgemäß erfolgt,
- die Daten Unbefugten nicht zugänglich sind.

All das unter Berücksichtigung des Standes der technischen Möglichkeiten und der wirtschaftlichen Vertretbarkeit.

1.5. Erforderliche Maßnahmen

Was bedeutet das konkret? Das DSG 2018 zählt beispielhaft einige erforderliche Maßnahmen auf. Es obliegt jedoch der Verantwortung jedes Anwenders, weitere notwendige Maßnahmen zu treffen, die der Datensicherheit dienen.

Als grundsätzlich wichtige Maßnahmen gelten:

- die Aufgabenverteilung zwischen allen Beteiligten (Rechtsanwältin/Rechtsanwalt, Mitarbeiterinnen/Mitarbeitern) festzulegen, diese schriftlich festzuhalten und die Verwendung von Daten an ebenfalls schriftliche Aufträge zu koppeln

- alle Beteiligten schriftlich über die Datenschutzvorschriften zu belehren, insbesondere die Mitarbeiter zu schulen und dies zu dokumentieren

- die Zutrittsberechtigung zu den Räumlichkeiten der Kanzlei zu regeln

- die Zugriffsberechtigung auf Daten und Programme festzulegen

- Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge nachvollzogen werden können: insbesondere Änderungen, Abfragen und Übermittlungen (Log-Files der Anbieter)

- über alle Maßnahmen eine Dokumentation zu führen. Diese ist wesentlicher Bestandteil eines „IT-Sicherheitskonzeptes“ und eines Datenschutzkonzeptes.

Direkt abgeleitet aus den gesetzlichen Verpflichtungen können insbesondere folgende Maßnahmen werden:

- die Sicherung vor Verlust und Zerstörung (Hardware-Gebrechen, Sabotage, Fehleingaben, etc)

- Vorkehrungen gegen zufällige Ereignisse (Stromausfall, Wasserschaden, Feuer, etc)

- regelmäßige Datensicherung

- Sicherstellung eines reibungslosen und dauerhaften Betriebs der IT in der Kanzlei.

Seit der DSG-Novelle 2010 besteht auch eine Informationsverpflichtung bei Datenmissbrauch (*Data Breach Notification Duty*). **Diese Informationsverpflichtung wird in der ab 25.5.2018 geltenden EU-DSGVO noch wesentlich verschärft.** Auch die Information der Datenschutzbehörde durch den Verantwortlichen hat innerhalb von 72 Stunden zu erfolgen.

Eine mangelnde IT-Sicherheit in einer Rechtsanwaltsgesellschaft kann auch zu einer Verantwortlichkeit nach dem Verbandsverantwortlichkeitsgesetz führen, welches die strafrechtliche Verantwortung juristischer Personen normiert. Dieses kommt zur Anwendung, wenn eine Straftat zugunsten der Rechtsanwaltskanzlei begangen wurde oder wenn bestimmte Sorgfaltspflichten (Verbandspflichten) verletzt wurden, zB dann, wenn eine Mitarbeiterin oder ein Mitarbeiter einer Rechtsanwaltsgesellschaft unter Ausnutzung der IT-Infrastruktur eine Straftat begeht, weil die Rechtsanwaltskanzlei die gebotenen Maßnahmen zur Vorbeugung nicht gesetzt hat.

Praxistipps	
√	Verschriftlichen Sie alle Vorgänge
√	Berücksichtigen Sie die Prinzipien eines umfassenden IT-Sicherheitsmanagements
√	Erstellen Sie ein IT-Sicherheitskonzept – siehe dazu Kapitel „IT-Sicherheitskonzept“

2. Das IT-Sicherheitsmanagement

Zur Gewährleistung von IT-Sicherheit bedarf es eines kontinuierlichen Prozesses, dessen Strategien und Konzepte ständig auf seine Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen sind.

Dieser Prozess kann keine 100%-ige Sicherheit garantieren, bei Berücksichtigung der wesentlichen Aspekte kann jedoch das Risiko auf ein akzeptierbares Maß reduziert werden. Es muss auch bedacht werden, dass Sicherheit „kostet“, sowohl Geld als auch Zeit und Bequemlichkeit, zB durch zusätzliche Sicherheitsschritte.

Zentrale und wesentliche Elemente eines IT-Sicherheitsmanagements sind:

- Durchführung einer Risikoanalyse
- Erstellung eines IT-Sicherheitskonzeptes auf Basis der Risikoanalyse
- Umsetzung des IT-Sicherheitskonzeptes
- Kontrolle des IT-Sicherheitskonzeptes und Anpassung

2.1. Die Risikoanalyse

Durch den Einsatz immer komplexerer IT-Systeme in einer Kanzlei entstehen Risiken, die wie andere unternehmerische Risiken in eine umfassende Risikoanalyse einfließen sollten.

In einem ersten Schritt sollten die Unternehmenswerte in Zusammenhang mit IT festgestellt und bewertet werden (Wertanalyse).

- Welche IT-Systeme werden verwendet?
- Welche Unternehmenswerte (bspw Server, PC, Infrastruktur, Lizenzen, Informationen) habe ich im IT-Bereich?

Die Identifikation von möglichen Bedrohungen und die Ermittlung einer Eintrittswahrscheinlichkeit stellt den nächsten Schritt dar (Bedrohungsanalyse). Bedrohungen können aufgrund technischer Probleme (bspw Hardware-Ausfälle) sowie organisatorischer Mängel (bspw mangelnde Schulungen) entstehen oder durch fahrlässige (bspw Bedienungsfehler) bzw vorsätzliche Handlungen (bspw Datendiebstahl) herbeigeführt werden. Höhere Gewalt ist ebenfalls zu berücksichtigen.

- Welche Schäden können bei diesen Unternehmenswerten eintreten?
- Wie wahrscheinlich ist das Eintreten des Schadensfalls und welche Folgen hat dieser für meine Kanzlei?

Eine Bedrohung kann nur durch die Ausnutzung einer vorhandenen Schwachstelle wirksam werden. Es ist daher erforderlich, mögliche Schwachstellen des Systems zu identifizieren und ihre Bedeutung zu klassifizieren (Schwachstellenanalyse).

- Welche Schwachstellen in meiner Kanzlei könnten den Schadensfall unterstützen?
- Welche Maßnahmen wären geeignet, diese Schwachstellen zu beseitigen?

Sind Bedrohungen und Schwachstellen bekannt, sollte im Zuge einer Risikobewertung eine Priorisierung von Maßnahmen erfolgen.

- Welche Maßnahmen muss ich zuerst treffen, für welche habe ich mehr Zeit?

2.2. Das IT-Sicherheitskonzept ist Teil des Datenschutzmanagements

Auf Basis der durchgeführten Risikoanalyse sollten entsprechende Maßnahmen gesetzt werden, die das Risiko auf ein akzeptables Maß reduzieren, denn wie bereits erwähnt, eine 100%-ige Sicherheit besteht niemals.

Die gesamte Dokumentation der getroffenen IT-Sicherheitsmaßnahmen wird in unserem Zusammenhang als IT-Sicherheitskonzept bezeichnet.

Man kann die getroffenen Maßnahmen wie folgt klassifizieren:

- (informations-)technische Maßnahmen (zB Zugriffskontrollen, Berechtigungskonzepte)
- bauliche Maßnahmen (zB Zugangskontrollen, Einbruchsschutz)
- organisatorische Maßnahmen (zB klare Verantwortlichkeiten, Richtlinien)
- personelle Maßnahmen (zB Sensibilisierungen, Schulungen).

Nur ein Zusammenspiel dieser verschiedenen Maßnahmen kann ein ausreichendes Maß an Sicherheit gewährleisten. Verlässt man sich zu sehr auf technische Lösungen, kann das Risiko durch andere Schwachstellen (zB mangelnde bauliche Sicherungsmaßnahmen, unzureichendes Rechtekonzept, etc) weiterbestehen.

Mit dem IT-Sicherheitskonzept können Sie im Anlassfall nachweisen, dass Sie „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung […] geeignete technische und organisatorische Maßnahmen“ (§ 54 DSG 2018 bzw Art 32 EU-DSGVO) getroffen haben.

Diese Dokumentation dient daher Ihrem Schutz und der Sicherheit Ihrer Mitarbeiter!

2.2.1. So kommen Sie zu einem IT-Sicherheitskonzept

Als ersten Schritt sollten Sie alle relevanten Dokumente sammeln und diese an einem Ort (in einem Ordner) sicher aufbewahren. **Wichtig:** Alle Dokumente sind immer auf dem aktuellen Stand zu halten!

2.2.2. Kontrolle des IT-Sicherheitskonzepts

Praxistipps	
√	Sammeln Sie alle relevanten Dokumente
√	Überprüfen Sie laufend die Unterlagen auf Vollständigkeit und Aktualität
√	Führen Sie in regelmäßigen Abständen bzw im Anlassfall eine Überprüfung Ihres IT-Sicherheitskonzepts durch

3. Organisation, physischer Schutz, Regelung mit Mitarbeitern

3.1. Datenschutz ist mehr als EDV-Sicherheit

Datensicherheit beginnt nicht erst beim Einsatz eines IT-Systems. Viele grundlegende Prozesse in einer Kanzlei haben nichts mit der IT zu tun, trotzdem geht es dabei um Daten. Gerade in diesem Bereich können meist ohne großen Aufwand wesentliche Verbesserungen erzielt und damit die Datensicherheit deutlich erhöht werden.

3.2. Örtliche Gegebenheiten

Stellen Sie sicher, dass betriebsfremde Personen (Klienten, Dienstleister, etc) nicht versehentlich oder absichtlich Daten einsehen können:

- Drehen Sie PC-Monitore so, dass nur Sie und Ihre Mitarbeiter die Daten einsehen können
- Benutzen Sie Bildschirmschoner, die sich nach kurzer Zeit einschalten
- Behandeln Sie Ausdrucke und ankommende Faxe sorgfältig und lassen Sie diese nicht unbeaufsichtigt liegen
- Gestalten Sie den Anmelde-/Rezeptionsbereich so, dass die dort geführten Gespräche vertraulich bleiben
- Minimieren Sie im täglichen Arbeitsablauf die Möglichkeiten zur Einsichtnahme in fremde Daten.

3.3. Physischer Zugriff auf Daten

- Halten Sie Ihre Daten verschlossen:
  - Server in einen eigenen, absperrbaren Raum stellen; steht kein abgeschlossener Bereich zur Verfügung, sollten PC und Datenserver durch andere geeignete Maßnahmen gegen Diebstahl gesichert werden, zB durch spezielle Kabelbefestigungen oder verschweißte Computer-Gehäuse („Cases“)
- Stellen Sie sicher, dass betriebsfremde Personen keinen Zugriff auf Ihre Rechner haben (zB kleben Sie nicht das Passwort für den Arbeitsplatz auf den PC-Bildschirm)
- Versperren Sie Ihre Datensicherungsmedien, um Missbrauch zu verhindern
- Vergessen Sie nicht auf Daten in Papierform wie Faxe, Briefe oder Formulare – auch diese sollten nicht von unbefugten Personen gelesen werden können (Vorsicht bei der Altpapierentsorgung!).

3.4. Verträge mit Mitarbeitern und Dienstleistern

Die gesetzlichen Verpflichtungen schreiben vor, dass datenschutzrechtliche Auftraggeber sowie Dienstleister und ihre Mitarbeiter alle Daten aus Datenanwendungen, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut oder zugänglich wurden, geheim zu halten haben. Zusätzlich müssen Sie als Kanzleiinhaber festlegen, welche Mitarbeiterinnen und Mitarbeiter auf welche Daten Zugriff haben dürfen. Es empfiehlt sich, nur den unbedingt notwendigen Datenzugriff zu gestatten.

Die Vereinbarungen über Datenzugriff, die Belehrungen über die Verschwiegenheits- und andere Pflichten dokumentieren Sie am besten durch nachweisliche Unterfertigung einer ausgehändigten Vorlage der gesetzlichen Bestimmung.

Im ÖRAK-Mitgliederbereich finden Sie eine Musterbelehrung zur Verschwiegenheitsverpflichtung von Angestellten, Lehrlingen und sonstigen Mitarbeitern bei Rechtsanwälten unter Service / IT-Sicherheit/Datenschutz.

Praxistipps:	
√	Gestalten Sie Ihre Kanzlei und den täglichen Ablauf so, dass möglichst wenig Gelegenheit zur Dateneinsicht entstehen kann
√	Sorgen Sie auch ohne IT für Datenschutz
√	Belehren Sie Ihre Mitarbeiterinnen und Mitarbeiter ausführlich und schriftlich

3.5. Software und IT-Sicherheit

Fast jede Kanzlei setzt eine (Kanzlei-)Software ein. Diese dient hauptsächlich der administrativen Verwaltung der Kanzlei. Aus Sicht der IT-Sicherheit stehen im Folgenden nicht die benötigten Funktionalitäten im Vordergrund, sondern der sichere Umgang mit Daten.

Erforderlich ist selbstverständlich ein „personalisiertes Login“, das auch konsequent verwendet werden muss: Jeder Benutzer hat sich mit einem persönlichen Kennwort der Kanzlei-Software gegenüber zu identifizieren, nur so kann die Software die Berechtigungen der einzelnen Benutzer verwalten und den Zugriff freigeben. Auf eine ausreichende Passwortqualität ist zu achten. Es sollten sowohl Buchstaben als auch Ziffern verwendet werden. Die Verwendung von Sonderzeichen erhöht die Passwortqualität beträchtlich. Empfohlen ist bei normalen Anwendern eine Passwortlänge von mindestens 8 Zeichen, im Falle von besonderen Rechten (bspw Administrator) sollte ein Passwort mindestens 12 Zeichen lang sein. Nicht geeignet als Passwörter sind bspw Namen, Geburtsdaten oder Trivialpasswörter (123456, qwertz, aaaaaa). Es ist dringend anzuraten, bei unterschiedlichen Anwendungen auch unterschiedliche Passwörter zu verwenden. Passwörter müssen in regelmäßigen Abständen geändert werden.

Verwenden wir zur Veranschaulichung ein kleines Beispiel. Im Internet kann man sich leicht Software für „Brute-Force“-Attacken herunterladen. Diese Software probiert selbständig alle möglichen Zeichenkombinationen aus. Verwendet man nun bspw ein Passwort aus 6 Kleinbuchstaben, ergibt dies eine theoretische Möglichkeit von ca 300 Millionen Kombinationen (308.915.776 um genau zu sein). Hört sich im ersten Moment sehr viel an. Ein handelsüblicher Prozessor schafft jedoch mehr als 40 Millionen Anschläge pro Sekunde. Dies bedeutet für unser Passwortbeispiel maximal 7,5 Sekunden, bis unsere Hürde überwunden wird. Automatische Sperren von Benutzern bei wiederholt falscher Passworteingabe können dieser Art des Angriffes entgegenwirken.

3.6. Dokumentation für den Ernstfall

Außerdem ist von der Software Protokoll über die tatsächlich durchgeführten Verwendungsvorgänge zu führen. Es muss für den Datenverantwortlichen (idR der Inhaber der Kanzlei) jederzeit ersichtlich sein, welcher Mitarbeiter auf welche Weise (lesen, schreiben, ändern) auf welche Daten zugegriffen hat. Diese Dokumentation ist vor allem bei mutmaßlichen Verletzungen des Datenschutzes von Bedeutung, weil bei einem Gerichtsverfahren derartige Aufzeichnungen als Beweise vorgelegt werden müssen.

Grundsätzlich haben Sie zur Abwehr von Schadenersatzansprüchen die Protokoll- und Dokumentationsdaten **entsprechend der gesetzlichen Verjährungsfristen aufzubewahren.**

3.7. Erwünschter Datenzugriff von außen

Durch den Fortschritt der Technik ist es vielfach bereits möglich, dass auf die Kanzlei-Software von außen zugegriffen wird. Das ist zB im Falle eines zweiten Standortes oder für Arbeiten im privaten Umfeld sehr praktisch, auch die Betreuer der Kanzlei-Software greifen oftmalig per Fernwartung auf diese zu. Der Zugriff kanzleifremder Personen (Hard- und Softwarebetreuung, EDV-Dienstleister, etc) ist jedenfalls vertraglich zu regeln, Dritte müssen schriftlich die Einhaltung des Datenschutzes garantieren. Für alle Fernzugriffe ist die technische Sicherheit, der Schutz vor unbefugtem Zugriff, zu garantieren, alle Maßnahmen sind zu dokumentieren.

Stellen Sie sich vor …

Sie kommen Montagfrüh in Ihre Kanzlei, ein arbeitsreicher Tag erwartet Sie. Sie versuchen, Ihre EDV einzuschalten – leider ohne Erfolg. Der Server startet nicht, Sie haben keinen Zugriff auf Ihre Daten.

Was tun Sie? Zusperren? Alles manuell schreiben und nachtragen? Bereiten Sie also am besten möglichst bald für solche Fälle einen Notfallplan vor:

- Wo können Sie Ersatz-Hardware organisieren?
- Gibt es Garantien, Wartungsverträge?
- Wer installiert die Software auf der neuen Hardware?
- Ist der IT-Dienstleister schnell genug verfügbar?
- Sind Passwörter, Codes, Lizenzen verfügbar?
- Haben Sie die Notrufnummern ihrer Dienstleister?
- Wurden Reaktionszeiten vertraglich geregelt?

Für jede Kanzlei sind die Daten in der Kanzlei-Software als äußerst wichtig einzustufen, meistens ist eine Arbeit ohne entsprechende Software kaum noch vorstellbar. Daher ist die Sicherung dieser Daten eine unerlässliche Maßnahme, die jeden Tag durchgeführt werden muss. Die Datensicherung besteht im Wesentlichen in einer Kopie der Daten auf externen Medien (zB Festplatte, Band, USB-Stick), wobei Sie folgende Punkte sicherstellen müssen:

- Sichern Sie alle Daten, die für einen reibungslosen Betrieb notwendig sind, auch Konfigurationsdateien, Mail und notwendige Software

- Prüfen Sie die Korrektheit der Sicherung. Kann man alle Daten aus der Sicherung wiederherstellen, ist Ihr System nach einer Wiederherstellung vollständig benutzbar?

- Sollten Sie dies nicht selbst durchführen können, beauftragen Sie Ihren IT-Dienstleister damit und lassen Sie sich das Ergebnis schriftlich bestätigen – damit haftet der Dienstleister auch für die Korrektheit der Sicherung

- Sollten der Kanzlei-Software-Hersteller und der IT-Dienstleister unterschiedliche Firmen sein, legen Sie eine eindeutige Verantwortung für Sicherung und Wiederherstellung fest.

Verwehren Sie Unbefugten den Zugriff auf die Sicherungen. Dies kann durch Datenverschlüsselung oder durch sichere physische Verwahrung (Safe) geschehen. Verteilen Sie die Sicherung auf mehrere Orte. Nach einem Brand oder Wasserschaden können alle in der Kanzlei gelagerten Sicherungskopien unbrauchbar sein.

Praxistipps	
√	Stellen Sie sicher, dass Ihre Kanzlei-Software dem Datenschutzgesetz entspricht
√	Sichern Sie Ihre Daten und überprüfen Sie die Wiederherstellbarkeit
√	Lassen Sie sich schriftlich die Korrektheit der Sicherung Ihrer Daten von externen Dienstleistern bestätigen

3.8. Betriebssystem und Browser

3.8.1. Wie neu muss eine IT sein?

IT-Systeme sind heute üblicherweise mit anderen IT-Systemen verbunden, entweder lokal (Stationen, Server) oder global (Internet). Die Kommunikation mit anderen Systemen sollte deshalb sicher gestaltet werden. Die für die IT-Sicherheit relevanten Teile der gesamten IT-Ausrüstung sind das Betriebssystem, der Browser und die Kanzlei-Software.

3.8.2. Das Betriebssystem

Das Betriebssystem ist die Software, die zwischen Hardware und Anwendungsprogrammen vermittelt und die grundlegenden Funktionen der Hardware für andere Softwareteile verfügbar macht. Es ist das wohl komplexeste Softwareprodukt auf Ihrem Rechner und dementsprechend anfällig für Fehler und Sicherheitslücken.

Die Hersteller liefern über eine bestimmte Frist „Updates“ für das Betriebssystem:

- Funktionelle Updates: Neue Funktionen werden bereitgestellt, Fehler werden ausgebessert („Mainstream Support“)

- Sicherheits-Updates: Sicherheitslücken werden geschlossen („Extended Support“), jedoch keine Funktionsverbesserungen mehr durchgeführt

Für einen sicheren Betrieb ist es wichtig, dass der Hersteller regelmäßig Sicherheits-Updates ausliefert und damit eventuell auftretende Sicherheitslücken kurzfristig repariert werden.

Von der Arbeit mit einem Betriebssystem, dessen Support eingestellt wurde, ist abzuraten.

3.8.3. Der Browser

Der Browser ist unter Sicherheitsaspekten die wichtigste Komponente des Betriebssystems. Er wird für die Internet-Kommunikation verwendet und ist daher das „Gesicht“ des Rechners zum Internet. Auch zahlreiche Drittprogramme (auch Kanzlei-Software) verwenden unsichtbar den Browser, um die Kommunikation (zB mit dem Internet) abzuwickeln. Wie beim Betriebssystem ist es wichtig, dass der Browser durch den Hersteller aktuell gehalten wird, denn allfällige Sicherheitslücken im Browser werden – zB von Hackern – besonders schnell ausgenützt.

Ein aktueller Browser ist unerlässlich, um Webseiten anzeigen zu können, die besondere „Usability“ und Komfort bieten. Denn dabei werden Technologien verwendet (zB HTML5), die in älteren Browsern nicht unterstützt werden. Es sollte daher darauf geachtet werden, dass Browser regelmäßig upgedatet werden.

3.9. Die Kanzleisoftware

Praxistipps	
√	Ein Betriebssystem verwenden, das mit Sicherheitsupdates versorgt wird
√	Einen Browser verwenden, der mit Sicherheitsupdates versorgt wird
√	Bei Internetzugriff einen Virenschutz verwenden
√	Alle von den Herstellern angebotenen Updates einspielen
√	Nachdem diese Maßnahmen tief in die Funktionalität Ihres IT-Systems eingreifen, ändern Sie die Ausgangskonfiguration nur im Einvernehmen mit Ihrer IT-Betreuung
√	Bitte treffen Sie endgültige Entscheidungen bei neuen Investitionen nur in Absprache und im Einvernehmen mit Ihrem betreuenden IT-Dienstleister

4. Weniger bekannte Aspekte der IT-Sicherheit

4.1. Fernwartung

Üblicherweise wird Ihr IT-System durch IT-Dienstleister gewartet und betreut. Diese Wartung kann persönlich, per Datenträger oder per Fernwartung ausgeführt werden. Fernwartung bedeutet in diesem Zusammenhang, dass betriebsfremde Personen über elektronische Netze (Internet) Zugriff auf das IT-System in Ihrer Kanzlei haben und zB Wartungsarbeiten durchführen können. Sie sollten wissen, dass der Zugriff per Fernwartung ein Vollzugriff ist, der grundsätzlich auch den Zugriff auf die Klientendaten ermöglicht.

Grundsätzlich soll bei einer Fernwartung darauf geachtet werden, dass die Initiative zur Fernwartung immer vom Kanzleimitarbeiter ausgehen muss. Die Fernwartungsverbindung muss verschlüsselt sein.

Die Durchführung der Fernwartung soll protokolliert werden (Beginn, Abschluss, Beteiligte, allenfalls die durchgeführten Tätigkeiten).

4.2. Daten an Dritte

Geben Sie Daten an Dritte (Backupdienstleister, Firmen die statistische Datenauswertung betreiben, oä) weiter, so setzt Ihnen das DSG 2018 und die EU-DSGVO enge Grenzen. Ein Backup-Dienstleister ist jemand, bei dem Sie eine oder mehrere Datenkopien ablegen können, meistens in verschlüsselter Form. Üblicherweise findet die Datenübertragung über Internet verschlüsselt und automatisiert statt. Ein Backupdienstleister ist wie ein IT-Dienstleister zu sehen und es sind die entsprechenden **Verträge unter Einhaltung der EU-DSGVO-Vorschriften** mit ihm abzuschließen.

4.3. E-Mails, externe Datenträger

Öffnen Sie keine dubiosen E-Mails. Schadprogramme verstecken sich oft in Grafiken oder E-Mail-Anhängen.

Sofern kein verschlüsselter Nachrichtenverkehr eingerichtet wird, soll vom Mandanten eine Einverständniserklärung eingeholt werden, dass dieser mit der Verwendung von (unsicheren) E-Mails ausdrücklich einverstanden ist.

Vor der Nutzung von Mandanten-CDs oder USB-Sticks soll der externe Datenträger auf Viren geprüft werden.

4.4. WLAN, Bluetooth, Mobilfunk, VPN

Denken Sie bei der Absicherung Ihres IT-Systems auch an drahtlose Netzwerke. Diese bringen zwar ein Plus an Bequemlichkeit, eröffnen allerdings Personen ohne physische Anwesenheit die Möglichkeit, auf Ihre Daten zuzugreifen.

Ein WLAN (Wireless Local Area Network) ermöglicht Datenübertragung per Funk, Der typische Einsatz von WLAN erfolgt bei Notebooks, Tablets, Smartphones oder Spielkonsolen. Sichern Sie WLAN-Netze immer mit der aktuellsten Technologie ab, verwenden Sie „starke Passwörter“ und wechseln Sie diese regelmäßig. Schalten Sie das WLAN ab, sobald Sie es nicht benötigen.

Bluetooth ermöglicht Funk-Kommunikation mit geringer Reichweite. Es wird typischerweise bei Headsets (Kopfhörern) eingesetzt. Sollten Sie Bluetooth nicht benötigen, deaktivieren Sie es.

Falls Sie Mobilfunk einsetzen, verwenden Sie für den Datenzugriff ein Virtual Private Network (VPN), eine verschlüsselte Datenverbindung über das Internet.

4.5. Sichere Netze

Neben der Behandlung der Daten selbst – Fälschungssicherheit durch Signierung, Verwehren unbefugter Einsicht durch Verschlüsselung – kann auch der Übertragungsweg abgesichert werden. Mittels elektronischer Verfahren (VPN, Kanaltrennung, etc) werden Datenströme getrennt geführt. Dadurch kann die Möglichkeit minimiert bzw ausgeschaltet werden, überhaupt die Leitung „anzuzapfen“ und damit Daten abrufen zu können.

4.6. Datensicherheit bei Tablet, Smartphone & Co

Achtung vor nicht-offiziellen Apps! Datensicherheit bei Tablets, Smartphones und Co sowie bei Sozialen Netzwerken ist derzeit leider nicht gegeben.

4.7. Datenlöschung, Datenvernichtung

Neben den angesprochenen Fristen für die Archivierung verpflichtet das DSG 2018 und die EU-DSGVO zur Löschung der Daten nach dem Datenschutzkonzept und der mitgeteilten Frist bzw dem gerechtfertigten Zweck der Aufbewahrung (zb Abwehr von Haftungsansprüchen).

Bei der Löschung bzw Vernichtung von Daten, sowohl in elektronischer als auch in Papierform, sind gewisse Grundsätze zu beachten, die eine unbeabsichtigte Wiederherstellung der Daten vermeiden sollen.

Einfaches Löschen von elektronischen Daten, bspw in Windows durch Verschieben in den Papierkorb, ist keine permanente Datenlöschung. Sollten Datenspeicher wie zB Festplatten getauscht werden, sind diese vor dem Ausscheiden mit einer entsprechenden Software zu überschreiben.

Praxistipps:	
√	Schließen Sie mit allen Dienstleistern, die Zugriff auf Ihr System haben, entsprechende Dienstleistungsverträge ab, die auch die Verschwiegenheitspflicht nach DSG 2018 und EU-DSGVO beinhalten
√	Stellen Sie sicher, dass bei Datenweitergabe an Dritte alle gesetzlich vorgesehenen Maßnahmen eingehalten werden und lassen Sie sich diese Einhaltung schriftlich bestätigen
√	Regeln Sie die Behandlung von Papierdokumenten schriftlich in den Verträgen mit Ihren Mitarbeitern
√	Setzen Sie drahtlose Netzwerke nur dann ein, falls Sie sie unbedingt benötigen. Sie stellen eine kaum zu kontrollierende Möglichkeit dar, auf Kanzleidaten zuzugreifen
√	Der Zugriff von mobilen Geräten auf Kanzleidaten ist derzeit als potentiell unsicher zu bewerten
√	Nur bewährte Methoden zur Datenübertragung verwenden
√	Vom Anbieter Datenschutzerklärungen nach EU-DSGVO verlangen
√	Niemals Daten per E-Mail versenden

5. 12 Anregungen zur Datensicherheit

1) **Physischer Schutz:** Stellen Sie sicher, dass betriebsfremde Personen keine Daten einsehen können. Beschränken und kontrollieren Sie den Zutritt, beschränken Sie absichtliche oder versehentliche Einblicke, schützen Sie die Bereiche, in denen mit Daten gearbeitet wird. Sehen Sie einen Einbruchs- und Diebstahlschutz vor.

2) **Mitarbeiter:** Weisen Sie auf die Geheimhaltungspflicht in den Dienstverträgen hin. Legen Sie in einem Schriftstück für jeden Mitarbeiter fest, welche Dateneinsicht jeder Mitarbeiter benötigt.

3) **Rechner/Betriebssystem:** Benutzen Sie ein Betriebssystem, das mit Sicherheitsupdates versorgt wird, einen aktuellen Browser sowie einen aktuellen Virenschutz. Falls Sie auf das Internet zugreifen, aktivieren Sie eine Software-Firewall.

4) **Software:** Überprüfen Sie, ob eine Mitarbeiterverwaltung mit persönlichem Login unterstützt wird, fordern Sie eine starke Passwortqualität. Beschränken Sie die Zugriffe Ihrer Mitarbeiter auf die notwendigen Daten und stellen Sie sicher, dass die tatsächlichen Datenzugriffe protokolliert werden.

5) **Datensicherung:** Sichern Sie regelmäßig alle wesentlichen Daten Ihres IT-Systems. Bewahren Sie die Sicherungsmedien extern oder an einem geschützten Ort (Safe) auf. Kontrollieren Sie periodisch die Qualität der Medien und prüfen Sie die Wiederherstellbarkeit Ihres Systems. Treffen Sie Vorkehrungen für einen Softwarewechsel oder die Beendigung Ihrer Tätigkeit (Aufbewahrungspflichten).

6) **Daten übertragen:** Übertragen Sie personenbezogene Daten nur über gesicherte Medien oder (unter den gesetzlich vorgesehenen Auflagen) per Fax. Verwenden Sie keinesfalls E-Mail!

7) **Dienstleisterverträge:** Stellen Sie die Geheimhaltungsverpflichtung schriftlich sicher. Regeln Sie die Möglichkeiten der Fernwartung und den Zugriff auf Daten oder Sicherungsmedien. Vermeiden Sie unbeschränkte Fernwartungszugänge.

8) **Reparatur, Entsorgung:** Geben Sie Datenträger nur ohne Daten an Dritte weiter, zerstören Sie gegebenenfalls selbst die Festplatten. Denken Sie an den Inhalt von Sicherungsmedien. Fordern Sie von dem Dienstleister eine schriftliche Bestätigung der Einhaltung des Datenschutzes.

9) **Persönliches Verhalten:** Gehen Sie mit den neuen Medien und Möglichkeiten kritisch um: Öffnen Sie keine E-Mails von unbekannten Personen, misstrauen Sie Gratisversprechungen, geben Sie keine vertraulichen Daten bekannt. Keine Bank oder Kreditkartenfirma wird von Ihnen per E-Mail Informationen einholen!

10) **Neue Gefahren bedenken:** Sichern Sie ein verwendetes WLAN nach dem Stand der Technik ab. Denken Sie an Daten auf mobilen Geräten (Notebook, Tablet, Smartphone), insbesondere bei Weitergabe und Diebstahl. Externe Zugriffe auf die Kanzleidaten sind entsprechend zu sichern.

11) **Regelmäßige Überprüfungen:** Die aktuelle Technik und die damit verbundenen Möglichkeiten und Gefahren schreiten rasant voran. Bedenken Sie bei allen Konfigurationsänderungen die IT-Sicherheit mit und dokumentieren Sie alle wesentlichen Vorgänge. Aktualisieren Sie in regelmäßigen Abständen Ihr IT-Sicherheitskonzept.

12) **Einverständniserklärung E-Mails:** Holen Sie eine Einverständniserklärung für unsichere E-Mail-Kommunikation von Ihrem Klienten ein.