DATENSICHERHEIT & IT-SECURITY IN ANWALTSKANZLEIEN

Die Österreichischen
Rechtsanwältinnen
und Rechtsanwälte

DATENSICHERHEIT & IT-SECURITY IN ANWALTSKANZLEIEN

Werden IT-Systeme von der Kanzlei eingesetzt, ist sicherzustellen, dass diese Systeme und die darin enthaltenen Daten vor unbefugten Zugriffen geschützt werden. Diese Verpflichtung zur Wahrung der bestehenden beruflichen Verschwiegenheitspflichten und datenschutzrechtlichen Anforderungen gilt unabhängig davon, ob IT-Systeme von der Kanzlei selbst betrieben werden oder ob unter Einhaltung der in § 40 Abs 3 RL-BA 2015 festgelegten Voraussetzungen externe Dienstleister zum Zwecke der elektronischen Datenverarbeitung eingesetzt werden. In dieser Anleitung finden sich praktische Tipps und Empfehlungen zur Sicherstellung der Datensicherheit und IT-Security.

1. IT-Security Basics

- **Firewall und Antivirus-Software:** Stellen Sie sicher, dass sämtliche beruflich genutzten Geräte mit einer Firewall und zuverlässiger Antivirus-Software geschützt sind.
- **Regelmäßige Software-Updates:** Halten Sie alle Betriebssysteme, Anwendungen und Sicherheitssoftware auf dem neuesten Stand, um bekannte Sicherheitslücken zu schließen.
- **Verschlüsselte Kommunikation:** Nutzen Sie verschlüsselte E-Mails und sichere Kommunikationskanäle (zB der context Services GmbH), besonders beim Austausch von vertraulichen Informationen.
- **Starke Passwörter und Zwei-Faktor-Authentifizierung:** Stellen Sie sicher, dass nur starke, einzigartige Passwörter gewählt werden und implementieren Sie soweit möglich eine Zwei-Faktor- bzw Multi-Faktor-Authentifizierung.
- **Datensicherung und Disaster Recovery:** Sichern Sie regelmäßig wichtige Daten und entwickeln Sie einen Notfallplan für den Fall eines Datenverlusts oder eines Cyberangriffs. Der Abschluss einer Cyber-Versicherung wird empfohlen.
- **Mobile Gerätesicherheit:** Schützen Sie mobile Geräte mit alphanumerischen Passwörtern statt mit PINs und installieren Sie Sicherheits-Apps, welche Sie befähigen, verlorene oder gestohlene Geräte zu orten und deren Inhalte zu löschen.
- **Netzwerksicherheit:** Richten Sie ein sicheres, internes Netzwerk ein und beschränken Sie den Zugriff auf sensible Daten auf autorisierte Benutzer.
- **Datensynchronisation:** Vermeiden Sie jedenfalls automatische Synchronisierung von Daten mit Dritten, die nicht die entsprechenden datenschutzrechtlichen Rahmenbedingungen erfüllen. Dies sind zB die Synchronisierung der Kontakte mit Apps oder der automatische Upload von Fotos und Dokumenten. Stellen Sie sicher, dass die Datenübertragung (zB Transfer von Fotos am Mobilgerät in den Akt) insb zwischen Mobilgerät und PC/Notebooks/Tablets (zB über eine sichere Cloud) sicher ist.
- **Einsatz von Cloudlösungen:** Achten Sie auf die Einhaltung der der datenschutzrechtlichen und berufsrechtlichen Vorgaben (s.u.).

2 . Datenschutz und anwaltliche Verschwiegenheit

- **Datenschutz:** IT-Security ist Teil der Datenschutz-Compliance und der Pflichten, die sich ua aus der DSGVO ergeben. Hierzu gehören die Sicherheit von personenbezogenen Daten vor Zugriff Unberechtigter, der Schutz vor Verlust der Daten und die Gewährleistung der Datenintegrität (Art 5 Abs 1 lit f DSGVO).
- **Geheimhaltungsvereinbarungen allgemein:** Stellen Sie die Geheimhaltungsverpflichtung schriftlich sicher und schließen Sie, wo notwendig, Auftragsverarbeitungsvereinbarungen ab.
- **Standesrechtliche Pflichten:** Zur allgemeinen berufsrechtlichen Pflicht der anwaltlichen Geheimhaltung, die auch auf Mitarbeiterinnen und Mitarbeiter sowie Dienstleister überbunden werden muss, wurden mit der Aktualisierung des § 40 RL-BA im Jahr 2020 in dessen Abs 3 konkrete Pflichten für Rechtsanwältinnen und Rechtsanwälte eingeführt. Ein externer Dienstleister kann danach zum Zwecke der elektronischen Datenverarbeitung eingesetzt werden, wenn
  - ❶ die Interessen des Klienten gewahrt werden,
  - ❷ der Rechtsanwalt den externen Dienstleister sorgfältig auswählt,
  - ❸ der Rechtsanwalt den externen Dienstleister nachweislich vertraglich dazu verpflichtet, ihn im Falle einer Hausdurchsuchung unverzüglich zu informieren,
  - ❹ unter Berücksichtigung des Stands der Technik technische und organisatorische Maßnahmen ergriffen werden, um ein angemessenes Niveau der Datensicherheit und der Vertraulichkeit der Daten zu gewährleisten, und
  - ❺ der Rechtsanwalt den Klienten über die Kategorien der in Anspruch genommenen externen Dienstleister und der von diesen zu erbringenden Dienstleistungen informiert.

Vorgeschlagene Klausel für § 40 Abs 3 Z 3 RL-BA:

Der Dienstleister nimmt zur Kenntnis, dass es sich bei den von ihm verarbeiteten Daten auch um solche handelt, die der anwaltlichen Verschwiegenheit (§ 9 Abs 2 RAO) unterliegen. Sollten diese Daten im Zuge einer Hausdurchsuchung direkt oder indirekt (zB weil sie sich auf demselben physischen Server befinden) betroffen sein, ist der Dienstleister

dazu verpflichtet, KUNDEN unverzüglich über die Hausdurchsuchung zu informieren und die jeweilige einschreitende Behörde darüber in Kenntnis zu setzen, dass es sich bei den betreffenden Daten (auch) um solche handelt, die der anwaltlichen Verschwiegenheit unterliegen.

- **Fernwartung:** Bei Fernwartung durch externe Dienstleister ist besonders auf die Zugriffsberechtigungen zu achten. Zugriffe auf dem Verschwiegenheitsgebot unterliegende Daten sind möglichst nicht zu erlauben. Zu vermeiden sind jedenfalls unbeaufsichtigte unbeschränkte Fernwartungszugänge.
- **Anbieter aus Drittstaaten:** Eine generelle Nutzung in (nicht sicheren) Drittstaaten ist standesrechtlich nicht gedeckt, da die Durchsetzbarkeit der standesrechtlichen Pflichten nicht gegeben ist. Sichere Drittstaaten wären zB die Schweiz oder Großbritannien (Angemessenheitsbeschluss gem. Art 45 DSGVO, wobei dies für die USA nicht generell gesagt werden kann, da hier bereits mehrmals die Rechtsgrundlagen durch den EuGH aufgehoben wurden). Aber auch hier müssen die oben genannten datenschutz- und standesrechtlichen Rahmenbedingungen eingehalten werden. Im Einzelfall kann eine Nutzung von Anbietern aus Drittstaaten zulässig sein (siehe auch Art 49 Abs 1 lit e DSGVO, für einzelne Causen), es muss aber zusätzlich die Rechtsgrundlage des Datenexports (Art 44 ff DSGVO, wie zB das EU-US Datenschutzabkommen, oder Standardvertragsklauseln mit zusätzlichen technischen Maßnahmen und Risikoanalyse (Transfer Impact Assessment)) sichergestellt werden.
- **Technisch organisatorische Maßnahmen (TOM):** Die von Ihnen für IT-Security erstellte Dokumentation und die von Ihren Dienstleistern getroffenen Maßnahmen bilden einen Teil der technisch-organisatorischen Maßnahmen, die gemäß DSGVO zu führen sind (siehe zB auch Art 32 DSGVO).

2. Backups und Löschung

- **Datensicherung / Backup:** Sichern Sie regelmäßig (im Idealfall automatisch) 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 den Fall eines Softwarewechsels oder die Beendigung Ihrer Tätigkeit (Aufbewahrungspflichten).
- **Externe Sicherung:** Stellen Sie sicher, dass auch bei externen Dienstleistern ein Backup Teil der Leistung ist.
- **Entsorgung:** Vermeiden Sie die Weitergabe von Datenträgern, auf welchen zuvor sensible Kanzleidaten gespeichert waren. Diese könnten unter Umständen wiederhergestellt werden. Bei der Entsorgung sollten derartige Datenträger physisch zerstört werden, um eine Wiederherstellung zu verunmöglichen. Fordern Sie von externen Dienstleistern eine schriftliche Bestätigung der Löschung.

3. Kommunikation mit Mandantinnen und Mandanten

- **Datenaustausch per E-Mail:** Obwohl E-Mail weiterhin als einer der gängigsten Kommunikationskanäle verwendet wird, sei darauf hingewiesen, dass eine Datenübermittlung per (unverschlüsselter) E-Mail nicht ausreichend sicher ist. Sie sollten daher alternative Möglichkeiten (zB context Services GmbH) in der Kanzlei einführen, um insb vertrauliche Daten zwischen Ihnen und Ihren Mandantinnen und Mandanten, Mitarbeiterinnen und Mitarbeitern sowie Kolleginnen und Kollegen austauschen zu können. Zwischen Teilnehmern des ERV können Dateien übrigens auch direkt per Teilnehmer-Direktzustellung übermittelt werden.
- **Datenräume:** Zusätzlich zu Kommunikationskanälen kann auch ein sicherer Datenraum (zB selbst gehostete Nextcloud, context Services GmbH) eingerichtet werden, um Dateien wie zB Gerichtskorrespondenz, Entwürfe oder Verträge zu teilen. Kostenlose Online-Angebote zum Transfer größerer Datenvolumen, die nicht den rechtlichen Anforderungen entsprechen, sind zu meiden.
- **Messenger:** Versenden Sie keine Daten über Messenger-Dienste oder Social Media Nachrichten. Sollten Sie von Mandantinnen und Mandanten unaufgefordert Nachrichten über diese Kanäle erhalten, verweisen Sie diese umgehend auf sichere Kommunikationsmittel.

4. Mitarbeiterinnen und Mitarbeiter sowie externe Dienstleister

- **Sensibilisierung und Schulungen:** Führen Sie regelmäßige Sicherheitsschulungen für Mitarbeiterinnen und Mitarbeiter durch, um sie über die neuesten Bedrohungen und Sicherheitspraktiken aufzuklären.
- **Phishing-Erkennung:** Schulen Sie Mitarbeiterinnen und Mitarbeiter im Erkennen von Phishing-E-Mails und anderen Social-Engineering-Angriffen, um zu verhindern, dass sie auf betrügerische Links oder Anhänge klicken.
- **Einschränkung von Berechtigungen:** Gewähren Sie Mitarbeiterinnen und Mitarbeiter nur die Berechtigungen, die sie für ihre Arbeit benötigen, um den Zugang zu sensiblen Daten zu beschränken.
- **Sichere Dokumentenfreigabe:** Implementieren Sie sichere Methoden zur gemeinsamen Nutzung von Dokumenten, um zu verhindern, dass vertrauliche Informationen in falsche Hände geraten.
- **Verantwortlichkeiten klären:** Definieren Sie klare Verantwortlichkeiten für die IT-Sicherheit im Team, damit alle wissen, welche Rolle sie bei der Sicherung der Daten spielen.
- **Meldepflicht für Vorfälle:** Etablieren Sie eine klare Richtlinie für die sofortige Meldung von verdächtigem Verhalten oder möglichen Sicherheitsvorfällen.
- **Externe Dienstleister überprüfen:** Falls Sie externe IT-Dienstleister nutzen, stellen Sie sicher, dass diese angemessene Sicherheitsmaßnahmen treffen, welche regelmäßig überprüft werden.
- **Privatnutzung der Geräte:** Legen Sie fest, welche Geräte für eine dienstliche Nutzung und welche für eine Privatnutzung vorgesehen sind, und trennen Sie dies im Idealfall strikt.
- **Home-Office:** Schließen Sie Home-Office-Vereinbarungen ab und klären Sie Ihre Mitarbeiterinnen und Mitarbeiter über die Verhaltensregeln im Home-Office auf.
- **Vereinbarung gemäß § 40 Abs 3 RL-BA:** Beachten Sie beim Einsatz externer Dienstleister die Notwendigkeit entsprechender Geheimhaltungsvereinbarungen bzw die Vereinbarung gemäß § 40 Abs 3 RL-BA (s.o. Punkt 2).
- **Beendigung:** Achten Sie bei Beendigung von der Zusammenarbeit mit Mitarbeiterinnen und Mitarbeitern und externen Dienstleistern darauf, dass alle Zugriffe entzogen (insb Passwörter geändert) werden und Daten bei diesen gelöscht werden.

5. Berechtigungen

- **Zugriff auf interne Dokumente:** Erstellen Sie ein Berechtigungskonzept und prüfen Sie, welche Mitarbeiterinnen und Mitarbeiter auf welche Daten Zugriff haben. Beispielsweise sollten HR-Daten nur von den betroffenen Personen und beispielsweise der Buchhaltung eingesehen werden können.
- **Zugriff auf Akten:** Legen Sie fest, ob alle Mitarbeiterinnen und Mitarbeiter auf alle Akten Zugriff haben sollen, und schränken Sie diesen allenfalls ein.
- **Zugriffsprotokollierung:** Stellen Sie sicher, dass die tatsächlichen Datenzugriffe protokolliert werden.

6. Online-Meetings und Vorträge

- **Vertraulichkeit vor dem Anruf überprüfen:** Starten Sie jeden Videocall mit einer kurzen Erinnerung an die Vertraulichkeit und bitten Sie alle Teilnehmer, sich in einer vertraulichen Umgebung aufzuhalten.
- **Vertrauliche Dokumente vorher prüfen:** Bevor Sie Screensharing verwenden, überprüfen Sie den Inhalt der zu teilenden Dokumente, um sicherzustellen, dass keine vertraulichen Informationen enthalten sind.
- **Screensharing mit Bedacht verwenden:** Erlauben Sie Screensharing nur, wenn es wirklich notwendig ist, und sorgen Sie dafür, dass nur der benötigte Bildschirmbereich geteilt wird, um sensible Daten zu schützen. Schließen Sie alle Programme und Fenster, die Sie nicht benötigen und teilen Sie wenn möglich einen zweiten erweiterten Bildschirm.
- **Mitteilungseinstellungen verwalten:** Stellen Sie sicher, dass bei Screensharing Ihre Mitteilungen auf stumm geschalten sind, damit nicht vertrauliche Inhalte, wie zB Mitteilungen über neue E-Mails, am Bildschirm erscheinen.
- **Sichere Videokonferenztools verwenden:** Nutzen Sie vertrauenswürdige Videokonferenzplattformen, die die entsprechenden datenschutz- und standesrechtlichen Rahmenbedingungen erfüllen, um sicherzustellen, dass die Kommunikation geschützt ist.
- **Passwortschutz für Meetings:** Verwenden Sie Passwortschutz für Videocalls, um sicherzustellen, dass nur autorisierte Personen teilnehmen können.
- **Wartezimmer-Funktion nutzen:** Aktivieren Sie die Wartezimmer-Funktion, um Teilnehmerinnen und Teilnehmer zu überprüfen, bevor sie dem Gespräch beitreten können.
- **Aufzeichnungen einschränken:** Beschränken Sie die Möglichkeit, Videocalls aufzuzeichnen, und speichern Sie Aufzeichnungen sicher, falls sie für zukünftige Referenzen benötigt werden.
- **Klare Anweisungen geben:** Geben Sie klare Anweisungen an Ihre Mitarbeiterinnen und Mitarbeiter, welche Informationen während des Gesprächs geteilt werden dürfen und welche nicht.

7. Sicherheit unterwegs

- **Sichere Wi-Fi-Verbindungen:** Sichern Sie Ihr Wi-Fi-Netzwerk (nur mit Passwortzugang) und benutzen Sie öffentliche Wi-Fi-Hotspots nicht, um das Risiko von Cyber-Angriffen, bei denen die Angreifer den Datenverkehr zwischen den Kommunikationspartnern abfangen und manipulieren, zu minimieren, und verpflichten Sie Ihre Mitarbeiterinnen und Mitarbeiter entsprechend. Alternativ kann der eigene mobile Hotspot oder auch eine sichere VPN-Verbindung für die Datenübertragung in das Kanzleinetzwerk verwendet werden.
- **Endgeräte-Sicherheit:** Stellen Sie sicher, dass auch die Endgeräte gesichert sind, Festplatten verschlüsselt und ein Passwortschutz besteht. Lassen Sie Ihre Geräte nie unbeaufsichtigt.
- **Vertrauliche Arbeit:** Vertrauliche Gespräche sollen in geschlossenen Räumen geführt werden, um sicherzustellen, dass sensible Informationen nicht unbeabsichtigt von anderen Personen gehört werden. Bei der Arbeit am Laptop oder Tablet muss sichergestellt werden, dass der Bildschirm nicht von Dritten einsehbar ist (zB mit Bildschirmschutz, Positionierung im Raum).
- **Sichere Dateifreigabe:** Setzen Sie sichere Plattformen/Datenräume ein, wenn Dateien geteilt werden müssen, und etablieren Sie Prozesse, wie mit Synchronisierung und Datensharing umgegangen wird. Möglich ist beispielsweise auch ein Remote-Zugriff auf die Rechner in der Kanzlei, bei dem keine Daten am mobilen Gerät gespeichert werden.
- **Daten bei Gericht:** Stellen Sie sicher, dass Sie auch ohne Internet Zugriff auf alle Daten haben, die Sie vor Gericht benötigen, da dort eine durchgehende und stabile Internetverbindung meist nicht gewährleistet ist bzw der Zugriff aufs Internet nicht erlaubt ist (zB im Halbgesperre).

8. Hacker, Scammer, usw

- **E-Mail Betrug:** Stellen Sie sicher, dass Ihr Virenschutz auch E-Mail (Anhänge) überprüft, und öffnen Sie keine E-Mails, die bereits auf den ersten Blick SPAM sind. Folgen Sie keinen Links in E-Mails von Sendern, die Sie nicht kennen. Achten Sie bei E-Mails, die geheime Daten von Ihnen fordern (zB Bankdaten, Passwörter) noch kritischer auf den Sender, indem Sie die E-Mail-Adresse und nicht nur den Anzeigenamen überprüfen und in den Header der E-Mail blicken. Folgen Sie nicht den Links aus diesen E-Mails, sondern geben Sie die Ihnen bekannte Website, beispielsweise des Onlinebankings, direkt im Browser sein. Gehen Sie auch besonders kritisch mit Gratisangeboten in E-Mails um, wenn Sie den Sender nicht kennen, löschen Sie diese ungelesen.
- **Daten per E-Mail:** Übermitteln Sie niemals Daten wie Kreditkarteninformationen oder Passwörter per E-Mail.
- **Social Engineering:** Oft wird mit diesem Begriff das Ausnutzen von Menschen beim unbefugten Zugriff auf Systeme und Daten bezeichnet. Es ist daher wichtig, dass Sie auch Ihre Mitarbeiterinnen und Mitarbeiter entsprechend schulen.

9. Physischer Schutz

- **Bildschirmsperre:** Sperren Sie den Bildschirm, wenn Sie Ihren Platz verlassen und weisen Sie Ihre Mitarbeiterinnen und Mitarbeiter entsprechend ein.
- **Offene Geräte:** Stellen Sie sicher, dass betriebsfremde Personen keine Geräte oder Daten einsehen, oder auf Kanzleigeräte zugreifen können. Kontrollieren Sie den Zutritt und prüfen Sie auch, dass es keine Möglichkeit zur Einsicht in Daten für Externe (zB auch Mandantinnen und Mandanten bei Meetings, Reinigungspersonal) gibt.
- **Einbruchs- und Diebstahlschutz:** Sichern Sie Ihre Geräte auch physisch in der Kanzlei vor unberechtigten Zugriffen.

Stand: Februar 2024
AK IT und Digitalisierung

Österreichischer Rechtsanwaltskammertag
Wollzeile 1 - 3, 1010 Wien
Tel: +43 (1) 535 12 75, Fax: +43 (1) 535 12 75-13
E-Mail: office@oerak.at, www.oerak.at