Datenschutz-Grundverordnung
Datenschutzempfehlungen ADVOKAT

Die Ausführungen in diesem Dokument folgen der unverbindlichen Interpretation der DSGVO durch die ADVOKAT Unternehmensberatung Greiter & Greiter GmbH. Wir haben uns mit der Materie intensiv beschäftigt und Vorschläge für die DSGVO-konforme Anwendung der von uns hergestellten Software erarbeitet. Bitte überprüfen Sie diese Vorschläge und ziehen Sie bedarfsweise professionelle Beratung hinzu. Die ADVOKAT Unternehmensberatung Greiter & Greiter GmbH macht mit diesem Dokument keine Versprechungen oder Zusicherungen, sondern stellt eine unverbindliche Meinung zur Verfügung.


ADVOKAT

1 Datensicherheit mit ADVOKAT Software

1.1 Datenschutz-Grundsätze

1.1.1 Rechtmäßigkeit

Artikel 5 Abs. 1 lit. a DSGVO – ErwG 39 DSGVO
Artikel 6, 7, 9-11, 22 DSGVO – ErwG 32, 33, 40-56 DSGVO

Sämtliche Datenverarbeitung erfolgen auf Basis einer nachweisbaren Rechtsgrundlage. Die jeweiligen Rechtsgrundlagen sind im Verarbeitungsverzeichnis dokumentiert.

Zusätzlich wird die Rechtsgrundlage für jede Person separat in der Anwaltssoftware „ADVOKAT“ hinterlegt, und zwar einerseits der zur Anwendung kommende Tatbestand der DSGVO und andererseits die dokumentierte Rechtsgrundlage (z.B. der Mandatsvertrag) selbst.

Die Anwaltssoftware „ADVOKAT“ ermöglicht den Ausdruck einer personenbezogenen Datenschutzmitteilung, welche sämtliche Informationen wiedergibt, die gemäß der Artikel 12 bis 14 DSGVO bei Datenerhebungen zu erteilen sind. Die Datenschutzmitteilung als Bestandteil eines Mandats- oder Beratungsvertrages qualifiziert den Vertrag als ausreichende Rechtsgrundlage gemäß Artikel 6 DSGVO.

1.1.2 Transparenz

Artikel 5 Abs. 1 lit. a DSGVO – ErwG 39 DSGVO

Sämtliche Verarbeitungstätigkeiten der Anwaltssoftware „ADVOKAT“ sind vollständig im Programmhandbuch dargelegt. Weiters sind sämtliche Verarbeitungsvorgänge der Kanzlei im Verarbeitungsverzeichnis vollständig und nachvollziehbar dokumentiert.

Im Verarbeitungsverzeichnis ist für alle Verarbeitungsvorgänge und dort je Personenkategorie dargelegt, wie die Erfüllung der Informationspflichten sichergestellt ist.

Die Anwaltssoftware „ADVOKAT“ ermöglicht den Ausdruck einer personenbezogenen Datenschutzmitteilung, welche sämtliche Informationen wiedergibt, die gemäß der Artikel 12 bis 14 DSGVO bei Datenerhebungen zu erteilen sind.

Die Anwaltssoftware „ADVOKAT“ ermöglicht die Erstellung eines Auskunftsberichts. Der Auskunftsbericht stellt umfangreich die zur Person gespeicherten Daten anschaulich zusammen. Zusätzlich enthält der Auskunftsbericht sämtliche Informationen der Artikel 12 bis 15 DSGVO.

Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende (Klient/innen) im Sinne des Erwägungsgrundes 63 DSGVO (Fernzugang für betroffene Person) einen permanenten Zugang auf deren Akten und Aktendaten durch Anmeldung am Klient/innen-Portal (Lesezugriff).

Protokollierungsfunktionen schaffen zusätzlich Transparenz und Nachvollziehbarkeit. Details dazu sind im Kapitel „Sicherheitsprotokollierung“ ausgeführt.

1.1.3 Zweckbindung

Artikel 5 Abs. 1 lit. b DSGVO – ErwG 39 DSGVO

Die Verarbeitung von personenbezogenen Daten erfolgt ausschließlich für festgelegte, eindeutige, legitime Zwecke. Diese Zwecke sind einerseits im Verarbeitungsverzeichnis je Verarbeitungsvorgang dokumentiert und werden andererseits für jede Person separat festgehalten und in der Anwaltssoftware „ADVOKAT“ dokumentiert. Die für eine Person geltenden Zwecke können jederzeit genannt bzw. beauskunftet werden.

Bei Annahme eines neuen Auftrages werden die Zwecke zu Beginn festgelegt, festgehalten und in der Anwaltssoftware „ADVOKAT“ dokumentiert. Die Zwecke finden sich in den personenbezogenen Ausdrucken „Datenschutzmitteilung“ und „Auskunftsbericht“ wieder.

1.1.4 Datenminimierung

Artikel 5 Abs. 1 lit. c DSGVO – ErwG 39 DSGVO

Datenminimierung hat viele Facetten (Datenmenge, Umfang der Verarbeitung, Speicherfrist, Zugänglichkeit). Im Verarbeitungsverzeichnis ist je Verarbeitungsvorgang dargelegt, wie dieser Grundsatz in all seinen Facetten verankert ist.

Der Zugang zu personenbezogenen Daten ist generell dadurch minimiert, dass die Daten mit der Anwaltssoftware „ADVOKAT“ verarbeitet werden. Im Kapitel „Zugangssicherung“ ist dargelegt, wie der Zugang zu Systemen einerseits und der Zugang zu bestimmten Daten im System andererseits eingeschränkt werden kann.

Bei Verwendung von ADVOKAT Security: Es gibt einige Rechte für Stapelverarbeitungen – das ist die gleichzeitige Verarbeitung einer größeren Zahl von Datensätzen. Mit einem restriktiven Berechtigungskonzept wird so sichergestellt, dass Daten nicht in umfangreicher Form durchsucht (Beschränkung der Suchergebnisse) oder ausgegeben (Beschränkung von Druck- und Exportfunktionen) werden können.

1.1.5 Richtigkeit

Artikel 5 Abs. 1 lit. d DSGVO – ErwG 39 DSGVO

Der Richtigkeit der Daten dient die relationale Speicherung von Daten durch die Anwaltssoftware „ADVOKAT“. Dadurch werden Änderungen an Personenstammdaten in sämtliche Verwendungsbereiche automatisch übernommen.

Um die Aktualität der Daten sicherzustellen, werden vorhandene Daten bei neuerlicher Beauftragung vorgelegt (*„Bitte prüfen Sie Ihre Daten.“*) und erforderlichenfalls aktualisiert. Dazu kann mit der Anwaltssoftware „ADVOKAT“ ein Auskunftsbericht, welcher sämtliche Daten anführt, erstellt und den Klient/innen zur Prüfung vorgelegt werden.

Durch Übernahme-Funktionen der Anwaltssoftware „ADVOKAT“ werden aus Registern (z.B. Grundbuch, Firmenbuch, ZMR, Edikte, Compliance Check) abgefragte Daten automationsunterstützt verglichen und übernommen. Die Anlage bzw. Aktualisierung von Personenstammdaten erfolgt dadurch unter Ausschaltung von Eingabefehlern.

Für im Kanzleialltag relevante und öffentlich bekannte Personen – d.s. Rechtsanwält/innen, Notar/innen, Gerichte, Behörden, Kammern, Gläubigerschutzverbände und Versicherungen – erfolgt eine laufende Aktualisierung durch die Anwaltssoftware „ADVOKAT“. Diese gewärtigt einen höchst aktuellen Stand, was die Datensicherheit vor allem auch dahingehend fördert, dass Daten nicht an falsche (alte) Adressen übermittelt werden.

1.1.6 Speicherbegrenzung

Artikel 5 Abs. 1 lit. e DSGVO – ErwG 39 DSGVO

Personenbezogene Daten sind im anwaltlichen Geschäftsalltag ein wesentlicher Bestandteil. Sofern personenbezogene Daten über den Abschluss eines Auftrags hinaus aufbewahrt werden, erfolgt dies ausschließlich innerhalb des Kanzleinetzwerks und bei Anwendung zusätzlicher Sicherheitsmaßnahmen. Im Verarbeitungsverzeichnis ist je Verarbeitungsvorgang dargelegt, wie diesem Grundsatz entsprochen wird.

Gemäß § 12 Abs. 2 RATG besteht eine Pflicht zur Aufbewahrung für die Dauer von fünf Jahren ab Beendigung der Vertretung. Für bestimmte Daten (Rechnungen, Buchhaltung) besteht darüber hinaus eine Aufbewahrungspflicht von jedenfalls 7 Jahren ab Schluss des Kalenderjahres in welchem das Wirtschaftsjahr endet, dem die Daten zugehören (§ 11 UStG, § 132 Abs. 1 BAO, §§ 147-151 BAO).

Darüber hinaus besteht für Rechtsanwält/innen die Pflicht, eine Interessenkollision zu vermeiden (§ 10 RAO, § 12a RL-BA, Punkt 3.2. der CCBE-Standesregeln). Eine dafür vorgesehene Funktion der Anwaltssoftware „ADVOKAT“ ermöglich die Prüfung auf Kollision. Eine solche Prüfung erfordert allerdings das Vorhandensein entsprechender Personendaten.

Die Anwaltssoftware „ADVOKAT“ ermöglicht je Akt das Hinterlegen eines Ablagedatums sowie bedarfsweise das Hinterlegen auch anderer löschrelevanten Daten (z.B. durch Anlegen freier Felder wie „Datenkategorie“ und „Datum“). Mit dem integrierten Suchassistenten können zu löschende Daten einfach und schnell angezeigt und die Löschung davon ausgehend vollzogen werden.

Mit Funktionen zur Pseudonymisierung und Anonymisierung von Personen ermöglicht die Anwaltssoftware „ADVOKAT“ zusätzliche Maßnahmen zur Verminderung bzw. Ausschaltung der Identifizierbarkeit von Personen. Diese Funktionen können mit ADVOKAT Security auf einzelne Sachbearbeiter/innen eingeschränkt werden. Pseudonymisierte Personen sind nicht mehr identifizierbar (in der Datenbank und in der Software selbst), bis eine dazu berechtigte Person die Pseudonymisierung zurücknimmt. Anonymisierte Personen sind unwiderruflich nicht mehr identifizierbar.

Bei Verwendung von ADVOKAT Security: Durch Ablagen von Akten in der Anwaltssoftware „ADVOKAT“ werden diese automatisch in einen virtuellen versperrten Aktenschrank (durch Anlage einer dafür vorgesehenen Aktengruppe) gelegt, zu welchem nur definierte Personen Zugang haben. Es können auch mehrere solcher „Aktenschränke“ angelegt werden (z.B. einer je Abteilung/Partnerteam). Nach Abschluss eines Auftrags aufbewahrte Daten werden so effektiv geschützt, weil der Zugang durch Aktablage automatisch stark eingeschränkt wird.

Eine dafür geschaffene Suchfunktion der Anwaltssoftware „ADVOKAT“ listet sämtliche Personen, welche aufgrund eines fehlenden Verarbeitungszwecks gelöscht werden können bzw. müssen. Die solcherart gelisteten Personen können direkt gelöscht werden.

Mit der Anwaltssoftware „ADVOKAT“ verwaltete Insolvenzen können einfach und schnell bereinigt werden. Durch Hinterlegung des Abschlussdatums kann ausgehend davon eine regelmäßige Bereinigung nach Verstreichen einer definierten Aufbewahrungsfrist erfolgen.

1.1.7 Integrität und Vertraulichkeit

Artikel 5 Abs. 1 lit. f DSGVO – ErwG 39 DSGVO

Neben der Absicherung der Kanzleiräumlichkeiten gegen unbefugten Zutritt und der Absicherung des Kanzleinetzwerks gegen unbefugte Zugriffe via Internet sorgt eine Sicherung des Zugangs zu Rechnern mittels Kennwortanmeldung für die Wahrung dieses Grundsatzes.

Ein zuverlässiges Backup-Konzept, welches sich am Stand der Technik befindet, beugt einem unbeabsichtigten Verlust und einer unbeabsichtigten Zerstörung und Schädigung vor.

Mit Verwendung der Anwaltssoftware „ADVOKAT“ wird durch eine Kombination aus sicherer Datenhaltung, effektiver Zugangssicherung (inkl. sicherer Datenübertragung) und Nachvollziehbarkeit (Sicherheitsprotokollierung) ein sehr hohes Maß an Integrität und Vertraulichkeit sichergestellt.

Details sind in den Kapiteln „Sichere Datenhaltung“, „Zugangssicherung“ und „Sicherheitsprotokollierung“ beschrieben. Die Anwaltssoftware „ADVOKAT“ bietet darüber hinaus diverse Sicherheitsfunktionen um Integrität und Vertraulichkeit zu stärken (z.B. Pseudonymisierung). Diese sind mitunter bei den anderen Grundsätzen beschrieben.

Integrität und Vertraulichkeit können zusätzlich durch Verwendung von ADVOKAT Security sowie der Verwendung des Dokumentenmanagementsystems Microsoft SharePoint samt Anbindung an ADVOKAT erhöht werden.

1.1.8 Privacy by design & privacy by default

Artikel 24, 25, 32 DSGVO – ErwG 74-78, 83 DSGVO

Hohe Sicherheit bei der Verarbeitung personenbezogener Daten wird vor allem durch den Einsatz sicherer Software gewärtigt. Die Anwaltssoftware „ADVOKAT“ ermöglicht die Wahrung der sich aus der DSGVO ergebenden Pflichten und bietet eine Reihe von Funktionen, welche die Erfüllung der entsprechenden Anforderungen unterstützen.

Zu diesen Funktionen gehören neben klassischen Datensicherheitsfeatures (siehe hierzu die Kapitel „Sichere Datenhaltung“, „Zugangssicherung“ und „Sicherheitsprotokollierung“) insbesondere Masken und Felder zur Dokumentation und Verwaltung der erforderlichen Daten (z.B. Verarbeitungszwecke, Rechtsgrundlagen, Personenkategorien, Datenkategorien, Empfängerkategorien, Datenquellen, u.a.m.) sowie damit zusammenhängende Funktionen wie bspw. die Erstellung von Datenschutzmitteilungen (zur Erfüllung von Informationspflichten) und Auskunftsberichten.

1.2 Betroffenenrechte und Informationspflichten

1.2.1 Informationspflicht bei Datenerhebung

Artikel 12-14 DSGVO – ErwG 58-62 DSGVO

Die Wahrnehmung der Informationspflicht ist separat für jeden Verarbeitungsvorgang und wiederum für jede Personenkategorie je Verarbeitungsvorgang im Verarbeitungsverzeichnis dokumentiert.

Mit Verwendung der Funktion zur Erstellung von personenbezogenen Datenschutzmitteilungen der Anwaltssoftware „ADVOKAT“ kann zu jedem Zeitpunkt eine Datenschutzmitteilung für eine beliebige Person ausgegeben und diese ausgedruckt oder per E-Mail versendet werden. Die Datenschutzmitteilung gibt sämtliche Informationen gemäß der Artikel 12 bis 15 DSGVO wieder und ist in Form und Sprache präzise und verständlich gefasst.

In manchen Fällen unterliegen Datenerhebungen der anwaltlichen Verschwiegenheitspflicht (§ 9 RAO, § 305 Z. 4 und § 321 Z. 4 ZPO, § 144 Abs. 2 iVm § 157 Abs. 2 StPO) weshalb die Bestimmungen zur Informationspflicht bei Erhebung von Daten bei Dritten (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Dies ist im Verarbeitungsverzeichnis entsprechend ausgeführt.

Die Datenschutzmitteilung ist Bestandteil des Vertretungs- oder Beratungsauftrags und wird somit bei Auftragserteilung übergeben und akkordiert. Sie gibt bereits alle erforderlichen Informationen auch für zukünftige Datenerhebungen im Zusammenhang mit dem konkreten Auftrag, womit bei späteren Datenerhebungen gem. Art. 14 Abs. 5 lit. a in der Regel keine neuerliche oder zusätzliche Informierung erforderlich ist. Im persönlichen Gespräch werden etwaige Fragen direkt besprochen.

1.2.2 Recht auf Auskunft

Artikel 12, 15 DSGVO – ErwG 58, 59, 63, 64 DSGVO

Die Anwaltssoftware „ADVOKAT“ ermöglicht die Erstellung eines Auskunftsberichts. Der Auskunftsbericht stellt umfangreich die zur Person gespeicherten Daten anschaulich zusammen. Zusätzlich enthält der Auskunftsbericht sämtliche Informationen der Artikel 12 bis 15 DSGVO.

Auf Anfrage wird ein solcher Auskunftsbericht erstellt. Die Ausgabe erfolgt in Microsoft Word, wodurch eine allenfalls nötige Überarbeitung („Schwärzen“) möglich ist. Dies kann gem. ErwG 63 DSGVO im Einzelfall erforderlich sein, um die Freiheiten und Rechte anderer Personen zu schützen (z.B. Geschäftsgeheimnisse, Rechte des geistigen Eigentums).

Bei Bedarf können zusätzliche, informative Berichte wie bspw. Aktenstammblätter und Aktenhistorien über alle Akten zu einer Person mit Hilfe der Anwaltssoftware „ADVOKAT“ ausgefertigt werden.

Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende (Klient/innen) im Sinne des Erwägungsgrundes 63 DSGVO (Fernzugang für betroffene Person) einen permanenten Zugang auf deren Akten und Aktendaten durch Anmeldung am Klient/innen-Portal (Lesezugriff).

1.2.3 Recht auf Berichtigung und Vervollständigung

Artikel 12, 16, 19 DSGVO – ErwG 58, 59, 65 DSGVO

Auf Wunsch jeder Person werden auf diese Person bezogene Daten unmittelbar richtiggestellt oder vervollständigt. Aufgrund des relationalen Datenkonzepts der Anwaltssoftware „ADVOKAT“ werden Anpassungen automatisch in sämtliche Bereiche übernommen, sofern Daten nicht bspw. durch Ausfertigung von Dokumenten manifestiert wurden.

Nach Vornahme einer Berichtigung bzw. Vervollständigung wird die betroffene Person über diese Maßnahme informiert.

1.2.4 Recht auf Löschung

Artikel 12, 17, 19 DSGVO – ErwG 58, 59, 65, 66 DSGVO – § 4 Abs. 2 DSG idF BGBl. I 120/2017

Auf Wunsch einer Person, zu welcher Daten gespeichert sind, werden diese sofort und vollständig gelöscht, sofern nicht berechtigte Gründe gegen die Löschung sprechen. Berechtigte Gründe sind bspw. ein aufrechtes Vertragsverhältnis und gesetzliche Aufbewahrungspflichten.

Im Verarbeitungsverzeichnis sind die je Verarbeitungsvorgang vorgesehenen Aufbewahrungsfristen samt den Grundlagen (Rechtsgrundlagen, Aufbewahrungspflichten, berechtigte Gründe) festgelegt. Ein Antrag auf Löschung wird im Zusammenhang mit diesen geprüft.

Soweit die Verteidigung gegen die Geltendmachung etwaiger Schadenersatzansprüche der einzige verbleibende Grund für die Aufbewahrung von personenbezogenen Daten ist, wird eine Löschung dennoch vollzogen, wenn Auftraggebende eine entsprechende Enthaftungsvereinbarung unterschreiben. Dadurch können betroffene Personen ihr Recht durchsetzen, ohne dass dadurch ein Risiko für die Kanzlei begründet wird.

Anstatt einer physischen Löschung von Daten werden diese bedarfsweise anonymisiert. Dies geschieht durch Verwendung einer entsprechenden Funktion der Anwaltssoftware „ADVOKAT“. Die Daten verlieren dabei unwiderruflich ihren Personenbezug, bleiben jedoch für interne Zwecke wie insb. Controlling als Daten ohne Personenbezug erhalten. Die Software ermöglicht auch eine Pseudonymisierung, die jedoch im Zusammenhang mit dem Recht auf Löschung keine Anwendung findet, allerdings als Sicherheitsmaßnahme verwendet werden kann.

Um Daten vor unbeabsichtigtem Verlust sowie unbeabsichtigter Zerstörung und Schädigung zu schützen erfolgt die Sicherung sämtlicher Daten durch ein modernes Backup-Konzept. Nach einer Löschung bzw. Anonymisierung von Daten bleiben personenbezogene Daten in Form von Datensicherungen für eine gewisse Dauer bestehen. Im Sinne des § 4 Abs. 2 DSG kann eine Löschung oder Anonymisierung in Datensicherungen aus technischen Gründen nicht erfolgen. Nach Vornahme einer Löschung oder Anonymisierung für eine bestimmte Person sind spätestens nach zwei Jahren in Datensicherungen keine personenbezogenen Daten zu dieser Person mehr vorhanden.

Nach Vornahme einer Löschung bzw. Anonymisierung wird die betroffene Person über diese Maßnahme informiert.

1.2.5 Recht auf Einschränkung der Verarbeitung

Artikel 12, 18, 19 DSGVO – ErwG 58, 59, 67 DSGVO

Auf Wunsch einer Person, zu welcher Daten gespeichert sind bzw. verarbeitet werden, wird die Verarbeitung dieser Daten sofort vollständig gesperrt, sofern nicht berechtigte Gründe gegen die Einschränkung sprechen. Berechtigte Gründe sind bspw. ein aufrechtes Vertragsverhältnis, welches die Verarbeitung der Daten erfordert, gesetzliche Meldepflichten, denen ohne Verarbeitung der Daten nicht

entsprochen werden kann, die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, zum Schutz der Rechte einer anderen Person oder für ein wichtiges öffentliches Interesse.

Die Sperrung erfolgt durch Hinterlegung einer Verarbeitungssperre bei der Person in der Anwaltssoftware „ADVOKAT“, welche eine entsprechende Funktionalität anbietet. Die Hinterlegung einer Verarbeitungssperre hat zur Folge, dass bei jeder Initiation einer Verarbeitung von Daten zur betreffenden Person eine Warnmeldung ausdrücklich auf die Verarbeitungssperre hinweist („unmissverständlicher Hinweis im System“ gemäß ErwG 67 DSGVO).

Eine entsprechende Arbeitsanweisung sorgt dafür, dass sämtliche Mitarbeiter/innen diese Funktion kennen und dass im Falle einer solchen Meldung bis auf Weiteres keine Verarbeitung erfolgen darf.

Nach Hinterlegung einer Verarbeitungssperre wird die betroffene Person über diese Maßnahme informiert. Sobald der Grund für die Hinterlegung einer Verarbeitungssperre weggefallen ist, wird die betroffene Person informiert, dass die Sperre aufgehoben und die Verarbeitung der personenbezogenen Daten zur Verfolgung der vereinbarten Zwecke wiederaufgenommen wird.

Als zusätzliche Möglichkeit bietet die Anwaltssoftware „ADVOKAT“ die Möglichkeit, Akten gänzlich wegzusperren, um eine Verarbeitung zu verunmöglichen. Dies geschieht durch Anlage einer speziellen Security-Aktengruppe (z.B. „Verarbeitungsgesperrte Akten“) und der Einordnung eines zu sperrenden Akts in diese Gruppe.

1.2.6 Recht auf Datenübertragbarkeit

Artikel 12, 20 DSGVO – ErwG 58, 59, 68 DSGVO

Das Recht auf Datenübertragbarkeit verlangt die Möglichkeit, für eine betroffene Person alle diese betreffenden personenbezogenen Daten, die sie zur Verfügung gestellt hat, strukturiert exportieren zu können. Nicht Teil eines solchen Exportes sind Daten, die auf Grundlage dieser Daten von der Kanzlei erstellt wurden (z.B. Schriftsätze) (vgl. Artikel-29-Datenschutzgruppe, Working Paper 242, S. 8).

Im Rechtsanwaltsbereich sind hier vor allem Klient/innen angesprochen, da sich Beklagte, Zeug/innen, gegnerische Rechtsanwält/innen, Sachverständige, etc. nicht gegen die Verarbeitung der Daten durch von Klient/innen beauftragte Rechtsanwält/innen wehren können. In diese Richtung gehen auch die Ausführungen des ÖRAK („Vertreterwechsel“) (vgl. Leitfaden für Rechtsanwälte zur Datenschutz-Grundverordnung, 5.4.13).

Weil die zur Verfügungstellung von Daten vor allem in Form von Dokumenten und E-Mails erfolgt, empfehlen wir, im Bedarfsfall die Aktenordner, welche diese beinhalten, an Klient/innen zu übermitteln. Dazu empfehlen wir die Ablagestruktur „Ein Ordner pro Klient und ein Unterordner pro Gegner“.

Zusätzlich ermöglicht ADVOKAT die Erstellung eines Auskunftsberichts. Der Auskunftsbericht stellt umfangreich die zur Person gespeicherten Daten anschaulich zusammen. Darüber hinaus enthält der Auskunftsbericht sämtliche Informationen der Artikel 12 bis 15 DSGVO.

Auf Anfrage wird ein solcher Auskunftsbericht erstellt. Die Ausgabe erfolgt in Microsoft Word, wodurch eine allenfalls nötige Überarbeitung („Schwärzen“) möglich ist. Dies kann gem. ErwG 63 DSGVO im Einzelfall erforderlich sein, um die Freiheiten und Rechte anderer Personen zu schützen (z.B. Geschäftsgeheimnisse, Rechte des geistigen Eigentums).

Der Auskunftsbericht ist strukturiert aufgebaut und kann erforderlichenfalls maschinell verarbeitet werden. Gemeinsam mit der Übermittlung der digitalen Aktenordner und den darin enthaltenen Dateien kann dem Recht auf Datenübertragbarkeit einfach und schnell entsprochen werden.

1.2.7 Recht auf Widerspruch

Artikel 12, 21 DSGVO – ErwG 58, 59, 69, 70 DSGVO

Auf Wunsch einer Person („Widerspruch“), deren Daten zur Betreibung von Direktmarketing verwendet werden, wird die Verarbeitung der Daten für diesen Zweck sofort gesperrt.

Per Standard werden Daten einer Person nicht zu Direktmarketingzwecken verarbeitet (privacy by default), sondern nur durch entsprechende Nominierung der Person. Eine solche Nominierung erfolgt mit Hilfe der Anwaltssoftware „ADVOKAT“ durch Setzen der Information (z.B. „Newsletter: Ja/Nein“) bei der jeweiligen Person in einem dafür angelegten freien Feld.

Die Sperrung für Direktmarketing wird durch Entfernen der zu einem früheren Zeitpunkt gesetzten Information bei der betreffenden Person vollzogen.

Nach Vollziehung einer Direktmarketing-Sperre wird die betroffene Person über diese Maßnahme informiert.

Ein auf Artikel 6 Abs. 1 lit. e oder lit. f gestütztes Profiling findet nicht statt, sodass ein Widerspruch gegen ein solches mit einer entsprechenden Mitteilung beantwortet wird.

1.2.8 Keine automatisierte Entscheidung im Einzelfall

Artikel 12, 22 DSGVO – ErwG 58, 59, 71, 72 DSGVO

Entscheidungen, welche rechtliche Wirkungen oder erhebliche Beeinträchtigungen für betroffene Personen zur Folgen haben, werden in keinem Fall automatisiert gefällt. Eine Anfrage in diese Richtung wird durch Darlegung der Entscheidungswege beantwortet.

1.3 Sichere Datenhaltung

1.3.1 ADVOKAT Desktop

Bei der Datenhaltung werden folgende Datengruppen unterschieden:
- Daten in Datenbanken
- Dateien (insb. Word- und PDF-Dokumente)
- Systemdateien

1.3.1.1 Daten in Datenbanken

Die allermeisten Daten werden in Datenbanken gespeichert. ADVOKAT bietet hierfür zwei verschiedene Möglichkeiten an:

- Microsoft Access Datenbanken (MDB-Dateien)
- Microsoft SQL Datenbanken

Aus Sicherheitsgründen wird empfohlen, Microsoft SQL Datenbanken zu verwenden. Gegenüber Microsoft Access Datenbanken ergeben sich folgende Sicherheitsvorteile (vgl. *https://msdn.microsoft.com/en-us/library/bb421308(v=office.12).aspx*):

- **Trennung des Datenzugriffs vom Zugriff auf die Datenbankdatei**
  Bei Microsoft Access Datenbanken ist ein Zugriff auf die Datenbankdatei notwendig, um auf die Daten zugreifen zu können. Dadurch kann die Datei von allen Personen, welche auch nur beschränkten Zugriff auf die Daten haben, missbräuchlich verwendet werden (löschen, stehlen, hacken).
  Bei Microsoft SQL Datenbanken sorgt ein SQL Serverprozess für eine Trennung, d.h. dass nur der SQL Serverprozess Zugriff auf die Datenbankdateien hat, währende Anwender lediglich mit dem SQL Serverprozess kommunizieren, welcher die Daten aus den Datenbanken zur Verfügung stellt.

- **Sicheres Authentifizierungsverfahren**

Zwar sind die von ADVOKAT angelegten Microsoft Access Datenbanken durch ein Kennwort geschützt, doch ist der bei MDB-Dateien zum Einsatz kommende Verschlüsselungsstandard nicht aktuell, sodass entschlossene Benutzer/innen in der Lage sein werden, das Kennwort zu knacken. Bei Verwendung von Microsoft SQL Datenbanken wird die Authentifizierung vom SQL Serverprozess vorgenommen. Microsoft publiziert alle paar Jahre eine neue SQL Server Version, womit auch die Sicherheitsstandards mit der Zeit mitwachsen.

- **Volle Kompatibilität mit ADVOKAT Security**
  Microsoft SQL Datenbanken ermöglichen deutlich höhere Verarbeitungsgeschwindigkeiten, sodass die bedeutsame Sicherheitsfunktion zur Einschränkung des Zugriffs auf Akten (Recht „Akt sehen“) nur mit Microsoft SQL Datenbanken zur Anwendung kommt.

In kleineren Kanzleiorganisationen kann die Verwendung von Microsoft Access Datenbanken unter Umständen ausreichende Sicherheit gewähren. Voraussetzung dafür sind entsprechende Maßnahmen um sicherzustellen, dass nur Berechtigte Zugang zu den Systemen bekommen (Absicherung der Kanzleiräumlichkeiten, Windows-Anmeldung, Sicheres Netzwerk).

Um dieser Empfehlung Rechnung zu tragen, wird das ADVOKAT Setup so ausgestaltet, dass bereits bei Installation die Verwendung von Microsoft SQL Datenbanken gewählt werden kann und als empfohlene Variante auch nahegelegt wird (privacy by design & privacy by default).

1.3.1.2 Dokumente und Dateien in ADVOKAT

Wenn Dateien (insbesondere Word- und PDF-Dokumente) in ADVOKAT erzeugt und/oder verwaltet werden (z.B. Dokumente in Akten), bleiben diese Dateien als Dateien bestehen. Eine Datei ist durch einen Dokumentdatensatz mit ADVOKAT verknüpft. ADVOKAT bietet zwei verschiedene Möglichkeiten zur Verwaltung der Dateien an:

- Verwaltung im Dateisystem
- Verwaltung im Dokumentenmanagementsystem Microsoft SharePoint

Bei Verwaltung im Dateisystem sind die Dateien grundsätzlich allen ADVOKAT Anwender/innen, z.B. via Windows Explorer, unbeschränkt zugänglich. Dies gilt selbst dann, wenn einzelnen Anwender/innen der Zugriff auf manche Akten in ADVOKAT via ADVOKAT Security versperrt wurde. Zu möglichen Schutzmaßnahmen in diesem Kontext siehe gleich unten (*„Dateien im Dateisystem schützen“*).

Bei Verwaltung in Microsoft SharePoint erfolgt ein Zugriff auf die Dateien nicht direkt, sondern mittelbar durch Kommunikation mit einem SharePoint-Serverprozess. Aufgrund des SharePoint-Berechtigungssystems, welches mit dem Berechtigungssystem in ADVOKAT (Security) gekoppelt werden kann, ist ein effektiver und effizienter Schutz der Dateien möglich. So können bspw. Anwender/innen, welche auf bestimmte Akten keinen Zugriff haben, die in diesen Akten enthaltenen Dokumente und Dateien auch nicht via Explorer oder SharePoint-Web-Oberfläche sehen; die Aktenordner und die darin befindlichen Dateien sind für diese Anwender/innen nicht vorhanden.

Die Anschaffung und Verwendung von Microsoft SharePoint ist üblicherweise mit einmaligen und laufenden Kosten verbunden. Zwar ist Microsoft SharePoint auch in einer kostenlosen Ausführung erhältlich, doch ist unter Umständen die Anschaffung leistungsfähigerer Hardware erforderlich. Weiters wird für die laufende Betreuung der IT ein dafür qualifiziertes Personal benötigt.

In kleineren Kanzleiorganisationen kann die Verwaltung im Dateisystem ohne zusätzliche Schutzmaßnahmen für die Dateien unter Umständen ausreichende Sicherheit gewähren. Voraussetzung dafür sind entsprechende Maßnahmen um sicherzustellen, dass nur Berechtigte Zugang zu den Systemen bekommen (Absicherung der Kanzleiräumlichkeiten, Windows-Anmeldung, Sicheres Netzwerk).

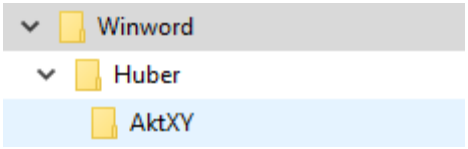
1.3.1.2.1 Dateien im Dateisystem schützen

Wenn Sie der Meinung sind, dass die Verwaltung im Dateisystem ohne zusätzliche Schutzmaßnahmen nicht die erforderliche Sicherheit gewährleistet, Sie aber Microsoft SharePoint nicht verwenden möchten, gibt es ein paar Möglichkeiten, den Schutz der Dateien im Dateisystem zu verbessern.

Sensible Akten schützen oder Aktengruppen fixieren

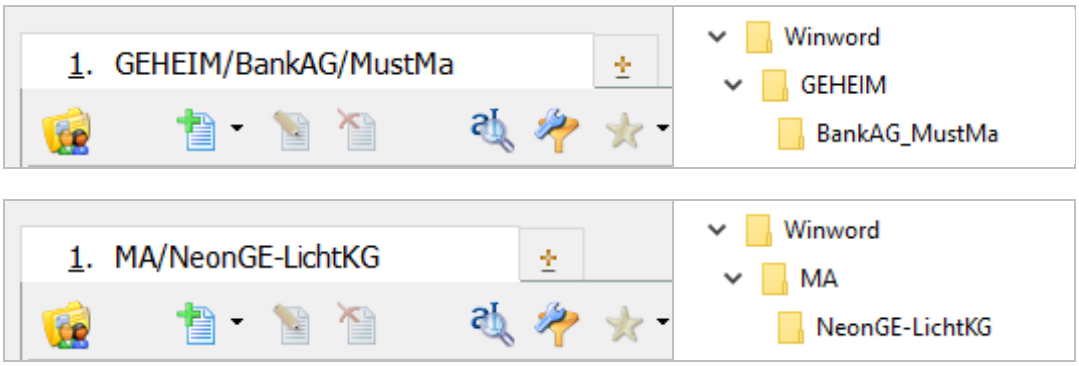
Sie haben die Möglichkeit, die Ordnerstruktur für ADVOKAT-Dateien so zu definieren, dass sich diese aus der Aktenkurzbezeichnung wie folgt ergibt:
Erster Namensteil = Hauptordner (Aktengruppe)
Zweiter Namensteil = Unterordner (Einzelner Akt)

Beispiel: Die Aktenkurzbezeichnung lautet „Huber/AktXY“.
ADVOKAT legt für diesen Akt folgende Ordner an:



Mit dieser Konfiguration kann bspw. der Zugriff auf alle Akten eines Herrn Dr. Huber auf jene Personen eingeschränkt werden, welche diesen Zugriff benötigen, während alle anderen Personen davon ausgeschlossen werden können. Dies erreichen Sie durch Definition entsprechender Berechtigungen für den Ordner „Huber“ im Dateisystem (Windows-Berechtigungen).

Diese Ablagestruktur kann auch so verwendet werden, dass nur einzelne (sensible) Akten mit eingeschränkten Zugriffsrechten behandelt werden oder durch Organisierung nach Fachbereichen oder Abteilungen:



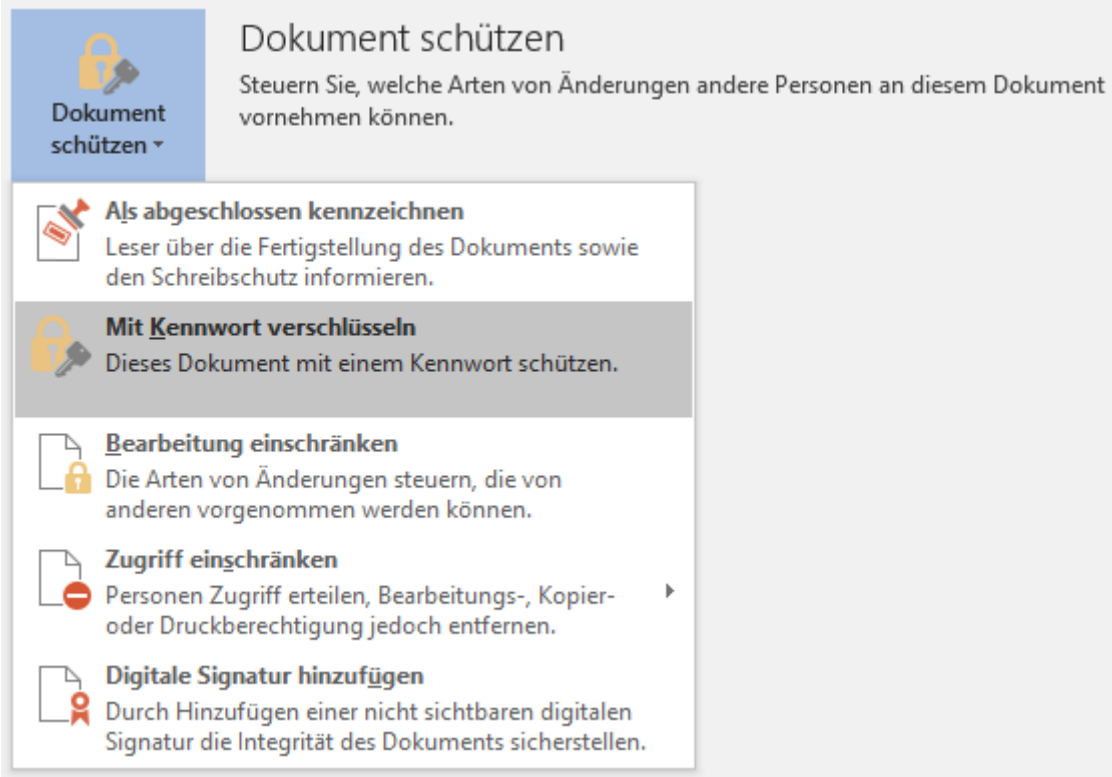
Um diese Ablagestruktur zu verwenden, klicken Sie im ADVOKAT Startbildschirm auf *„System / Einstellungen / Dokumente / Weitere Einstellungen ...“* und wählen Sie *„Ein Ordner pro Klient und ein Unterordner pro Gegner“*. Lassen Sie sich von der Bezeichnung der Option nicht irritieren. Diese ist so gewählt, weil Akten häufig mit „<Klient/in>/<Gegner/in>“ benannt werden.

Nachteil dieser Lösung ist, dass die Zugriffsrechte wenig flexibel sind, d.h., dass die Änderung der Zugriffsrechte für einen Akt nur auf zwei Weisen erfolgen kann:
- Umbenennung des Aktes (dadurch wird auch die Ordnerstruktur aktualisiert)
- Änderung der Berechtigungen im Dateisystem

Dateien mit Kennwort verschlüsseln

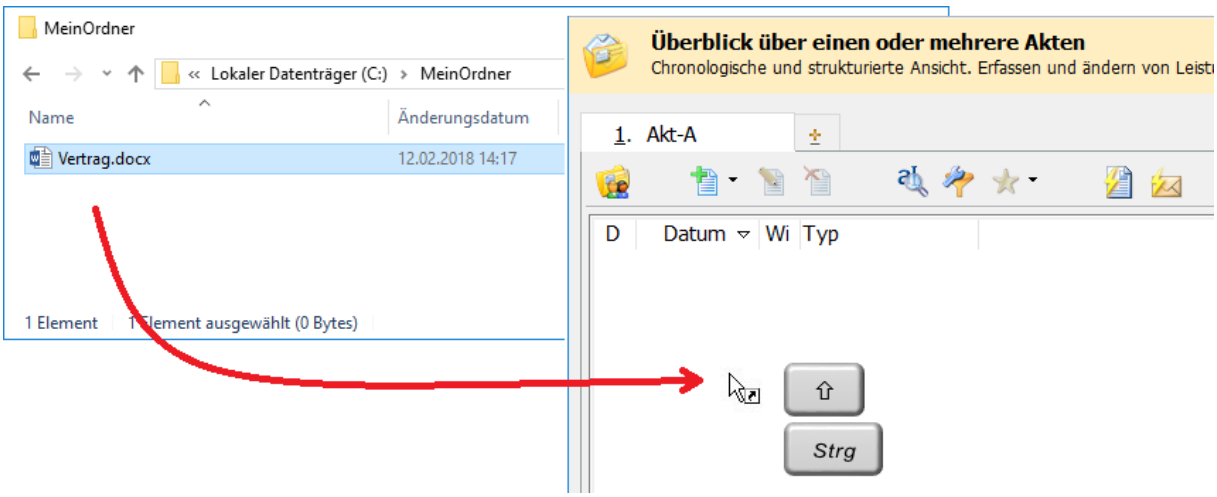
Office-Dateien (Word, Excel) sowie PDF-Dateien können mit einem Kennwort geschützt werden. Dabei wird die jeweilige Datei verschlüsselt. Beim Öffnen der Datei ist die Eingabe des Kennworts erforderlich.

Bspw. kann in Microsoft Word ein Kennwortschutz via „Datei / Informationen / Dokument Schützen / Mit Kennwort verschlüsseln“ aktiviert werden.



Sensible Dokumente auslagern

Ein Dokumentendatensatz in ADVOKAT kann jede beliebige Datei im Dateisystem mit ADVOKAT verbinden. Es besteht daher die Möglichkeit, einzelne Dateien an einem sicheren Ort abzuspeichern (z.B. abgesicherter Ordner am Server, verschlüsseltes Verzeichnis, verschlüsselte externe Festplatte) und diese nicht in den Aktenordner zu übernehmen. Dies können Sie erreichen, indem Sie eine Datei mit der Maus in den Akt hineinziehen (Drag & Drop), während Sie die Strg-Taste und die Hochstell-Taste (Shift-Taste) gedrückt halten.



Alte (abgelegte) Akten archivieren

Sie können die Dokumente (Dateien) von alten Akten archivieren. Alte Akten können Sie z.B. am Ablagedatum (Suche im ADVOKAT Suchassistent) oder am letzten Änderungsdatum der Aktenordner erkennen. Die Archivierung können Sie auf verschiedene Weisen vornehmen. Beispiele:

- die Dateien in einen sicheren Ordner verschieben (z.B. abgesicherter Ordner am Server, verschlüsseltes Verzeichnis, verschlüsselte externe Festplatte),

- die Dateien im Ordner in ein kennwortgeschütztes Archiv verpacken (z.B. Zip-Datei),
- die Windows-Berechtigungen für diese Ordner ändern.

Dateien verschlüsseln

Mit Verschlüsselungssoftware können Sie die Dateien eines, mehrerer oder sämtlicher Akten verschlüsseln. Es gibt verschiedene Lösungen. So gibt es bspw. die Möglichkeit, ein Verzeichnis (z.B. das Hauptverzeichnis für alle Akten) wie einen Tresor zu behandeln. Diesen Tresor kann man auf- und zusperren. Nachteil dieser Lösung ist, dass der Tresor die meiste Zeit über offen sein müsste, um nicht das Arbeiten zu blockieren. Zwar könnten auch einzelne Aktenorder zu einzelnen Tresoren gemacht werden, doch wäre der Administrationsaufwand sehr hoch.

Eine andere Verschlüsslungslösung verschlüsselt die Dateien permanent, erlaubt jedoch den Zugriff für definierte Benutzer/innen. Vorteile einer solchen Lösung sind vor allem der ununterbrochene Schutz sowie eine Verwaltung mit Benutzer/innen und -gruppen für auszuwählende Verzeichnisse.

1.3.1.2.2 Sicherheitsvorteile von Microsoft SharePoint

Hauptsicherheitsvorteil ist, wie oben bereits angesprochen, das mit dem Berechtigungssystem in ADVOKAT (Security) gekoppelte SharePoint-Berechtigungssystem. So können bspw. Anwender/innen, welcher auf bestimmte Akten keinen Zugriff haben, die in diesen Akten enthaltenen Dokumente und Dateien auch nicht via Explorer oder SharePoint-Web-Oberfläche sehen; die Aktenordner und die darin befindlichen Dateien sind für diese Anwender/innen nicht vorhanden.

Die Berechtigungen auf Dateiebene sind damit immer deckungsgleich mit den Berechtigungen in ADVOKAT. Änderungen in ADVOKAT werden unmittelbar in SharePoint vollzogen.

Ein weiteres Sicherheitsfeature von SharePoint ist der Manipulationsschutz. Wenn Word-Dokumente bearbeitet werden, wird nicht das bestehende Dokument durch das bearbeitete Dokument ersetzt, sondern legt SharePoint eine zusätzliche Dokumentversion an. So kann der Zustand des Dokuments zu jedem Zeitpunkt festgestellt werden. Die Versionshistorie gibt Aufschluss darüber, wer das Dokument wann bearbeitet hat. Ein Versionskommentar hilft dabei, den Lebenszyklus des Dokuments auf einem Blick zu erfassen.

Abhängig von der Ausstattungsvariante könne noch mehr Sicherheitsfunktionen von Microsoft SharePoint genutzt werden. Zu diesen gehören etwa Protokollierungsfeatures sowie definierbare Ereignisse, welche Alarme auslösen (z.B. bei massenhaften Operationen).

1.3.1.3 Systemdateien

Systemdateien sind im Dateisystem gespeicherte Daten, welche ADVOKAT Desktop für die Erledigung der erforderlichen Aufgaben erzeugt und bearbeitet. In aller Regel enthalten diese Dateien keine personenbezogenen Daten und dienen bspw. der Speicherung von Konfigurationen oder der technischen Protokollierung (kritische Ereignisse, Fehlermeldungen). In Ausnahmefällen können diese Dateien aber auch personenbezogene Daten beinhalten, weshalb diese von ADVOKAT geschützt werden.

ERV Nachrichten

Im ERV versendete und empfangene Nachrichten werden in einem proprietären Dateiformat abgespeichert. Zusätzlich werden diese Dateien mit AES-256 verschlüsselt. Dieser Verschlüsselungsstandard gilt derzeit als am sichersten.

Upload für Internet-Akteneinsicht

Beim Hochladen von Akten für die Internet-Akteneinsicht wird ein Statistik-Bericht erstellt, hochgeladen und unmittelbar im Anschluss gelöscht.

DFU-Verzeichnis

Im DFU werden diverse Exporte abgelegt. Die Anwender/innen werden jeweils darauf hingewiesen. Diese Exporte werden unmittelbar von den Anwender/innen benötigt, weshalb diese nicht geschützt werden. Anwender/innen sollten diese Dateien daher immer sofort löschen. Beispiele: Export von Überweisungen für den Import in einer Electronic Banking Software, Exporte aus der Buchhaltung (CSV-Export), Zusammenfassende Meldung

1.3.2 ERV, ADVOKAT Online & ADVOCOM

Die Verarbeitung sämtlicher ERV-Nachrichten, Abfragen via ADOVKAT Online und Kommunikationen via ADVOCOM werden über Server abgewickelt, welche ausschließlich von ADVOKAT betrieben werden. Die Server befinden sich in hochmodernen Rechenzentren in Österreich. Nur ADVOKAT hat Zugang zu diesen Servern.

Die Server sind durch eine Firewall und einen Virenschutz geschützt. Diese werden ständig aktuell gehalten.

Die Verfügbarkeit der Dienste wird durch redundante Server mit gegenseitiger Spiegelung sichergestellt.

Ein modernes Backup-Konzept schützt die Daten vor Verlust und Zerstörung.

Bei der Nutzung von ADVOCOM sollten Daten (z.B. Kommunikationen) gelöscht werden, sobald diese nicht mehr kommunikationsrelevant sind. Eine darüberhinausgehende (für andere Zwecke) längere Aufbewahrung sollte durch Übernahme von Nachrichten und Dateien oder ganzer Kommunikationsverläufe nach ADVOKAT erfolgen.

1.3.3 ADVOKAT mobil

Die Speicherung von Daten am Mobilgerät erfolgt in einer SQLite-Datenbank. Auch werden Dateien am Mobilgerät gespeichert, welche mit anderen Apps (bspw. der Word-App von Microsoft) geöffnet werden können.

Um diese Daten zu schützen, sollte das Mobilgerät so konfiguriert sein, dass sämtliche Daten verschlüsselt gespeichert werden. Bei iOS ist dies Standard, bei Android gibt es die Möglichkeit, dies zu aktivieren. Zusätzlich sollte eine gesicherte Anmeldung eingerichtet werden (siehe dazu beim Kapitel „Zugangssicherung“). Damit ist sichergestellt, dass die Daten auch bei Verlust oder Diebstahl des Mobilgerätes geschützt sind.

1.3.4 Internet-Akteneinsicht

Die mit der Internet-Akteneinsicht zur Verfügung gestellten Daten werden auf ADVOKAT Servern gespeichert. Es gilt das bei „ERV & ADVOKAT Online“ Gesagte.

1.4 Zugangssicherung

Zugangssicherung umfasst technisch gesprochen die Authentisierung, Authentifizierung und Autorisierung. Einfacher ausgedrückt ist dies die Anmeldung am System (ADVOKAT Desktop, ERV, ADVOKAT Online, ADVOKAT mobil, Internet-Akteneinsicht) und das Gewähren von konkreten Rechten für die angemeldeten Benutzer/innen.

1.4.1 ADVOKAT Desktop

1.4.1.1 Anmeldung

Eine sichere Anmeldung kann auf zwei Weisen erfolgen:

- Vergabe eines Kennwortes für ADVOKAT-Sachbearbeiter/innen
- Koppelung der ADVOKAT-Sachbearbeiter/innen mit Windows-Benutzer/innen (Windows-Authentifizierung)

Vergabe eines Kennworts für ADVOKAT-Sachbearbeiter/innen

In „Programme / Tabellen warten / Benutzer und Gruppen“ können Sie Benutzer/innen und -gruppen verwalten. Auch können Sie Kennwörter für Sachbearbeiter/innen vergeben und ein Kennwortintervall hinterlegen. Bei Hinterlegung eines Kennwortintervalls werden Sachbearbeiter/innen nach Verstreichen des Intervalls zur Vergabe eines neuen Kennworts aufgefordert. Im Anschluss beginnt das Intervall von neuem zu laufen. Zusätzlich können Sachbearbeiter/innen ihre Kennwörter via „System / Kennwort ändern“ jederzeit ändern.

Windows-Authentifizierung

In „Programme / Tabellen warten / Benutzer und Gruppen“ können Sie Benutzer/innen und -gruppen verwalten. Sie können hier auch ADVOKAT Sachbearbeiter/innen mit Windows-Benutzer/innen koppeln. Wenn Sie dies tun, entfällt die Notwendigkeit einer Kennworteingabe beim Starten von ADVOKAT, da die Sicherung des Zugangs durch die Windows-Anmeldung erfolgt.

Empfehlung

ADVOKAT empfiehlt die Windows-Authentifizierung. Diese ist nicht nur komfortabler in der Anwendung, sondern sollte ohnehin ein gesicherter Zugang zu Rechnern eingerichtet werden, zumal auf den Rechnern personenbezogene Daten in vielfältiger Weise vorliegen können (Dateien am Desktop oder in temporären Ordnern, diverse Software wie z.B. E-Mail-Clients mit unter Umständen fehlenden oder unbekannten Sicherheitsstandards).

1.4.1.2 Autorisierung – ADVOKAT Security

Wenn sich eine Person erfolgreich bei ADVOKAT angemeldet hat, stellt sich noch die Frage, was diese Person in ADVOKAT alles sehen und tun darf. Diese Frage beantwortet das Berechtigungssystem „ADVOKAT Security“.

Für die Einrichtung und Administration von ADVOKAT Security sind zwei Bereiche wesentlich:
- Programme / Tabellen warten / Benutzer und Gruppen
- Programme / Tabellen warten / Security

In „Benutzer und Gruppen“ können Sie Benutzergruppen anlegen und Benutzer/innen in Gruppen organisieren. Benutzer/innen kann Mitglied beliebig vieler Benutzergruppen sein.

In „Security“ können Sie für einzelne Benutzer/innen und -gruppen Rechte für Programmbereiche sowie für einzelne Akten oder Aktengruppen definieren.

Wir empfehlen, soweit es nur sinnvoll möglich ist, mit Benutzergruppen und Aktengruppen zu arbeiten, um Übersichtlichkeit und Flexibilität zu wahren. Ein solcherart umgesetztes, durchdachtes Berechtigungskonzept erspart die Auseinandersetzung mit Berechtigungsfragen im laufenden Betrieb sowie bei fluktuierendem Personal.

Um Personen zu schützen, kann im Personenstamm eine ausschließlich berechtigte Benutzergruppe hinterlegt werden. Die Person kann dann nur von Mitgliedern dieser Benutzergruppe gesehen und verarbeitet werden.

ADVOKAT Security und Datenbanken

Microsoft SQL Datenbanken ermöglichen deutlich höhere Verarbeitungsgeschwindigkeiten als Microsoft Access Datenbanken, sodass die bedeutsame Sicherheitsfunktion zur Einschränkung des Zugriffs auf Akten (Recht „Akt sehen“) nur mit Microsoft SQL Datenbanken zur Anwendung kommt.

ADVOKAT Security und Dateien

Bei Verwaltung von Dateien im Dateisystem sind die Dateien grundsätzlich allen ADVOKAT Anwender/innen, z.B. via Windows Explorer, unbeschränkt zugänglich. Dies gilt selbst dann, wenn einzelnen Anwender/innen der Zugriff auf manche Akten in ADVOKAT via ADVOKAT Security versperrt wurde. Siehe im Detail hierzu beim Kapitel *„Sichere Datenhaltung“*.

1.4.2 ERV, ADVOKAT Online & ADVOCOM

1.4.2.1 Anmeldung im ERV

Um Ihre Identität bei der Teilnahme am ERV (Senden und Empfangen von ERV-Nachrichten) sicherzustellen, stellen wir Softwarezertifikate aus. Dabei kommt der SHA-2-Standard zum Einsatz. Jedes Mal, wenn Sie in ADVOKAT eine Verbindung zu unseren Servern aufbauen (via „Senden/Empfangen“) erfolgt im Hintergrund eine solche Anmeldung. Dies geschieht verschlüsselt über einen sicheren Kanal (HTTPS).

Die Berechtigungen für die Verwendung des ERVs können Sie wiederum in ADVOKAT Desktop via Security bestimmen.

1.4.2.2 Anmeldung bei ADVOKAT Online & ADVOKAT Online Diensten

Sie können ADVOKAT Online via Browser aufrufen und sich dort durch Eingabe von Benutzername und Kennwort anmelden. Alternativ können Sie die Zugangsdaten in ADVOKAT Desktop hinterlegen und ADVOKAT Online direkt aus der Aktenverwaltung aufrufen. In diesem Fall werden die hinterlegten Zugangsdaten im Hintergrund verschlüsselt über eine gesicherte Verbindung (HTTPS mit TLS-Transportverschlüsselung) übermittelt.

Die in ADVOKAT Desktop hinterlegten Zugangsdaten werden verschlüsselt gespeichert.

Für alle ADVOKAT Online Dienste (inkl. ADVOCOM) fungiert ein hochmoderner Anmeldedienst nach dem Open ID Connect Standard (auf Basis von OAuth 2.0) als zentrale Stelle zur Anmeldung und Autorisierung.

1.4.2.3 Autorisierung in ADVOKAT Online

In ADVOKAT Online können Sie beliebig viele Benutzer/innen anlegen. Zu Beginn gibt es nur die/den Hauptbenutzer/in (z.B. „KANZLEI“). Zusätzlich angelegte Benutzer/innen lauten bspw. „KANZLEI/MM“ (als Bsp. für eine/n Sachbearbeiter/in mit Kürzel „MM“). Hauptbenutzer/innen können Kennwörter für alle Benutzer/innen festlegen und zurücksetzen. Die Benutzer/innen können auch selbst ihre eigenen Kennwörter ändern.

Weiters können Hauptbenutzer/innen Rechte für alle Benutzer/innen festlegen und so den Zugang zu Daten in ADVOKAT Online steuern.

In ADVOKAT Desktop können für alle Sachbearbeiter/innen unterschiedliche ADVOKAT Online Zugangsdaten hinterlegt werden, sodass sich alle Kanzleimitarbeiter/innen mit ihren persönlichen ADVOKAT Online Benutzer/innen in ADVOKAT Online anmelden.

1.4.3 ADVOKAT mobil

Um ADVOKAT mobil verwenden zu können, muss ein Webservice von ADVOKAT im Kanzleinetzwerk eingerichtet werden. ADVOKAT mobil (am Mobilgerät) kommuniziert mit diesem Webservice (im Kanzleinetzwerk) verschlüsselt über eine sichere Verbindung (HTTPS). Um dies zu ermöglichen gibt es zwei Möglichkeiten:

- VPN-Verbindung
- Portweiterleitung

Details zu diesen beiden Möglichkeiten können Sie der aktuellen Dokumentation zu ADVOKAT mobil entnehmen, welche Sie jederzeit beim ADVOKAT Support anfordern können.

Aus Sicherheitsgründen empfehlen wir die Verwendung einer VPN-Verbindung, da diese ein deutlich höheres Sicherheitsniveau gewährt. Dies hat den wesentlichen Mehrwert, dass die Kommunikationsstelle „Kanzleiserver“ vor externen Angreifer/innen geschützt ist, welche Schwachstellen im Betriebssystem ausnutzen wollen.

1.4.4 Internet-Akteneinsicht

Das Hochladen von Aktendaten auf die ADVOKAT Server sowie sämtliche Kommunikation (z.B. das Einsehen von Akten durch Klient/innen) erfolgt verschlüsselt über eine sichere Verbindung (HTTPS).

Damit eine Person Zugang zu Aktendaten bekommt, muss diese sich auf der Website mit Benutzerkennung und Kennwort anmelden. Diese Zugangsdaten werden von der publizierenden Kanzlei definiert und beim Aktenupload am ADVOKAT Server aktualisiert.

1.5 Sicherheitsprotokollierung

Bei Protokollierung ist zu unterscheiden zwischen technischer Protokollierung (Fehlermeldungen, kritische Ereignisse) und Sicherheitsprotokollierung. Sicherheitsprotokollierung umfasst die Protokollierung sicherheitsrelevanter Vorgänge, welche zur Vorbeugung von Datenschutzverletzungen und/oder zur Nachforschung nach einer Datenschutzverletzung dienen können.

1.5.1 ADVOKAT Desktop

ADVOKAT Security beinhaltet eine Sicherheitsprotokollierung. Diese protokolliert Zugriffe auf diverse Datenobjekte (Akten, Personen, Dokumente, ERV-Nachrichten, etc.) sowie die Ausgabe von Daten an sehr vielen Stellen. Vor allem für den Fall einer Datenschutzverletzung können diese Protokolle wesentliche Informationen für eine Analyse liefern.

Bei Verwendung von Microsoft SharePoint entsteht durch die automatische Versionierung von Dokumenten eine Historie zum Dokument. Je Version werden Zeitpunkt und Benutzer/in dokumentiert.

Abhängig von der Ausstattungsvariante verfügt Microsoft SharePoint auch über umfangreiche Protokollierungsfeatures. Auch können Ereignisse definiert werden, welche Alarme auslösen (z.B. bei massenhaften Operationen).

1.5.2 ERV

Der Übermittlungsvorgang jeder ERV-Nachricht (Hin- und Rückverkehr) wird umfangreich dokumentiert.

1.5.3 ADVOKAT Online

Viele sicherheitsrelevante Vorgänge werden protokolliert und sind für Hauptbenutzer/innen in der Ereignisanzeige einsehbar. Beispiele für protokollierte Vorgänge: Login (auch Fehlversuche), Logout, Kennwortänderung und -zurücksetzung, Aktionen der Benutzer/innen- und Rechteverwaltung, Zugriffe durch ADVOKAT (im Supportfall)

Jeder Protokolleintrag nennt Datum, Uhrzeit, Benutzer/in, IP-Adresse sowie ereignisabhängige Zusatzinformationen.

1.5.4 ADVOKAT mobil

Jede einzelne Datenübertragung wird protokolliert. Festgehalten werden Datum, Uhrzeit, Gerät (UDID) und Datenkategorien.

1.5.5 Internet-Akteneinsicht

Für die Internet-Akteneinsicht wird eine Protokollierung sämtlicher Uploadvorgänge (inkl. Uploadinhalte) und Zugriffe geschaffen. Durch ein entsprechendes Feature kann das Protokoll eingesehen werden.