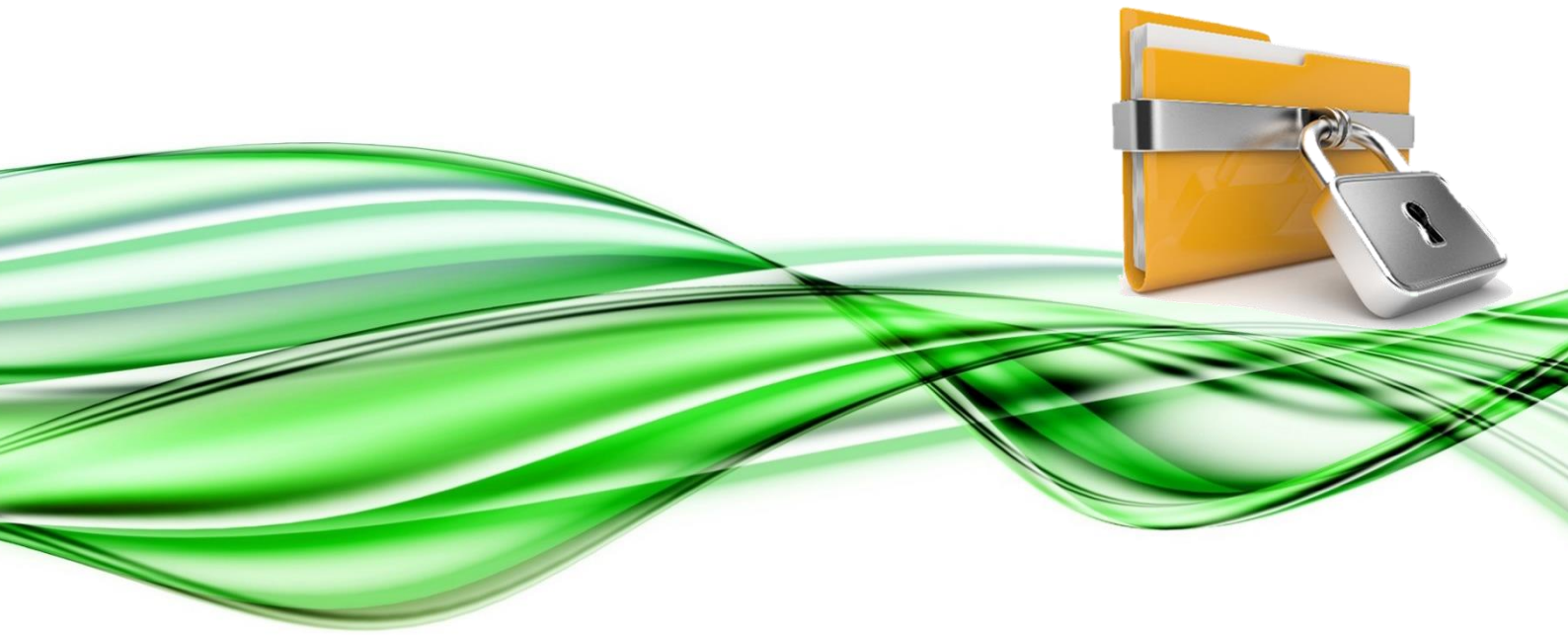
Datenschutz-Grundverordnung
Verarbeitungsverzeichnis



Stammdaten des Verantwortlichen gem Art 4 Z 7 DSGVO

Name: Mag. Marcus Hohenecker; Rechtsanwalt
Adresse: Kaiser Franz Josef-Straße 7, 2301 Groß-Enzersdorf
Tel.: +43 660 343 70 70
E-Mail: anwalt@hohenecker.at

1. Verarbeitungsverzeichnis

1.1 Haupttätigkeiten

1.1.1 Aktanlage (Datenerfassung, Kollisionsprüfung, Vollmacht, Stammdaten, GwG-Prüfung)

1.1.1.1 Kurzbeschreibung

Im Zusammenhang mit der anwaltschaftlichen Vertretung und Beratung von Personen werden Akten und in die Causa involvierte Personen angelegt, die Personen und Aktendaten werden im Akt erfasst, und dort weiterbearbeitet und -verarbeitet.

Dieser Verarbeitungsvorgang umfasst sämtliche Vorgänge vor Beginn der eigentlichen Aktbearbeitung (Erfassen aller benötigten Daten zur Person, Prüfung auf Interessenkollision, Einholen der Vollmacht, Anlage von Personen und Einpflegen der Stammdaten, Anlage des Aktes und Einpflegen von Stammdaten, Überprüfung gemäß der Geldwäsche-Richtlinie). Der Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“ schließt direkt an diesen an.

1.1.1.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die rechtsanwaltliche Vertretung von Auftraggebern im Umfang des jeweiligen Mandats, die Leistung rechtsanwaltlicher Dienste für Auftraggeber im Umfang des Auftrages sowie die rechtliche Beratung von Auftraggebern.

1.1.1.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige.
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird eine Datenschutzmitteilung übersendet.

Kategorie C	Alle im System vorhandenen Personen
Anmerkungen zur Personenkategorie	Alle Personen, welche im Adressbestand des Systems vorhanden sind.
Rechtsgrundlage für diese Personenkategorie	**Rechtliche Verpflichtung (von Rechtsanwält/innen) der Kanzlei (Art. 6 Abs. 1 lit. c DSGVO):** Um das Doppelvertretungsverbot (§ 9 Abs. 1 und § 10 Abs. 1 RAO, §§ 10 und 12a RL-BA) zu achten und zu wahren, ist für alle potentiellen Klient/innen und Gegner/innen einer Causa eine mögliche Interessenkollision zu prüfen. Dies erfolgt durch Abgleich mit den im System (aus früheren Causen) vorhanden Personen.
Erfüllung der Informations-pflichten für diese Personenkategorie	<u>Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO):</u> Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. <u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird eine Datenschutzmitteilung übersendet.

Kategorie D	Gerichte und Behörden inkl. Kontaktpersonen bei diesen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der jeweiligen Causa befasste Gerichte (zuständige Zivil- und Strafgerichte) und Behörden (z.B. Finanzämter, Vermessungsämter, Grundverkehrsbehörden, Bezirkshauptmannschaften, Gemeinden, Kammern).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie E	Kanzleimitarbeiter/innen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der Aktanlage werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet (z.B. zuständige/r Rechtsanwält/in, zuständige/r Sachbearbeiter/in, aktbezogene Stundensätze). Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.1.1.4 <u>Kategorien der verarbeiteten Daten und Empfänger</u>

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger								
				ADVOKAT & KSV[1)]	Ggf. IT-Support[2)]							

A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X								
	2	Foto	Nein		X								
	3	Anschrift	Nein	X	X								
	4	Kontaktdaten (Tel., Mail, Fax)	Nein		X								
	5	Bank- und Überweisungsdaten	Nein		X								
	6	Geburtsdatum	Nein	X	X								
	7	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein		X								
	8	UID-, FB-, ZVR-Nummer	Nein	X	X								
	9	Sozialversicherungsdaten	Nein		X								
	10	Kontaktpersonen und deren Kontaktdaten	Nein		X								
	11	Beteiligte Personen (Aktbeteiligte Personen, Gerichte und Behörden)	Nein		X								
	12	Abrechnungsdaten	Nein		X								
	13	GwG-Daten[1)]	Nein		X								
C	14	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein		X								
	15	Anschrift	Nein		X								
	16	Kontaktdaten	Nein		X								
	17	Geburtsdatum	Nein		X								
	18	UID, FB-, ZVR-Nummer	Nein		X								
	19	Sozialversicherungsdaten	Nein		X								
D	20	Kontaktpersonen und deren Kontaktdaten	Nein		X								
E	21	Name	Nein		X								
	22	Funktion in der Kanzlei	Nein		X								

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] ADVOKAT & KSV, GwG-Daten: Aufgrund der §§ 8aff RAO (basierend auf der vierten Geldwäsche-Richtlinie – RL 2015/849) muss bei jedem neuen Mandat eine Prüfung vorgenommen werden, ob ein Geldwäsche geneigtes Geschäft vorliegt. Dies erfolgt durch eine Compliance Check Abfrage, welche an die ADVOKAT Unternehmensberatung Greiter & Greiter GmbH (als Auftragsverarbeiterin) gesendet und von dieser an die KSV1870 Information GmbH (Sub-Auftragsverarbeiterin) weitergeleitet wird. Dabei werden zur Identifizierung der zu prüfenden Person erforderliche Daten übermittelt und ein Prüfungsergebnis (GwG-Daten) wird auf demselben Weg zurückgeliefert.

[2)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.1.1.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
ADVOKAT & KSV	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.1.1.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt in Erfüllung der rechtsanwaltlichen Aufbewahrungspflichten gemäß § 12 RAO für die Dauer von fünf Jahren ab Abschluss der jeweiligen Causa und umfasst sämtliche Datenkategorien. Der Abschluss wird durch Vergabe eines Ablagedatums je Akt dokumentiert, wodurch ein systemisches Bereinigen (Löschen von alten Akten) möglich ist.

Soweit es zur Abwehr etwaiger Schadenersatzansprüche erforderlich ist, werden die Daten eines Aktes und der involvierten Personen für die Dauer von 30 Jahren (lange Verjährungsfrist) ab Abschluss der jeweiligen Causa aufbewahrt.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT" Möglichkeiten, welche den Schutz der Daten, die über den Abschluss einer Causa hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs").

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT" sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.1.1.7 Datenminimierung

Nicht nur zur Sicherung eines hohen Datenschutzniveaus, sondern auch für eine schlanke und effiziente Kanzleiverwaltung werden ausschließlich Daten erfasst, welche für die Bearbeitung der jeweiligen Causa, und damit zur Erfüllung des Zweckes dieses Verarbeitungsvorgangs, erforderlich oder zumindest zweckdienlich sind.

Das Erfassen von Daten erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Datenerfassung fördert den Grundsatz der Datenminimierung, zumal das Erfassen jedes einzelnen Datums mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Die Bearbeitung von Akten erfolgt häufig arbeitsteilig, sodass ein reduzierter Akt Grundvoraussetzung für ein effizientes Arbeiten ist. Das zweckfreie Sammeln von Daten ist der Arbeitsweise einer Rechtsanwaltskanzlei fremd.

Die genannten Gründe gelten entsprechend auch für den Umfang der Verarbeitung.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu den in Akten gespeicherten Daten haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT" (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bieten ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung) und die Verwendung von Microsoft SharePoint (Dokumentenmanagementsystem mit Anbindung an ADVOKAT-Security) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

1.1.1.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:

- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:

- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine automatisierte Verarbeitung von Daten
- Verarbeitung aller Daten erfolgt zum überwiegenden Teil nur innerhalb des Kanzleinetzwerks
- Keine Weitergabe von Daten bei diesem Verarbeitungsvorgang
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (keine Weitergabe von Daten; aufgrund ausschließlich manueller Verarbeitung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (die Beauftragung und Verarbeitung erfolgt vornehmlich innerhalb der Kanzleiräumlichkeiten und damit durch qualifiziertes Kanzleipersonal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (die Verarbeitungszwecke sind in der westlichen Gesellschaft nicht nur anerkannt, sondern sogar hochgehalten; diese sind legitim und klar abgegrenzt)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.1.9 Spezifische TOMs

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

Bei Verwendung von ADVOKAT Security: Das Berechtigungssystem der Anwaltssoftware „ADVOKAT“ ermöglicht die Verwaltung von Rechten für Benutzer/innen und -gruppen betreffend einzelne Akten, Aktengruppen und einzelne Programmbereiche. Dieses Berechtigungssystem stellt sicher, dass nur jene Kanzleimitarbeiter/innen Zugang zu Daten eines Aktes haben, welche diesen auch tatsächlich für die Erfüllung der Verarbeitungszwecke benötigen.

Virtueller versperrter Aktenschrank

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 (z.B. zuständige/r Partner/in, Abteilungsleiter/in). Zusätzlich kann die Bearbeitung auch für diese definierte(n) Person(en) durch Setzen entsprechender Rechte gesperrt werden.

Es können auch mehrere solcher „Aktenschränke“ angelegt werden (z.B. einer je Abteilung). Nach Abschluss eines Auftrags aufbewahrte Daten werden so effektiv geschützt, weil der Zugang durch Aktablage automatisch stark eingeschränkt wird.

Personen schützen

Bei Verwendung von ADVOKAT Security: Die Anwaltssoftware „ADVOKAT“ ermöglicht die Hinterlegung von berechtigten Benutzergruppen bei Personen im Adressbestand. Nur die auf solche Weise berechtigten Personen können überhaupt feststellen, dass es diese Person im System gibt. Für nicht Berechtigte gibt es die Person nicht.

Als besonderes Feature können Benutzer/innen eine Person ausnahmsweise doch sehen, wenn diese in einem Akt beteiligt ist, auf welchen die/der Benutzer/in zugreifen darf. Das ist nötig, damit die/der Benutzer/in den Akt, welchen diese (mit)bearbeiten, bearbeiten können. Sobald jedoch die/der Benutzer/in den Zugriff auf den Akt verliert (idealerweise bei Ablage des Aktes) verliert sie/er damit auch den Zugriff auf die Person, sodass die Person, aus Sicht der Benutzerin / des Benutzers, aus dem System verschwindet.

Um die Erfüllung anderer Aufgaben und Pflichten (z.B. Auskunftsrecht) nicht zu gefährden, kann einem oder mehreren Benutzer/innen das Recht eingeräumt werden, sämtliche Personen sehen zu dürfen. Dieses Recht ist sehr restriktiv handzuhaben.

1.1.2 Aktbearbeitung und Aktkorrespondenz (Leistungen, Dokumente, Forderungen, Titel, Schriftsätze, Schriftverkehr, Telefonate, Termine)

1.1.2.1 Kurzbeschreibung

Im Zusammenhang mit der anwaltschaftlichen Vertretung und Beratung von Personen werden Akten und in die Causa involvierte Personen angelegt, die Personen und Aktendaten werden im Akt erfasst, und dort weiterbearbeitet und -verarbeitet.

Dieser Verarbeitungsvorgang schließt an den Verarbeitungsvorgang der Aktanlage an. Er umfasst das Erfassen, Bearbeiten und Verarbeiten von Leistungen, Dokumenten, zu betreibenden Forderungen, Titeln (z.B. gerichtliche und behördliche Entscheidungen), Schriftsätzen (inkl. ERV-Schriftsätze) sowie die Organisation, Verrichtung und Dokumentation der einhergehenden Korrespondenzen (z.B. Schriftverkehr, Telefonate, Postsendungen, Faxe, Termine).

1.1.2.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die rechtsanwaltliche Vertretung von Auftraggebenden im Umfang des jeweiligen Mandats, die Leistung rechtsanwaltlicher Dienste für Auftraggebende im Umfang des Auftrages sowie die rechtliche Beratung von Auftraggebenden.

1.1.2.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige

Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	**Gerichte und Behörden inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der jeweiligen Causa befasste Gerichte (zuständige Zivil- und Strafgerichte) und Behörden (z.B. Finanzämter, Vermessungsämter, Grundverkehrsbehörden, Bezirkshauptmannschaften, Gemeinden, Kammern).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie D	**Kanzleimitarbeiter/innen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit Bearbeitungen und Korrespondenzen zur jeweiligen Causa werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.1.2.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
				Aktbeteiligte P.[2)]	Gerichte & Beh.[3)]	Landes-RAK[4)]	ERV-Überm.St.[5)]	Ggf. IT-Support[6)]					

A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X	X	X	X						
	2	Foto	Nein			X		X						
	3	Anschrift	Nein	X	X	X	X	X						
	4	Kontaktdaten (Tel., Mail, Fax)	Nein	X	X	X	X	X						
	5	Bank- und Überweisungsdaten	Nein			X		X						
	6	Geburtsdatum	Nein	X	X	X	X	X						
	7	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein	X	X		X	X						
	8	Firmenbuch- und Gewerbedaten	Nein	X	X	X	X	X						
	9	Grundbuchdaten	Nein	X	X		X	X						
	10	UID-, FB-, ZVR-Nummer	Nein	X	X	X	X	X						
	11	Sozialversicherungsdaten	Nein	X	X	X	X	X						
	12	Kontaktpersonen und deren Kontaktdaten	Nein	X	X		X	X						
	13	Beteiligte Personen (Aktbeteiligte Personen, Gerichte und Behörden)	Nein	X	X	X	X	X						
	14	Leistungsnachweise	Nein	X	X		X	X						
	15	Vertragstexte und Geschäftskorrespondenzen	Nein	X	X		X	X						
	16	Sachverhaltsdaten und Schriftsätze	Nein	X	X		X	X						
	17	Gerichtliche / Behördliche Erledigungen	Nein	X	X		X	X						
	18	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein			X		X						
	19	Ggf. Daten zu Bonität / Solvenz, Mahndaten	Nein	X	X		X	X						
	20	Ggf. Daten woraus die rassische/ethische Herkunft hervorgehen (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	21	Ggf. Daten woraus politische Meinungen hervorgehen (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	22	Ggf. Daten woraus religiöse/weltanschauliche Überzeugungen hervorgehen (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	23	Ggf. Daten woraus eine Gewerkschafts-zugehörigkeit hervorgeht (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	24	Ggf. genetische Daten (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	25	Ggf. biometrische Daten (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	26	Ggf. Gesundheitsdaten (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	27	Ggf. Daten zu Sexualleben / sexueller Orientierung (Art. 9 DSGVO)	Ja[1)]	X	X		X	X						
	28	Ggf. strafrechtliche Daten (Art. 10 DSGVO)	Ja[1)]	X	X		X	X						
C	29	Kontaktpersonen und deren Kontaktdaten	Nein	X	X		X	X						
D	30	Name	Nein	X	X		X	X						
	31	Funktion in der Kanzlei	Nein	X	X		X	X						
	32	Dienstliche Kontaktdaten	Nein	X	X		X	X						

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Diese Datenkategorien werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

[2)] Aktbeteiligte P.: Alle aktbeteiligten Personen inkl. Auftraggeber/in (entspricht den Personenkategorien A und B)

[3)] Gerichte & Beh.: Gerichte und Behörden (entspricht der Personenkategorie C)

[4)] Landes-RAK: Landesrechtsanwaltskammer
Mit einer Treuhandmeldung (verpflichtend gem. § 10a Abs. 4 RAO) werden diverse Daten gegenüber der zuständigen Landesrechtsanwaltskammer offengelegt. Die Treuhandgeschäfte, sowie die Fremdgeldgebarung überhaupt, werden stichprobenartig von einem dafür bestellten Revisionsbeauftragten geprüft.

[5)] ERV-Überm.St.: Übermittlungsstellen für den elektronischen Rechtsverkehr, kundgemacht gemäß § 3 Abs. 1 der Verordnung über den elektronischen Rechtsverkehr auf *http://kundmachungen.justiz.gv.at*

[6)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.1.2.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Aktbeteiligte P.	Im Ausnahmefall[1)]	Im Ausnahmefall[2)]
Gerichte & Beh.	Im Ausnahmefall[3)]	Nein
ERV-Überm.St.	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

[1)] Sofern eine aktbeteiligte Person in einem Drittstaat ansässig ist, erfolgt die Übermittlung in diesen Drittstaat.

[2)] Sofern eine aktbeteiligte Person eine internationale Organisation ist, erfolgt die Übermittlung an diese internationale Organisation.

[3)] Sofern ein Gericht oder eine Behörde eines Drittstaates befasst wird, erfolgt eine Übermittlung in diesen Drittstaat.

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Die Übermittlung an Drittstaaten und an internationale Organisationen erfolgt ausschließlich unter Gewährleistung des durch die Datenschutzgrundverordnung normierten Schutzniveaus. Weil die ganze Welt und jede Person dieser Welt als Adressat in Frage kommen, kann dieser Aspekt nicht global für den Verarbeitungsvorgang, sondern nur im Einzelfall sichergestellt werden.

Im Einzelfall wird geprüft,
- ob ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, welcher ein angemessenes Schutzniveau bei der adressierten Person konstatiert (Art. 45 DSGVO)
- ob geeignete Garantien vorliegen oder geschaffen werden können (Art. 46f DSGVO)
- ob ein Ausnahmetatbestand, welcher die Übermittlung erlaubt, erfüllt ist (Art. 49 DSGVO) Vor allem diese Ausnahmetatbestände können zur Anwendung kommen:
  - Ausdrückliche Einwilligung nach Unterrichtung (Art. 49 Abs. 1 lit. a)
  - Im Interesse der betroffenen Person aufgrund eines Vertrages des verantwortlichen Parteimit einer anderen Person (Art. 49 Abs. 1 lit. c)
  - Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich (Art. 49 Abs. 1 lit. e)

1.1.2.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt in Erfüllung der rechtsanwaltlichen Aufbewahrungspflichten gemäß § 12 RAO für die Dauer von fünf Jahren ab Abschluss der jeweiligen Causa und umfasst sämtliche Datenkategorien. Der Abschluss wird durch Vergabe eines Ablagedatums je Akt dokumentiert, wodurch ein systemisches Bereinigen (Löschen von alten Akten) möglich ist.

Soweit es zur Abwehr etwaiger Schadenersatzansprüche erforderlich ist, werden die Daten eines Aktes und der involvierten Personen für die Dauer von 30 Jahren (lange Verjährungsfrist) ab Abschluss der jeweiligen Causa aufbewahrt.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT“ Möglichkeiten, welche den Schutz der Daten, die über den Abschluss einer Causa hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs“).

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.1.2.7 Datenminimierung

Nicht nur zur Sicherung eines hohen Datenschutzniveaus, sondern auch für eine schlanke und effiziente Kanzleiverwaltung werden ausschließlich Daten erfasst, welche für die Bearbeitung der jeweiligen Causa, und damit zur Erfüllung des Zweckes dieses Verarbeitungsvorgangs, erforderlich oder zumindest zweckdienlich sind.

Das Erfassen von Daten erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Datenerfassung fördert den Grundsatz der Datenminimierung, zumal das Erfassen jedes einzelnen Datums mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Die Bearbeitung von Akten erfolgt häufig arbeitsteilig, sodass ein reduzierter Akt Grundvoraussetzung für ein effizientes Arbeiten ist. Das zweckfreie Sammeln von Daten ist der Arbeitsweise einer Rechtsanwaltskanzlei fremd.

Die genannten Gründe gelten entsprechend auch für den Umfang der Verarbeitung.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu den in Akten gespeicherten Daten haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT“ (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bieten ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung) und die Verwendung von Microsoft SharePoint (Dokumentenmanagementsystem mit Anbindung an ADVOKAT-Security) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

1.1.2.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine automatisierte Verarbeitung von Daten
- Verarbeitung aller Daten erfolgt zum überwiegenden Teil nur innerhalb des Kanzleinetzwerks

- Die Weitergabe von Daten erfolgt ausschließlich an solche Empfänger/innen, welche ihrerseits ein hohes Schutzniveau bieten, zumal diese selbst ein Interesse an einem hohen Schutzniveau haben.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (nur sehr wenige Datenübermittlungen an einen geschlossenen Empfängerkreis; aufgrund ausschließlich manueller Verarbeitung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (die Beauftragung und Verarbeitung erfolgt vornehmlich innerhalb der Kanzleiräumlichkeiten und damit durch qualifiziertes Kanzleipersonal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (die Verarbeitungszwecke sind in der westlichen Gesellschaft nicht nur anerkannt, sondern sogar hochgehalten; diese sind legitim und klar abgegrenzt)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.2.9 Spezifische TOMs

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

Die Übermittlung von Daten in ein Drittland oder eine internationale Organisation wird im Einzelfall geprüft und das Schutzniveau der DSGVO sichergestellt. Siehe dazu die entsprechenden Ausführungen oberhalb.

Bei Verwendung von ADVOKAT Security: Das Berechtigungssystem der Anwaltssoftware „ADVOKAT“ ermöglicht die Verwaltung von Rechten für Benutzer/innen und -gruppen betreffend einzelne Akten, Aktengruppen und einzelne Programmbereiche. Dieses Berechtigungssystem stellt sicher, dass nur jene Kanzleimitarbeiter/innen Zugang zu Daten eines Aktes haben, welche diesen auch tatsächlich für die Erfüllung der Verarbeitungszwecke benötigen.

Bei Verwendung von Microsoft SharePoint: Das mit der Anwaltssoftware „ADVOKAT“ verbundene Berechtigungssystem stellt sicher, dass Dokumente und andere Dateien nur für jene Kanzleimitarbeiter/innen zugänglich sind, welche den Zugang für die Erfüllung der Verarbeitungszwecke benötigen. Die Versionierung von Dokumenten schafft zusätzlich einen Manipulationsschutz für alle Dokumente. Je nach Ausführungsvariante von Microsoft SharePoint stehen weitere Sicherheitsfunktionen zur Verfügung.

Virtueller versperrter Aktenschrank

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 (z.B. zuständige/r Partner/in, Abteilungsleiter/in). Zusätzlich kann die Bearbeitung auch für diese definierte(n) Person(en) durch Setzen entsprechender Rechte gesperrt werden.

Es können auch mehrere solcher „Aktenschränke“ angelegt werden (z.B. einer je Abteilung). Nach Abschluss eines Auftrags aufbewahrte Daten werden so effektiv geschützt, weil der Zugang durch Aktablage automatisch stark eingeschränkt wird.

Personen schützen

Bei Verwendung von ADVOKAT Security: Die Anwaltssoftware „ADVOKAT“ ermöglicht die Hinterlegung von berechtigten Benutzergruppen bei Personen im Adressbestand. Nur die auf solche Weise berechtigten Personen können überhaupt feststellen, dass es diese Person im System gibt. Für nicht Berechtigte gibt es die Person nicht.

Als besonderes Feature können Benutzer/innen eine Person ausnahmsweise doch sehen, wenn diese in einem Akt beteiligt ist, auf welchen die/der Benutzer/in zugreifen darf. Das ist nötig, damit Benutzer/innen den Akt, welchen diese (mit)bearbeiten, bearbeiten können. Sobald jedoch der Zugriff auf den Akt verloren geht (idealerweise bei Ablage des Aktes) entfällt damit auch der Zugriff auf die Person, sodass die Person, aus Sicht der Benutzerin / des Benutzers, aus dem System verschwindet.

Um die Erfüllung anderer Aufgaben und Pflichten (z.B. Auskunftsrecht) nicht zu gefährden, kann einzelnen Benutzer/innen das Recht eingeräumt werden, sämtliche Personen sehen zu dürfen. Dieses Recht ist sehr restriktiv handzuhaben.

1.1.3 Elektronischer Rechtsverkehr (ERV)

1.1.3.1 Kurzbeschreibung

Im Zusammenhang mit der anwaltschaftlichen Vertretung und Beratung von Personen werden Nachrichten im elektronischen Rechtsverkehr (ERV) gesendet und empfangen. Die Verwendung des ERV ist für Rechtsanwält/innen gemäß § 89c Abs. 5 Z. 1 Gerichtsorganisationsgesetz (GOG) verpflichtend.

Im ERV werden Schriftsätze bei Gerichten und Behörden eingebracht und Erledigungen von Gerichten und Behörden empfangen. Auch erfolgt die Kommunikation mit anderen österreichischen Rechtsanwält/innen, mit der Rechtsanwaltskammer (RAK) und Banken teilweise via ERV (Direktzustellung gemäß § 112 ZPO).

1.1.3.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist der für die rechtsanwaltliche Vertretung von Klient/innen erforderliche Schriftsatzverkehr mit Gerichten, Behörden, Rechtsanwaltskammern und Banken samt der Einbindung der involvierten Rechtsanwält/innen in diesen Schriftsatzverkehr.

1.1.3.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende im Sinne des Erwägungsgrundes 63 DSGVO (Fernzugang für betroffene Person) einen permanenten Zugang auf

Personenkategorie	deren Akten und Aktendaten durch Anmeldung am Klient/innen-Portal (Lesezugriff).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	<u>Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO):</u> Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. <u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	**Gerichte und Behörden inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der jeweiligen Causa befasste Gerichte (zuständige Zivil- und Strafgerichte) und Behörden (z.B. Finanzämter, Vermessungsämter, Grundverkehrsbehörden, Bezirkshauptmannschaften, Gemeinden, Kammern).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie D	**Kanzleimitarbeiter/innen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit dem Erfassen, Versenden, Empfangen und Verarbeitung von ERV-Nachrichten werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.1.3.4 <u>Kategorien der verarbeiteten Daten und Empfänger</u>

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
				Öst. Ger. & Beh.[2]	Österr. RAs[3]	ERV-Überm.St.[4]	Ggf. IT-Support[5]	RAK[6]	BANK[6]				
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X	X	X	X	X				
	2	Foto	Nein				X	X	X				
	3	Anschrift	Nein	X	X	X	X	X	X				
	4	Kontaktdaten (Tel., Mail, Fax)	Nein	X	X	X	X	X	X				
	5	Bank- und Überweisungsdaten	Nein				X	X	X				
	6	Geburtsdatum	Nein	X	X	X	X	X	X				
	7	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein	X	X	X	X						
	8	Firmenbuch- und Gewerbedaten	Nein	X	X	X	X	X	X				
	9	Grundbuchdaten	Nein	X	X	X	X	X	X				
	10	UID-, FB-, ZVR-Nummer	Nein	X	X	X	X	X	X				
	11	Sozialversicherungsdaten	Nein	X	X	X	X						
	12	Kontaktpersonen und deren Kontaktdaten	Nein	X	X	X	X						
	13	Beteiligte Personen (Aktbeteiligte Personen, Gerichte und Behörden)	Nein	X	X	X	X						
	14	Leistungsnachweise	Nein	X	X	X	X						
	15	Vertragstexte und Geschäftskorrespondenzen	Nein	X	X	X	X						
	16	Sachverhaltsdaten und Schriftsätze	Nein	X	X	X	X						
	17	Gerichtliche / Behördliche Erledigungen	Nein	X	X	X	X						
	18	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein				X						
	19	Ggf. Daten zu Bonität / Solvenz, Mahndaten	Nein	X	X	X	X						
	20	Ggf. Daten woraus die rassische/ethische Herkunft hervorgehen (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	21	Ggf. Daten woraus politische Meinungen hervorgehen (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	22	Ggf. Daten woraus religiöse/weltanschauliche Überzeugungen hervorgehen (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	23	Ggf. Daten woraus eine Gewerkschafts-zugehörigkeit hervorgeht (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	24	Ggf. genetische Daten (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	25	Ggf. biometrische Daten (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	26	Ggf. Gesundheitsdaten (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	27	Ggf. Daten zu Sexualleben / sexueller Orientierung (Art. 9 DSGVO)	Ja[1]	X	X	X	X						
	28	Ggf. strafrechtliche Daten (Art. 10 DSGVO)	Ja[1]	X	X	X	X						
C	29	Kontaktpersonen und deren Kontaktdaten	Nein	X	X	X	X						
D	30	Name	Nein	X	X	X	X						
	31	Funktion in der Kanzlei	Nein	X	X	X	X						
	32	Dienstliche Kontaktdaten	Nein	X	X	X	X						

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Diese Datenkategorien werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

[2)] Öst. Ger. & Beh.: Österreichische Gerichte und Behörden (entspricht der Personenkategorie C, soweit es sich dabei um Gerichte und Behörden in Österreich handelt)

[3)] Österr. RAs: Österreichische Rechtsanwält/innen, welche aktbeteiligte Personen vertreten und daher via ERV mitbefasst werden (insb. Direktzustellung gemäß § 112 ZPO).

[4)] ERV-Überm.St.: Staatlich konzessionierte Übermittlungsstellen für den elektronischen Rechtsverkehr, kundgemacht gemäß § 3 Abs. 1 der Verordnung über den elektronischen Rechtsverkehr auf *http://kundmachungen.justiz.gv.at*

[5)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

[6)] RAK und Bank: Im Rahmen des Elektronischen Treuhandbuchs der Rechtsanwaltskammern erfolgen Übermittlungen an die Rechtsanwaltskammer und die Bank

1.1.3.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Öst. Ger. & Beh.	Nein	Nein
Österr. RAs	Nein	Nein
ERV-Überm.St.	Nein	Nein
Ggf. IT-Support	Nein	Nein
Banken	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.1.3.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt in Erfüllung der rechtsanwaltlichen Aufbewahrungspflichten gemäß § 12 RAO für die Dauer von fünf Jahren ab Abschluss der jeweiligen Causa und umfasst sämtliche Datenkategorien. Der Abschluss wird durch Vergabe eines Ablagedatums je Akt dokumentiert, wodurch ein systemisches Bereinigen (Löschen von alten Akten) möglich ist.

Soweit es zur Abwehr etwaiger Schadenersatzansprüche erforderlich ist, werden die Daten eines Aktes und der involvierten Personen für die Dauer von 30 Jahren (lange Verjährungsfrist) ab Abschluss der jeweiligen Causa aufbewahrt.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT“ Möglichkeiten, welche den Schutz der Daten, die über den Abschluss einer Causa hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs“).

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

Die Aufbewahrung von personenbezogenen Daten bei ERV-Übermittlungsstellen erfolgt gemäß den Vertragsbedingungen zur Ausschreibung betreffend Übermittlungsstellen für den Elektronischen Rechtsverkehr. Gemäß diesen erfolgt eine Aufbewahrung von an die Kanzlei übermittelten Nachrichten (ERV-Rückverkehr) für die Dauer von drei Monaten (Punkte 7.5 und 13.1 der genannten

Vertragsbedingungen). Überhaupt werden sämtliche Daten höchstens für die Dauer von drei Monaten zwischengespeichert und im Anschluss vollständig gelöscht.

Es gilt zusätzlich das bei „Abfrage von Registern / Lösch- und Aufbewahrungsfristen“ unter „Das Folgende gilt für alle Dienste“ Ausgeführte.

1.1.3.7 Datenminimierung

Die Kommunikation via ERV ist detailliert reglementiert. Datenmenge und Umfang der Verarbeitung sind daher vorgegeben und durch die Kanzlei nicht beeinflussbar. Soweit Daten in freier Form (Weiteres Vorbringen, Anlagen) übermittelt werden, erfolgt dies nur in einem für die Zwecke der Verarbeitung notwendigen bzw. zweckmäßigen Umfang.

Das Erfassen und Senden von ERV-Nachrichten erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Erfassung und Übermittlung fördert den Grundsatz der Datenminimierung, zumal das Erfassen jedes einzelnen Datums und jede Übermittlung mit Arbeitszeit und damit auch mit Kosten verbunden sind.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu ERV-Nachrichten haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT“ (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bietet ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

1.1.3.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:

- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:

- Keine vollautomatisierte Verarbeitung von Daten (keine Verarbeitung ohne Benutzerinteraktion)
- Die Übermittlung von Daten im elektronischen Rechtsverkehr erfolgt ausschließlich durch die staatlich konzessionierte Übermittlungsstelle ADVOKAT Unternehmensberatung Greiter & Greiter GmbH. Sämtliche Übermittlungen erfolgen über einen verschlüsselten Kommunikationstunnel (HTTPS) und die Zwischenspeicherung bei der Übermittlungsstelle erfolgt auf von dieser betriebenen, in Österreich befindlichen Servern, welche in modernsten, hochsicheren Datenzentren untergebracht sind. Die Authentisierung und Authentifizierung erfolgt via von der ERV-Übermittlungsstelle ausgestelltem Softwarezertifikat (SHA-2-Standard).
- Die Übermittlung erfolgt über einen gesetzlich verpflichtend vorgegebenen Kanal und die Gesetzgebung hat ein hohes Interesse an der Sicherheit dieses Kanals, wie er aufgrund der DSGVO auch dazu verpflichtet ist.
- Die Weitergabe von Daten erfolgt ausschließlich an österreichische Gerichte, Behörden und Rechtsanwält/innen, welche ihrerseits ein hohes Schutzniveau bieten, zumal diese selbst ein Interesse an einem hohen Schutzniveau haben.

- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (sichere HTTPS-Kommunikation; sicheres Authentisierungs- und Authentifizierungsverfahren via Softwarezertifikate nach SHA-2-Standard)
- Art der Verarbeitung: Niedriges Risiko (Verarbeitung nur bei Benutzerinteraktion; Übermittlungen erfolgten nur durch vertrauenswürdige Auftragsverarbeiter: Gerichte, Behörden, von Ministerien beauftragte ERV-Übermittlungsstellen)
- Umfang der Verarbeitung: Niedriges Risiko (je Causa erfolgen nur sehr wenige Datenübermittlungen an einen geschlossenen und vertrauenswürdigen Empfängerkreis (Gerichte, Behörden, von Ministerien beauftragte ERV-Übermittlungsstellen, Rechtsanwälte); aufgrund hoher Formalisierung sind die Daten auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (Erfassen, Senden und Empfangen von ERV-Nachrichten erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und durch qualifiziertes Personal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation; die Nachrichten und der Übermittlungsweg sind gesetzlich vorgegeben)
- Zwecke der Verarbeitung: Niedriges Risiko (die Gesetzgebung hat den ERV als Kanal speziell für diesen Zweck geschaffen, sodass der Zweck als für die Allgemeinheit wesentlich und legitim betrachtet werden kann)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.3.9 Spezifische TOMs

Empfangene und gesendete ERV-Nachrichten werden, mit AES-256 verschlüsselt, in einem proprietären Format als Dateien gespeichert. Die Dateien können daher nur mit der Anwaltssoftware „ADVOKAT“ gelesen werden. Bei Verwendung von ADVOKAT Security kann der Zugriff auf ERV-Nachrichten auf einzelne Benutzer/innen und -gruppen eingeschränkt werden. Diese Einschränkung kann für ERV-Nachrichten generell, aber auch abhängig vom zugehörigen Akt erfolgen (z.B.: Wenn ein/e Benutzer/in Zugriff auf einen Akt hat, darf er auch zugehörige ERV-Nachrichten sehen). Auch kann der Zugriff auf das ERV-Programm insgesamt gesperrt bzw. erlaubt werden.

Die Übermittlung von Daten im elektronischen Rechtsverkehr erfolgt ausschließlich durch die staatlich konzessionierte Übermittlungsstelle ADVOKAT Unternehmensberatung Greiter & Greiter GmbH. Sämtliche Übermittlungen erfolgen über einen verschlüsselten Kommunikationstunnel (HTTPS) und die Zwischenspeicherung bei der genannten ERV-Übermittlungsstelle erfolgt auf von dieser betriebenen, in Österreich befindlichen Servern, welche in modernsten, hochsicheren Datenzentren untergebracht sind. Die Authentisierung und Authentifizierung erfolgt via von der ERV-Übermittlungsstelle ausgestelltem Softwarezertifikat (SHA-2-Standard).

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche

den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.1.4 Elektronische Akteneinsicht (eAkt)

1.1.4.1 Kurzbeschreibung

Im Zusammenhang mit der anwaltschaftlichen Vertretung von Personen nehmen Rechtsanwält/innen online Einsicht in Gerichtsakten (elektronische Akteneinsicht). Die elektronische Akteneinsicht ist eine gesetzlich vorgegebene Möglichkeit, welche über die staatlich konzessionierte Verrechnungsstelle ADVOKAT Unternehmensberatung Greiter & Greiter GmbH abgewickelt wird (§ 89i GOG, § 219 Abs. 1 ZPO, §§ 51, 57 Abs. 2 und 68 Abs. 1 und 2 StPO).

1.1.4.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die rechtsanwaltliche Vertretung von Klient/innen im Umfang des jeweiligen Mandats *„unter Bedachtnahme auf eine einfache und sparsame Verwaltung“* (vgl. § 89i GOG) und auf eine kosteneffiziente Bearbeitung durch die Kanzlei.

1.1.4.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	**Gerichte und Behörden inkl. Kontaktpersonen bei diesen**
Anmerkungen zur	Im Zusammenhang mit der jeweiligen Causa befasste Gerichte (zuständige Zivil- und Strafgerichte)

Personenkategorie	und Behörden (z.B. Finanzämter, Vermessungsämter, Grundverkehrsbehörden, Bezirkshauptmannschaften, Gemeinden, Kammern).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie D	**Kanzleimitarbeiter/innen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der Verarbeitung von Abfragen aus der elektronischen Akteneinsicht werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.1.4.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger								
				Verrechnungsst.[2)]	Ggf. IT-Support[3)]							
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X							
	2	Foto	Nein	X	X							
	3	Anschrift	Nein	X	X							
	4	Kontaktdaten (Tel., Mail, Fax)	Nein	X	X							
	5	Bank- und Überweisungsdaten	Nein	X	X							
	6	Geburtsdatum	Nein	X	X							
	7	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein	X	X							
	8	Firmenbuch- und Gewerbedaten	Nein	X	X							
	9	Grundbuchdaten	Nein	X	X							
	10	UID-, FB-, ZVR-Nummer	Nein	X	X							
	11	Sozialversicherungsdaten	Nein	X	X							
	12	Kontaktpersonen und deren Kontaktdaten	Nein	X	X							
	13	Beteiligte Personen (Aktbeteiligte Personen, Gerichte und Behörden)	Nein	X	X							
	14	Leistungsnachweise	Nein	X	X							
	15	Vertragstexte und Geschäftskorrespondenzen	Nein	X	X							

	16	Sachverhaltsdaten und Schriftsätze	Nein	X	X								
	17	Gerichtliche / Behördliche Erledigungen	Nein	X	X								
	18	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein	X	X								
	19	Ggf. Daten zu Bonität / Solvenz, Mahndaten	Nein	X	X								
	20	Ggf. Daten woraus die rassische/ethische Herkunft hervorgehen (Art. 9 DSGVO)	Ja[1)]	X	X								
	21	Ggf. Daten woraus politische Meinungen hervorgehen (Art. 9 DSGVO)	Ja[1)]	X	X								
	22	Ggf. Daten woraus religiöse/weltanschauliche Überzeugungen hervorgehen (Art. 9 DSGVO)	Ja[1)]	X	X								
	23	Ggf. Daten woraus eine Gewerkschafts-zugehörigkeit hervorgeht (Art. 9 DSGVO)	Ja[1)]	X	X								
	24	Ggf. genetische Daten (Art. 9 DSGVO)	Ja[1)]	X	X								
	25	Ggf. biometrische Daten (Art. 9 DSGVO)	Ja[1)]	X	X								
	26	Ggf. Gesundheitsdaten (Art. 9 DSGVO)	Ja[1)]	X	X								
	27	Ggf. Daten zu Sexualleben / sexueller Orientierung (Art. 9 DSGVO)	Ja[1)]	X	X								
	28	Ggf. strafrechtliche Daten (Art. 10 DSGVO)	Ja[1)]	X	X								
C	29	Kontaktpersonen und deren Kontaktdaten	Nein	X	X								
D	30	Name	Nein	X	X								
	31	Funktion in der Kanzlei	Nein	X	X								
	32	Dienstliche Kontaktdaten	Nein	X	X								

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Diese Datenkategorien werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

[2)] Verrechnungsst.: Staatlich konzessionierte Verrechnungsstelle (z.B. die ADVOKAT Unternehmensberatung Greiter & Greiter GmbH), welche das für die elektronische Akteneinsicht benötigte Online-Service anbietet. Bei diesem Unternehmen handelt es sich um eine staatlich konzessionierte Verrechnungsstelle.

[3)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.1.4.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Verrechnungsst.	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.1.4.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt in Erfüllung der rechtsanwaltlichen Aufbewahrungspflichten gemäß § 12 RAO für die Dauer von fünf Jahren ab Abschluss der jeweiligen Causa und umfasst sämtliche Datenkategorien. Der Abschluss wird durch Vergabe eines Ablagedatums je Akt dokumentiert, wodurch ein systemisches Bereinigen (Löschen von alten Akten) möglich ist.

Soweit es zur Abwehr etwaiger Schadenersatzansprüche erforderlich ist, werden die Daten eines Aktes und der involvierten Personen für die Dauer von 30 Jahren (lange Verjährungsfrist) ab Abschluss der jeweiligen Causa aufbewahrt.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT“ Möglichkeiten, welche den Schutz der Daten, die über den Abschluss einer Causa hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs“).

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

Die Aufbewahrung von personenbezogenen Daten bei der Verrechnungsstelle erfolgt gemäß den Vertragsbedingungen zur Ausschreibung betreffend Verrechnungsstellen. Gemäß diesen erfolgt eine Vorhaltung der getätigten Abfragen zur neuerlichen Abholung für die Dauer von fünf Werktagen (Punkte 7.5 und 13.1 der genannten Vertragsbedingungen). Darüber hinaus bleiben sämtliche Daten höchstens für eine Dauer von 3 Monaten zwischengespeichert, bis diese endgültig gelöscht werden.

Es gilt zusätzlich das bei „Abfrage von Registern / Lösch- und Aufbewahrungsfristen“ unter „Das Folgende gilt für alle Dienste“ Ausgeführte.

1.1.4.7 Datenminimierung

Die Elektronische Akteneinsicht ist detailliert reglementiert. Datenmenge und Umfang der Verarbeitung sind daher vorgegeben und durch die Kanzlei nicht beeinflussbar.

Die Einsichtnahme erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer Automation fördert den Grundsatz der Datenminimierung, zumal jede einzelne Abfrage mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Das Benutzer/innen- und Berechtigungssystem von ADVOKAT Online – dabei handelt es sich um das Portal für die Vornahme der elektronischen Akteneinsicht – ermöglicht die Beschränkung des Zugriffs auf diesen Dienst auf einen oder wenige Mitarbeiter/innen/innen.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst und abgefragt werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu abgefragten Aktenstücken haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT“ (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bietet ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

1.1.4.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:

- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:

- Keine automatisierte Verarbeitung von Daten. Jede Einsichtnahme erfolgt einzeln und durch manuelle Abfrage.
- Die Übermittlung von Daten im Zusammenhang mit der elektronischen Akteneinsicht erfolgt ausschließlich durch die staatlich konzessionierte Verrechnungsstelle ADVOKAT Unternehmensberatung Greiter & Greiter GmbH. Sämtliche Übermittlungen erfolgen über einen verschlüsselten Kommunikationstunnel (HTTPS) und der Transport erfolgt über, von der Verrechnungsstelle betriebenen, in Österreich befindlichen Servern, welche in modernsten, hochsicheren Datenzentren untergebracht sind. Die Authentisierung und Authentifizierung erfolgt via Benutzerkennung und Kennwort.
- Die Übermittlung erfolgt über einen gesetzlich verpflichtend vorgegebenen Kanal und die Gesetzgebung hat ein hohes Interesse an der Sicherheit dieses Kanals, wie er aufgrund der DSGVO auch dazu verpflichtet ist.
- Es erfolgt keine Offenlegung von Daten.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (sichere HTTPS-Kommunikation; sicheres Authentisierungs- und Authentifizierungsverfahren mit Benutzerkennung und Kennwort)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (keine Weitergabe von Daten; aufgrund ausschließlich manueller Verarbeitung und aufgrund hoher Formalisierung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (Einsichtnahmen erfolgen ausschließlich innerhalb der Kanzleiräumlichkeiten und durch qualifiziertes Personal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation; die Einsichtnahme und die konkrete Abwicklung sind gesetzlich vorgegeben)
- Zwecke der Verarbeitung: Niedriges Risiko (die Gesetzgebung hat die elektronische Akteneinsicht speziell für diesen Zweck geschaffen, sodass der Zweck als für die Allgemeinheit wesentlich und legitim betrachtet werden kann)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.4.9 Spezifische TOMs

Abgefragte Dokumente werden mit der Anwaltssoftware „ADVOKAT“ in den jeweiligen Akt abgelegt. Bei Verwendung von ADVOKAT Security kann der Zugriff auf Akten auf einzelne Benutzer/innen und -gruppen eingeschränkt werden.

Die Übermittlung von Daten in Zusammenhang mit der elektronischen Akteneinsicht erfolgt ausschließlich durch die staatlich konzessionierte Verrechnungsstelle ADVOKAT Unternehmensberatung Greiter & Greiter GmbH. Sämtliche Übermittlungen erfolgen über einen verschlüsselten Kommunikationstunnel (HTTPS) und der Transport erfolgt über, von der Verrechnungsstelle betriebenen, in Österreich befindlichen Servern, welche in modernsten, hochsicheren Datenzentren untergebracht sind. Die Authentisierung und Authentifizierung erfolgt via Benutzerkennung und Kennwort.

Ein Security-Logging sorgt für Nachvollziehbarkeit und Transparenz betreffend die getätigten Einsichtnahmen. Sicherheitskritische Vorgänge werden im Ereignislog protokolliert und können von Administrator/innen eingesehen werden.

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.1.5 Abfrage von Registern (GB, FB, ZMR, GISA, Insolvenzcheck, etc.)

1.1.5.1 Kurzbeschreibung

Im Zusammenhang mit der anwaltschaftlichen Vertretung und Beratung von Personen ist häufig die Abfrage von Daten aus diversen öffentlich zugänglichen Registern erforderlich, welche über das Online-Portal „ADVOKAT Online“, betrieben von der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH, abgewickelt werden. Diese Register sind das Grundbuch, das Firmenbuch, die internationale Firmensuche (Handelsregisterauszüge und Jahresabschlüsse aus anderen Staaten), das Zentrale Melderegister, das Zentrale Personenstandsregister, das Gewerbeinformationssystem Austria (GISA), die Geburtsdatenabfrage, die Abfrage von politisch exponierten und diesen nahestehenden Personen („Compliance Check“) und die Insolvenzdatei des Justizministeriums („Insolvenzcheck“).

1.1.5.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die effiziente Erlangung von für die rechtsanwaltliche Vertretung oder Beratung von Klient/innen erforderlichen, d.h. sachverhaltsrelevanten Informationen im Umfang des jeweiligen Mandats.

1.1.5.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)

Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

1.1.5.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
				Provider[1)]	Ggf. IT-Support[2)]								
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X								
	2	Anschrift	Nein	X	X								
	3	Bank- und Überweisungsdaten	Nein	X	X								
	4	Geburtsdatum	Nein	X	X								
	5	Firmenbuch- und Gewerbedaten	Nein	X	X								
	6	Grundbuchdaten	Nein	X	X								
	7	UID-, FB-, ZVR-Nummer	Nein	X	X								
	8	Veröffentlichte Insolvenzdaten	Nein	X	X								

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Provider = ADVOKAT Unternehmensberatung Greiter & Greiter GmbH via https://dienste.advokat.at bzw. https://online.advokat.at.

[2)] Ggf. IT-Support = Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.1.5.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Provider	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.1.5.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt in Erfüllung der rechtsanwaltlichen Aufbewahrungspflichten gemäß § 12 RAO für die Dauer von fünf Jahren ab Abschluss der jeweiligen Causa und umfasst sämtliche Datenkategorien. Der Abschluss wird durch Vergabe eines Ablagedatums je Akt dokumentiert, wodurch ein systemisches Bereinigen (Löschen von alten Akten) möglich ist.

Soweit es zur Abwehr etwaiger Schadenersatzansprüche erforderlich ist, werden die Daten eines Aktes und der involvierten Personen für die Dauer von 30 Jahren (lange Verjährungsfrist) ab Abschluss der jeweiligen Causa aufbewahrt.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT“ Möglichkeiten, welche den Schutz der Daten, die über den Abschluss einer Causa hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs“).

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

Die Aufbewahrung von personenbezogenen Daten beim Provider – ADVOKAT Unternehmensberatung Greiter & Greiter GmbH – erfolgt für eine Dauer von 3 Monaten (Zwischenspeichern zum erneuten Abholen / Einsehen und zum Nachvollziehen der Rechnungslegung). Anschließend werden die Daten endgültig gelöscht.

Zentrales Melderegister, Zentrales Personenstandsregister: Die ADVOKAT Unternehmensberatung Greiter & Greiter GmbH ist Dienstleister gemäß § 3 Abs. 2 Meldegesetz-Durchführungsverordnung und stellt die Nutzung der ZMR-Datenbank für Abfrageberechtigte zur Verfügung. Rechtsgrundlage für die Verarbeitung sind das Meldegesetz und die Meldegesetzt-Durchführungsverordnung.

Für die Rechnungskontrolle werden Metadaten zu jeder ERV-Nachricht und jeder Abfrage für die Dauer von drei Monaten vorgehalten. Metadaten beinhalten teilweise personenbezogene Daten folgender Kategorien:

- Name, Firma oder sonstige geschäftsmäßige Bezeichnung
- Anschrift
- Geburtsdatum
- Firmenbuchnummer

Diese personenbezogenen Daten sind notwendig, um die von der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH ausgestellten Rechnungen für die Nutzung der Dienste nachvollziehen zu können. Nach Ablauf der drei Monate werden sämtliche personenbezogenen Daten aus den Metadaten gelöscht, sodass nur ein Protokolleintrag ohne personenbezogene Daten erhalten bleibt.

Nach Löschung der ERV-Nachrichten und Abfragen von den Servern werden diese für weitere drei Jahre (kurze Verjährungsfrist) in verschlüsselten Archiven bei der ADOVKAT Unternehmensberatung Greiter & Greiter GmbH aufbewahrt (Backups). Die verschlüsselten Archive sind überdies nur sehr wenigen Mitarbeiter/-innen zugänglich und nur durch eine Spezialsoftware zugreifbar. Diese Aufbewahrung dient der Verteidigung der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH gegen etwaige Schadenersatzansprüche.

1.1.5.7 Datenminimierung

Alle Dienste sind detailliert reglementiert. Datenmenge und Umfang der Verarbeitung sind daher vorgegeben und durch die Kanzlei nicht beeinflussbar.

Die Nutzung der Dienste erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer Automation fördert den Grundsatz der Datenminimierung, zumal jede einzelne Abfrage mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Das Benutzer/innen- und Berechtigungssystem von ADVOKAT Online – dabei handelt es sich um das Portal für die Nutzung der Dienste – ermöglicht die Beschränkung des Zugriffs je Dienst auf einen oder wenige Mitarbeiter/innen.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst und abgefragt werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf

hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu Abfragen haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT“ (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bietet ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

1.1.5.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:

- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:

- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine automatisierte Verarbeitung von Daten. Jede Abfrage wird einzeln und manuelle ausgeführt.
- Die Übermittlung von Daten bei Nutzung der Dienste erfolgt ausschließlich durch die staatlich konzessionierte Verrechnungsstelle ADVOKAT Unternehmensberatung Greiter & Greiter GmbH. Sämtliche Übermittlungen erfolgen über einen verschlüsselten Kommunikationstunnel (HTTPS) und der Transport erfolgt über, von der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH betriebenen, in Österreich befindlichen Servern, welche in modernsten, hochsicheren Datenzentren untergebracht sind. Die Authentisierung und Authentifizierung erfolgt via Benutzerkennung und Kennwort.
- Die Übermittlung erfolgt über einen gesetzlich verpflichtend vorgegebenen Kanal (Grundbuch, Firmenbuch, GISA, ZMR) und die Gesetzgebung hat ein hohes Interesse an der Sicherheit dieses Kanals, wie er aufgrund der DSGVO auch dazu verpflichtet ist. Die Übermittlung betreffend die anderen Dienste erfolgt auf dieselbe Weise und es gilt dasselbe für die Datenlieferant/innen entsprechend.
- Es erfolgt keine Offenlegung von Daten.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (sichere HTTPS-Kommunikation; sicheres Authentisierungs- und Authentifizierungsverfahren mit Benutzerkennung und Kennwort)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (keine Weitergabe von Daten; aufgrund ausschließlich manueller Verarbeitung und aufgrund hoher Formalisierung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (Abfragen erfolgen ausschließlich innerhalb der Kanzleiräumlichkeiten und durch qualifiziertes Personal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation; die Abfragen betreffend Grundbuch, Firmenbuch, GISA und ZMR, sowie die konkrete Abwicklung sind gesetzlich vorgegeben; die anderen Abfragen und

deren Abwicklung erfolgen nach Vorgabe der jeweiligen international anerkannten Datenlieferant/innen)

- Zwecke der Verarbeitung: Niedriges Risiko (die Gesetzgebung hat die Abfragen aus Grundbuch, Firmenbuch, GISA und ZMR speziell für diesen Zweck geschaffen, sodass der Zweck als für die Allgemeinheit wesentlich und legitim betrachtet werden kann; auch die anderen Abfragen dienen allein diesem Zweck)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.5.9 Spezifische TOMs

Abgefragte Daten werden mit der Anwaltssoftware „ADVOKAT“ in den jeweiligen Akt abgelegt. Bei Verwendung von ADVOKAT Security kann der Zugriff auf Akten auf einzelne Benutzer/innen und -gruppen eingeschränkt werden.

Die Übermittlung von Daten bei Nutzung der Dienste erfolgt ausschließlich durch die staatlich konzessionierte Verrechnungsstelle ADVOKAT Unternehmensberatung Greiter & Greiter GmbH. Sämtliche Übermittlungen erfolgen über einen verschlüsselten Kommunikationstunnel (HTTPS) und der Transport erfolgt über, von der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH betriebenen, in Österreich befindlichen Servern, welche in modernsten, hochsicheren Datenzentren untergebracht sind. Die Authentisierung und Authentifizierung erfolgt via Benutzerkennung und Kennwort.

Ein Security-Logging sorgt für Nachvollziehbarkeit und Transparenz betreffend die getätigten Abfragen. Sicherheitskritische Vorgänge werden im Ereignislog protokolliert und können von Administrator/innen eingesehen werden.

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.1.6 Verwaltung von Insolvenzen

1.1.6.1 Kurzbeschreibung

Im Zusammenhang mit der Bearbeitung von Insolvenzen als Insolvenzverwalter werden Insolvenzen, Insolvenzakten und in die Insolvenzcausa involvierte Personen angelegt, die Personen und Insolvenzdaten werden im Akt und in der Insolvenz erfasst, und dort weiterbearbeitet und -verarbeitet.

Dieser Verarbeitungsvorgang umfasst das Erfassen und Verwalten von Insolvenzanmeldungen und Masseforderungen, die Sanierung und Abwicklung im Insolvenzverfahren, die Verteilung und Ausschüttung an Insolvenzgläubiger/innen, die Abrechnung zur Entlohnung der Insolvenzverwalterin / des Insolvenzverwalters und der Gläubigerschutzverbände sowie weitere im Zusammenhang mit der Verwaltung eines Insolvenzverfahrens anfallende Tätigkeiten.

1.1.6.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die Sanierung oder Abwicklung gemäß den Bestimmungen der Insolvenzordnung.

1.1.6.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	Schuldner/in inkl. Kontaktpersonen bei dieser/diesem
Anmerkungen zur Personenkategorie	Personen, über welche die Insolvenz eröffnet wurde und für welche das Insolvenzgericht eine/n Rechtsanwält/in der Kanzlei zur Insolvenzverwalterin / zum Insolvenzverwalter bestellt hat.
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO) & Rechtliche Verpflichtung (von Rechtsanwält/innen) der Kanzlei (Art. 6 Abs. 1 lit. c DSGVO):** Mit Bestellung zur Insolvenzverwalterin / zum Insolvenzverwalter gemäß § 80 IO ist diese/r *„kraft seiner Bestellung befugt, alle Rechtsgeschäfte und Rechtshandlungen vorzunehmen, welche die Erfüllung der Obliegenheiten seines Amtes mit sich bringt“* (§ 83 IO).
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Bestellung mittels Datenschutzmitteilung.

Kategorie B	Insolvenzbeteiligte Personen inkl. Kontaktpersonen bei diesen
Anmerkungen zur Personenkategorie	Alle Personen, welche in das Insolvenzverfahren involviert sind, ausgenommen der/dem Schuldner/in. Zu diesen gehören insbesondere Insolvenzgläubiger/innen, Massegläubiger/innen, Gläubigerschutzverbände, Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen und Notar/innen.
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO) & Rechtliche Verpflichtung (von Rechtsanwält/innen) der Kanzlei (Art. 6 Abs. 1 lit. c DSGVO):** Aufgrund der Bestellung zur Insolvenzverwalterin / zum Insolvenzverwalter gemäß § 80 IO und in Verbindung mit den Bestimmungen betreffend Gläubiger/innen (Insolvenzforderungen und Masseforderungen) und Gläubigerschutzverbände im Insolvenzverfahren (insb. §§ 45ff, §§ 102ff und §§ 88ff IO) besteht eine gesetzliche Rechtsgrundlage für die Verarbeitung. **Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Soweit die Person nicht Gläubiger/in oder Gläubigerschutzverband im Insolvenzverfahren ist, hat diese, aufgrund eines Geschäfts- oder Vertretungsverhältnisses mit einer solchen Person, ein berechtigtes Interesse an der Verarbeitung (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	<u>Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO):</u> Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. <u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Sofern die Daten nicht der anwaltlichen Verschwiegenheitspflicht (§ 9 RAO, § 305 Z. 4 und § 321 Z. 4 ZPO, § 144 Abs. 2 iVm § 157 Abs. 2 StPO) unterliegen (Ausnahme gemäß Art. 14 Abs. 5 lit. d DSGVO) und die Person noch nicht über die Informationen verfügt (Ausnahme gemäß Art. 14 Abs. 5 lit. a DSGVO) – in diesen Fällen sind die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) nicht anzuwenden – erfolgt dies mittels Datenschutzmitteilung.

Kategorie C	Gerichte und Behörden inkl. Kontaktpersonen bei diesen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der Verwaltung von Insolvenzen als Insolvenzverwalter/in befasste Gerichte (insb. das zuständige Insolvenzgericht) und Behörden (z.B. Finanzämter, Gemeinden).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie D	Kanzleimitarbeiter/innen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit Bearbeitungen und Korrespondenzen zum jeweiligen Insolvenzverfahren werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen,

	juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.1.6.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
				Insolvenzbet. Per.[1)]	Gerichte & Beh.[2)]	ERV-Überm.St.[3)]	Insolvenzdatei[4)]	Ggf. IT-Support[5)]					
A	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X	X	X	X					
	2	Foto	Nein					X					
	3	Anschrift	Nein	X	X	X	X	X					
	4	Kontaktdaten (Tel., Mail, Fax)	Nein	X	X	X		X					
	5	Bank- und Überweisungsdaten	Nein	X	X	X		X					
	6	Geburtsdatum	Nein	X	X	X	X	X					
	7	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein	X	X	X	X	X					
	8	Firmenbuch- und Gewerbedaten	Nein	X	X	X		X					
	9	Grundbuchdaten	Nein	X	X	X		X					
	10	UID-, FB-, ZVR-Nummer	Nein	X	X	X	X	X					
	11	Sozialversicherungsdaten	Nein	X	X	X		X					
	12	Kontaktpersonen und deren Kontaktdaten	Nein	X	X	X		X					
	13	Beteiligte Personen (Insolvenzbeteiligte Personen, Gerichte und Behörden)	Nein	X	X	X		X					
	14	Leistungsnachweise	Nein	X	X	X		X					
	15	Vertragstexte und Geschäftskorrespondenzen	Nein	X	X	X		X					
	16	Sachverhaltsdaten und Schriftsätze	Nein	X	X	X	X	X					
	17	Gerichtliche / Behördliche Erledigungen	Nein	X	X	X	X	X					
	18	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein	X	X	X		X					
B	19	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X	X		X					
	20	Foto	Nein					X					
	21	Anschrift	Nein	X	X	X		X					
	22	Kontaktdaten (Tel., Mail, Fax)	Nein	X	X	X		X					
	23	Bank- und Überweisungsdaten	Nein	X	X	X		X					
	24	Geburtsdatum	Nein	X	X	X		X					
	25	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein	X	X	X		X					
	26	Firmenbuch- und Gewerbedaten	Nein	X	X	X		X					
	27	Grundbuchdaten	Nein	X	X	X		X					

	28	UID-, FB-, ZVR-Nummer	Nein	X	X	X		X					
	29	Sozialversicherungsdaten	Nein	X	X	X		X					
	30	Kontaktpersonen und deren Kontaktdaten	Nein	X	X	X		X					
	31	Beteiligte Personen (Insolvenzbeteiligte Personen, Gerichte und Behörden)	Nein	X	X	X		X					
	32	Leistungsnachweise	Nein	X	X	X		X					
	33	Vertragstexte und Geschäftskorrespondenzen	Nein	X	X	X		X					
	34	Sachverhaltsdaten und Schriftsätze	Nein	X	X	X		X					
	35	Gerichtliche / Behördliche Erledigungen	Nein	X	X	X		X					
	36	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein	X	X	X		X					
C	37	Kontaktpersonen und deren Kontaktdaten	Nein	X	X	X	X	X					
D	38	Name	Nein	X	X	X		X					
	39	Funktion in der Kanzlei	Nein	X	X	X		X					
	40	Dienstliche Kontaktdaten	Nein	X	X	X		X					

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Insolvenzbet. Per.: Alle insolvenzbeteiligten Personen inkl. Schuldner/in (entspricht den Personenkategorien A und B)

[2)] Gerichte & Beh.: Gerichte und Behörden (entspricht der Personenkategorie C)

[3)] ERV-Überm.St.: Übermittlungsstellen für den elektronischen Rechtsverkehr, kundgemacht gemäß § 3 Abs. 1 der Verordnung über den elektronischen Rechtsverkehr auf *http://kundmachungen.justiz.gv.at*

[4)] Insolvenzdatei: Vom Insolvenzgericht aufgrund §§ 255f IO bekanntzumachende Daten, veröffentlicht auf *http://edikte.justiz.gv.at*.

[5)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.1.6.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Insolvenzbet. Per.	Im Ausnahmefall[1)]	Im Ausnahmefall[2)]
Gerichte & Beh.	Im Ausnahmefall[3)]	Nein
ERV-Überm.St.	Nein	Nein
Insolvenzdatei	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

[1)] Sofern eine insolvenzbeteiligte Person in einem Drittstaat ansässig ist, erfolgt die Übermittlung in diesen Drittstaat.

[2)] Sofern eine insolvenzbeteiligte Person eine internationale Organisation ist, erfolgt die Übermittlung an diese internationale Organisation.

[3)] Sofern ein Gericht oder eine Behörde eines Drittstaates befasst wird, erfolgt eine Übermittlung in diesen Drittstaat.

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Die Übermittlung in Drittländer und an internationale Organisationen erfolgt ausschließlich unter Gewährleistung des durch die Datenschutzgrundverordnung normierten Schutzniveaus. Weil die

ganze Welt und jede Person dieser Welt als Adressat in Frage kommen, kann dieser Aspekt nicht global für den Verarbeitungsvorgang, sondern nur im Einzelfall sichergestellt werden.

Im Einzelfall wird geprüft,

- ob ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, welcher ein angemessenes Schutzniveau bei der adressierten Person konstatiert (Art. 45 DSGVO)
- ob geeignete Garantien vorliegen oder geschaffen werden können (Art. 46f DSGVO)
- ob ein Ausnahmetatbestand, welcher die Übermittlung erlaubt, erfüllt ist (Art. 49 DSGVO) Vor allem diese Ausnahmetatbestände können zur Anwendung kommen:
  - Ausdrückliche Einwilligung nach Unterrichtung (Art. 49 Abs. 1 lit. a)
  - Im Interesse der betroffenen Person aufgrund eines Vertrages des verantwortlichen Parteimit einer anderen Person (Art. 49 Abs. 1 lit. c)
  - Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich (Art. 49 Abs. 1 lit. e)

1.1.6.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt in Erfüllung der rechtsanwaltlichen Aufbewahrungspflichten gemäß § 12 RAO für die Dauer von fünf Jahren ab Aufhebung der Insolvenz und umfasst sämtliche Datenkategorien. Die Aufhebung wird durch Hinterlegung des Aufhebungsdatums je Insolvenz dokumentiert, wodurch ein systemisches Bereinigen (Löschen von alten Insolvenzen) möglich ist.

Soweit es zur Abwehr etwaiger Schadenersatzansprüche erforderlich ist, werden die Daten einer Insolvenz und der involvierten Personen für die Dauer von 30 Jahren (lange Verjährungsfrist) ab Aufhebung der jeweiligen Insolvenz aufbewahrt.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT“ Möglichkeiten, welche den Schutz der Daten, die über den Abschluss einer Causa hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs“).

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.1.6.7 Datenminimierung

Nicht nur zur Sicherung eines hohen Datenschutzniveaus, sondern auch für eine schlanke und effiziente Kanzleiverwaltung werden ausschließlich Daten erfasst, welche für die Bearbeitung der jeweiligen Insolvenz, und damit zur Erfüllung des Zweckes dieses Verarbeitungsvorgangs, erforderlich oder zumindest zweckdienlich sind.

Das Erfassen von Daten erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Datenerfassung fördert den Grundsatz der Datenminimierung, zumal das Erfassen jedes einzelnen Datums mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Die Verarbeitung von personenbezogenen Daten bei der Bearbeitung von Insolvenzen erfolgt, bedingt durch die konkreten Regelungen der IO und die sich daran orientierende Software ADVOKAT, sehr formalisiert. Es werden daher nur die aufgrund dieser Formalien zu erhebenden Daten (insb. Insolvenzanmeldungen und Masseforderungen), erfasst und verarbeitet. Überhaupt ist das zweckfreie Sammeln von Daten der Arbeitsweise einer Rechtsanwaltskanzlei fremd.

Die genannten Gründe gelten entsprechend auch für den Umfang der Verarbeitung.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu den in Akten gespeicherten Daten haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT“ (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bieten ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung) und die Verwendung von Microsoft SharePoint (Dokumentenmanagementsystem mit Anbindung an ADVOKAT-Security) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

Bei Verwendung von ADVOKAT Security kann der Zugriff auf die Insolvenzverwaltung auf einzelne oder wenige Benutzer beschränkt werden. Zusätzlich ist es möglich, dass aufgehobene Insolvenzen automatisch in einen virtuellen, versperrten Aktenschrank abgelegt werden (sodass diese z.B. nur noch für den Insolvenzverwalter selbst oder dessen Vorgesetzten sichtbar und zugreifbar sind).

1.1.6.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Teilweise Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine automatisierte Verarbeitung von Daten
- Verarbeitung aller Daten erfolgt zum überwiegenden Teil nur innerhalb des Kanzleinetzwerks
- Die Weitergabe von Daten erfolgt ausschließlich an solche Empfänger/innen, welche ihrerseits ein hohes Schutzniveau bieten, zumal diese selbst ein Interesse an einem hohen Schutzniveau haben.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:
- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (nur sehr wenige Datenübermittlungen an einen geschlossenen Empfängerkreis; aufgrund ausschließlich manueller Verarbeitung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (die Verarbeitung erfolgt vornehmlich innerhalb der Kanzleiräumlichkeiten und damit durch qualifiziertes Kanzleipersonal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (die Verarbeitungszwecke sind gesetzlich dargelegt und in der westlichen Gesellschaft nicht nur anerkannt, sondern sogar hochgehalten; diese sind legitim und klar abgegrenzt)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.6.9 Spezifische TOMs

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

Die Übermittlung von Daten in ein Drittland oder eine internationale Organisation wird im Einzelfall geprüft und das Schutzniveau der DSGVO sichergestellt. Siehe dazu die entsprechenden Ausführungen oberhalb.

Bei Verwendung von ADVOKAT Security: Das Berechtigungssystem der Anwaltssoftware „ADVOKAT“ ermöglicht die Verwaltung von Rechten für Benutzer/innen und -gruppen betreffend einzelne Akten, Aktengruppen und einzelne Programmbereiche. Dieses Berechtigungssystem stellt sicher, dass nur jene Kanzleimitarbeiter/innen Zugang zu Daten eines Insolvenzaktes haben, welche diesen auch tatsächlich für die Erfüllung der Verarbeitungszwecke benötigen.

Bei Verwendung von Microsoft SharePoint: Das mit der Anwaltssoftware „ADVOKAT“ verbundene Berechtigungssystem stellt sicher, dass Dokumente und andere Dateien nur für jene Kanzleimitarbeiter/innen zugänglich sind, welche den Zugang für die Erfüllung der Verarbeitungszwecke benötigen. Die Versionierung von Dokumenten schafft zusätzlich einen Manipulationsschutz für alle Dokumente. Je nach Ausführungsvariante von Microsoft SharePoint stehen weitere Sicherheitsfunktionen zur Verfügung.

Personen schützen

Bei Verwendung von ADVOKAT Security: Die Anwaltssoftware „ADVOKAT“ ermöglicht die Hinterlegung von berechtigten Benutzergruppen bei Personen im Adressbestand. Nur die auf solche Weise berechtigten Personen können überhaupt feststellen, dass es diese Person im System gibt. Für nicht Berechtigte gibt es die Person nicht.

Als besonderes Feature können Benutzer/innen eine Person ausnahmsweise doch sehen, wenn diese in einem Akt beteiligt ist, auf welchen die/der Benutzer/in zugreifen darf. Das ist nötig, damit Benutzer/innen den Akt, welchen diese (mit)bearbeiten, bearbeiten können. Sobald jedoch der Zugriff auf den Akt verloren geht (idealerweise bei Ablage des Aktes) entfällt damit auch der Zugriff auf die Person, sodass die Person, aus Sicht der Benutzerin / des Benutzers, aus dem System verschwindet.

Um die Erfüllung anderer Aufgaben und Pflichten (z.B. Auskunftsrecht) nicht zu gefährden, kann einzelnen Benutzer/innen das Recht eingeräumt werden, sämtliche Personen sehen zu dürfen. Dieses Recht ist sehr restriktiv handzuhaben.

Insolvenzverwaltung

Bei Verwendung von ADVOKAT Security kann der Zugriff auf die Insolvenzverwaltung auf einzelne oder wenige Benutzer/innen beschränkt werden. Zusätzlich ist es möglich, dass aufgehobene Insolvenzen automatisch in einen virtuellen, versperrten Aktenschrank abgelegt werden (sodass diese z.B. nur noch für die/den Insolvenzverwalter/in selbst oder deren/dessen Vorgesetzten sichtbar und zugreifbar sind).

1.1.7 Elektronisches Urkundenarchiv (Archivium)

1.1.7.1 Kurzbeschreibung

Im Zusammenhang mit der verpflichtenden elektronischen Einbringung von Eingaben im Firmenbuch- und im Grundbuchverfahren via ERV besteht gemäß § 89c Abs. 2 Z. 3 GOG iVm § 89b Abs. 2 GOG

iVm §§ 8a, 9 und 10 ERV-Verordnung die Pflicht, Urkunden, die im Original oder in beglaubigter Abschrift vorzulegen sind, in das Urkundenarchiv des ÖRAK (§ 91c GOG iVm § 37 Abs. 1 Z. 7 RAO iVm der Urkundenarchiv-Richtlinie des ÖRAK) einzustellen.

Die dafür gemäß § 91d GOG von der ÖRAK beauftragte Dienstleisterin ist die Archivium Dokumentenarchiv GmbH – gemäß § 1 Abs. 1 Urkunden-RL kundgemacht auf der Webseite des ÖRAK (*https://www.rechtsanwaelte.at/kammer/oerak/archivium-gmbh/*) –, welche die Software „Archivium" zur Verfügung stellt.

Die mit der anwaltschaftlichen Vertretung und Beratung von Klient/innen erforderlichen elektronischen Urkundenübermittlungen werden gemäß den gesetzlichen Vorgaben mit Archivium und der Anwaltssoftware „ADVOKAT" durchgeführt. Mit Archivium werden die Urkunden in das elektronische Archiv hochgeladen und mit der Anwaltssoftware „ADVOKAT" werden die ERV-Nachrichten, in welchen auf die archivierten Urkunden verwiesen wird, eingebracht.

1.1.7.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die rechtskonforme Übermittlung von Urkunden im ERV, welche im Original oder in beglaubigter Abschrift vorzulegen sind, um den übergeordneten Zweck der rechtsanwaltlichen Vertretung und Beratung von Klient/innen erfüllen zu können.

1.1.7.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

1.1.7.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
				Gerichte[1)]	Archivium[2)]	Ggf. IT-Support[3)]							
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein			X							
	2	Anschrift	Nein			X							
	3	Geburtsdatum	Nein			X							
	4	UID-, FB-, ZVR-Nummer	Nein			X							
	5	Urkunden und Metadaten zu Urkunden	Nein	X	X	X							

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Gerichte: Empfänger der ERV-Nachricht, welche auf eine Urkunde im Urkundenarchiv verweist

[2)] Archivium: Archivium Dokumentenarchiv GmbH
Mit der Software Archivium werden Urkunden in das elektronische Urkundenarchiv hochgeladenen. Das elektronische Urkundenarchiv wird von der Archivium Dokumentenarchiv GmbH betrieben.

[3)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.1.7.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Gerichte	Nein	Nein
Archivium	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.1.7.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung von Urkunden im elektronischen Urkundenarchiv erfolgt gemäß § 6 Abs. 2 Urkundenarchiv-Richtlinie für die Dauer von wahlweise sieben oder 30 Jahren. Es wird jeweils die für den Einzelfall erforderliche, d.h. – sofern tunlich – die kürzere Dauer gewählt. Im Bedarfsfall kann eine Verlängerung der Aufbewahrung erfolgen. Aufgrund der mit der Aufbewahrungsdauer korrelierenden Kosten ist eine kurze Aufbewahrung auch wirtschaftlich im Interesse der Kanzlei.

1.1.7.7 Datenminimierung

Da die Archivierung von Urkunden im elektronischen Urkundenarchiv für jede einzelne Urkunde mit Arbeitsaufwand und Kosten verbunden ist, werden Urkunden nur dann archiviert, wenn dies für die Erfüllung der Verarbeitungszwecke notwendig oder zweckmäßig ist.

Das Archivieren erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Datenerfassung fördert den Grundsatz der Datenminimierung.

Der Umfang der Verarbeitung ist zur Gänze vorbestimmt und entzieht sich dem Einfluss der Kanzlei.

1.1.7.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine automatisierte Verarbeitung von Daten
- Die Archivierung von Urkunden ist vollständig reglementiert und in dieser Weise gesetzlich vorgeschrieben. Die Verarbeitung muss auf diese Weise erfolgen.
- Die Weitergabe von Daten erfolgt ausschließlich an Gerichte und an die per Gesetz über den ÖRAK ermächtigte Archivium Dokumentenarchiv GmbH. Beide Empfänger bieten ein hohes Schutzniveau, zumal diese selbst ein Interesse an einem hohen Schutzniveau haben.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:
- Verwendung neuer Technologien: Niedriges Risiko (sichere HTTPS-Kommunikation; sicheres Authentisierungs- und Authentifizierungsverfahren via Smartcard und PIN)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (Verarbeitung nur im erforderlichen Einzelfall; der Umfang der Verarbeitung je Einzelfall ist sehr gering und aufgrund von Vorgaben dem Einfluss der Kanzlei entzogen; Offenlegungen erfolgt nur an österreichische Gerichte)
- Umstände der Verarbeitung: Niedriges Risiko (die Verarbeitung erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und damit durch qualifiziertes Kanzleipersonal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (die Gesetzgebung hat die Archivierung in von

  Körperschaften des öffentlichen Rechts zu errichtenden Archiven legislativ bestimmt, sodass der Zweck für die Allgemeinheit als wesentlich und legitim zu betrachten ist)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.7.9 Spezifische TOMs

Die Vornahme von Archivierungen erfordert das Einstecken des Rechtsanwaltsausweises in ein Kartenlesegerät sowie die Eingabe eines PINs. Dadurch ist dieser Verarbeitungsvorgang auf die/den einzelnen Rechtsanwält/in als einzige berechtigte Person beschränkt.

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche

den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.1.8 Marketing und Akquise (Serienbrief, Anfragen, Erstberatung)

1.1.8.1 Kurzbeschreibung

Zur Förderung der Prosperität der Kanzlei werden mögliche neue Klient/innen angeworben. Dies geschieht durch Vorträge von Kanzleimitarbeiter/innenn, Aussendung von Postsendungen und Newslettern an einen definierten Empfängerkreis (Einwilligung vorausgesetzt), der Bearbeitung von Anfragen sowie dem Angebot einer kostenlosen bzw. kostengünstigen anwaltlichen Erstberatung.

Im Zusammenhang mit diesem Verarbeitungsvorgang wird kein Akt angelegt, es werden jedoch regelmäßig Personen erfasst, soweit dies dem Zweck dieses Verarbeitungsvorgangs dient.

1.1.8.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die Förderung der Prosperität der Kanzlei durch Anwerbung möglicher neuer Klient/innen. Existenzieller Minimalzweck ist die Aufrechterhaltung eines wirtschaftlich tragfähigen Kanzleibetriebes.

1.1.8.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Marketingadressat/innen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche aufgrund von Vorträgen, anderen geschäftlichen Veranstaltungen und Zusammentreffen oder aufgrund von Anfragen als Marketingadressat/innen erfasst wurden.
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Aussendung von Postsendungen Anwaltliche Erstberatung **Einwilligung (Art. 6 Abs. 1 lit. a DSGVO):** Aussendung von Newslettern (E-Mails)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt mittels Datenschutzmitteilung.

Kategorie B	**Kanzleimitarbeiter/innen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit Vorträgen und der Bearbeitung von Anfragen werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.1.8.4 Kategorien der verarbeiteten Daten und Empfänger

	Datenkategorien		Empfänger

				Ggf. IT-Support[1)]									
A	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X									
	2	Anschrift	Nein	X									
	3	Kontaktdaten (Tel., Mail, Fax)	Nein	X									
	4	Kontaktpersonen und deren Kontaktdaten	Nein	X									
B	5	Name	Nein	X									
	6	Funktion in der Kanzlei	Nein	X									
	7	Dienstliche Kontaktdaten	Nein	X									

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.1.8.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.1.8.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Es erfolgt keine, über die Zweckerreichung hinausgehende Aufbewahrung von personenbezogenen Daten. Die Daten werden gelöscht, sobald der Zweck der Verarbeitung wegfällt oder die betroffene Person der Verarbeitung zu diesem Zweck widerspricht.

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.1.8.7 Datenminimierung

Es werden ausschließlich jene Daten erfasst, welche zur Erreichung der Verarbeitungszwecke erforderlich sind (insb. Adresse für Postsendungen; E-Mail-Adresse für elektronische Sendungen).

Das Erfassen von Daten erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Datenerfassung fördert den Grundsatz der Datenminimierung, zumal das Erfassen jedes einzelnen Datums mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Personen werden in der Anwaltssoftware „ADVOKAT“ erfasst. Für den Zweck der Festlegung von Empfängerkreisen können freie Felder definiert werden, sodass es etwa die Ja/Nein-Felder „Newsletter“ und „Postwerbung“ geben kann, welche per Standard mit „Nein“ belegt sind (privacy by default). Die Anwaltssoftware „ADVOKAT“ ermöglicht das Versenden von Newslettern an einen so definierten Empfängerkreis sowie das Erstellen einer Datenquelle für Serienbriefe (Postaussendungen).

Aussendungen erfolgen nur in großen Zeitabständen. Je Aussendung werden personenbezogene Daten nur in dem für die Zustellung der Sendungen erforderlichen Umfang verarbeitet.

Bei Verwendung von ADVOKAT Security kann der Zugang zu Marketingadressat/innen auf einen oder wenige Benutzer beschränkt werden, sodass diese Personen und deren Daten für andere Benutzer gar nicht existieren.

1.1.8.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Keine

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Keine Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen
- Keine automatisierte Verarbeitung von Daten
- Verarbeitung aller Daten erfolgt zum überwiegenden Teil nur innerhalb des Kanzleinetzwerks
- Es erfolgte keine Weitergabe von Daten
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:
- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (Aussendungen erfolgen nur in großen Zeitabständen; je Aussendung werden personenbezogene Daten nur in dem für die Zustellung der Sendungen erforderlichen Umfang verarbeitet.)
- Umstände der Verarbeitung: Niedriges Risiko (die Verarbeitung erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und damit durch qualifiziertes Kanzleipersonal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (die Klient/innenakquise ist eine für den Kanzleibetrieb notwendige Tätigkeit und dient damit einer gesunden Wirtschaft; Werbung ist ein allgemein anerkannter Zweck)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.1.8.9 Spezifische TOMs

Bei Verwendung von ADVOKAT Security kann der Zugang zu in der Adressenverwaltung erfassten Personen, im konkreten Fall die Sichtbarkeit von Marketingadressat/innen, auf einen oder wenige Benutzer/innen beschränkt werden, sodass diese Personen und deren Daten für andere Benutzer/innen gar nicht existieren.

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.2 Allgemeine Nebentätigkeiten

1.2.1 Mobiles Arbeiten

1.2.1.1 Kurzbeschreibung

Für mobiles Arbeiten (z.B. in Zusammenhang mit Dienstreisen, Gerichtsverhandlungen) werden Mobilgeräte verwendet (Smartphones, Laptops). Das Arbeiten mit Mobilgeräten erfolgt entweder remote (z.B. durch Aufbau einer Fernverbindung via TeamViewer oder Remote Desktop Verbindung), lokal (z.B. durch vorangehende Übertragung von Daten auf das entsprechende Mobilgerät) oder via die Smartphone-App „ADVOKAT Mobil".

Dieser Verarbeitungsvorgang umfasst nur die Datenflüsse zur Ermöglichung und Abwicklung des mobilen Arbeitens, also insb. die Übertragung von Daten via Internet.

1.2.1.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist das mobile Arbeiten zur Erfüllung der Zwecke anderer Verarbeitungsvorgänge, für welche dieser Verarbeitungsvorgang in dienender Funktion steht (insb. der Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz").

1.2.1.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	**Gerichte und Behörden inkl. Kontaktpersonen bei diesen**
Anmerkungen zur	Im Zusammenhang mit der jeweiligen Causa befasste Gerichte (zuständige Zivil- und Strafgerichte)

Personenkategorie	und Behörden (z.B. Finanzämter, Vermessungsämter, Grundverkehrsbehörden, Bezirkshauptmannschaften, Gemeinden, Kammern).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie D	**Kanzleimitarbeiter/innen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit Bearbeitungen und Korrespondenzen zur jeweiligen Causa werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.2.1.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein										
	2	Anschrift	Nein										
	3	Kontaktdaten (Tel., Mail, Fax)	Nein										
	4	Geburtsdatum	Nein										
	5	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein										
	6	Firmenbuch- und Gewerbedaten	Nein										
	7	Grundbuchdaten	Nein										
	8	UID-, FB-, ZVR-Nummer	Nein										
	9	Sozialversicherungsdaten	Nein										
	10	Kontaktpersonen und deren Kontaktdaten	Nein										
	11	Beteiligte Personen (Aktbeteiligte Personen, Gerichte und Behörden)	Nein										
	12	Leistungsnachweise	Nein										
	13	Vertragstexte und Geschäftskorrespondenzen	Nein										
	14	Sachverhaltsdaten und Schriftsätze	Nein										
	15	Gerichtliche / Behördliche Erledigungen	Nein										

	16	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein											
	17	Ggf. Daten zu Bonität / Solvenz, Mahndaten	Nein											
	18	Ggf. Daten woraus die rassische/ethische Herkunft hervorgehen (Art. 9 DSGVO)	Ja[1)]											
	19	Ggf. Daten woraus politische Meinungen hervorgehen (Art. 9 DSGVO)	Ja[1)]											
	20	Ggf. Daten woraus religiöse/weltanschauliche Überzeugungen hervorgehen (Art. 9 DSGVO)	Ja[1)]											
	21	Ggf. Daten woraus eine Gewerkschafts-zugehörigkeit hervorgeht (Art. 9 DSGVO)	Ja[1)]											
	22	Ggf. genetische Daten (Art. 9 DSGVO)	Ja[1)]											
	23	Ggf. biometrische Daten (Art. 9 DSGVO)	Ja[1)]											
	24	Ggf. Gesundheitsdaten (Art. 9 DSGVO)	Ja[1)]											
	25	Ggf. Daten zu Sexualleben / sexueller Orientierung (Art. 9 DSGVO)	Ja[1)]											
	26	Ggf. strafrechtliche Daten (Art. 10 DSGVO)	Ja[1)]											
C	27	Kontaktpersonen und deren Kontaktdaten	Nein											
D	28	Name	Nein											
	29	Funktion in der Kanzlei	Nein											
	30	Dienstliche Kontaktdaten	Nein											

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Diese Datenkategorien werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

1.2.1.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Keine	-	-

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.2.1.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Bei mobilem Arbeiten via Fernverbindung (TeamViewer, Remote Desktop) werden keine Daten lokal gespeichert, sodass es keiner Löschung bedarf. Bei mobilem Arbeiten mit der Smartphone-App „ADVOKAT mobil“ werden Daten über eine HTTPS-Verbindung mit TLS-Transportverschlüsselung übertragen. Mit der Übertragung werden die Daten am Mobilgerät laufend bereinigt, d.h. dass ausschließlich das in der Kanzlei definierte Soll vom Mobilgerät zugreifbar und am Mobilgerät gespeichert ist. In einer Arbeitsanweisung bzw. im Dienstvertrag ist festgehalten, dass nur jene Daten an das Mobilgerät übertragen werden dürfen, welche für die Erfüllung konkreter Verarbeitungszwecke erforderlich sind.

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.2.1.7 Datenminimierung

Im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang erfolgt keine Datenerhebung. Zum Umfang der Verarbeitung wurde oberhalb ausgeführt (siehe dazu bei „Lösch- und Aufbewahrungsfristen“).

Bei Verwendung von ADVOKAT Security: Die Verwaltung der über Mobilgeräte zugänglichen Daten kann auf einzelne Benutzer/innen eingeschränkt werden und kann für jedes Mobilgerät unabhängig erfolgen. Die am Mobilgerät gespeicherten Daten sind verschlüsselt (bei Android muss diese Option aktiv aktiviert werden) und aufgrund eines gesicherten Zugangs (Codesperre) nur durch den Inhaber des Mobilgeräts verwendbar. Auch kann der Zugang zur Mobilgeräteverwaltung zur Registrierung neuer Mobilgeräte im Anwaltsprogramm „ADVOKAT“ nur für einzelne Benutzer/innen freigeschalten werden.

1.2.1.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen
- Übertragung über das Internet

Für ein niedriges Risiko sprechen folgende Faktoren:
- Die Weitergabe von Daten erfolgt ausschließlich an Mitarbeiter der Kanzlei.
- Die Übermittlung von Daten im Zusammenhang mit der Smartphone-App „ADVOKAT mobil“ erfolgt ausschließlich über eine sichere HTTPS-Verbindung mit TLS-Transportverschlüsselung. Die Authentisierung und Authentifizierung für den Zugriff durch Mobilgeräte erfolgt via Benutzerkennung (eindeutige Geräte-ID) und Kennwort.
- Es werden nur jene Daten übertragen und es sind nur jene Daten am Mobilgerät gespeichert, welche aktuell von dem Inhaber des Mobilgeräts zur Erreichung konkreter Verarbeitungszwecke erforderlich sind. Die am Mobilgerät gespeicherten Daten sind verschlüsselt und können nur durch Anmeldung am Mobilgerät (Codesperre) entschlüsselt werden (bei Android muss diese Option aktiv aktiviert werden).
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (sichere HTTPS-Kommunikation mit TLS-Transportverschlüsselung; sicheres Authentisierungs- und Authentifizierungsverfahren mit Benutzerkennung und Kennwort)
- Art der Verarbeitung: Niedriges Risiko (der Umfang der Verarbeitung wird ausschließlich manuell durch berechtigte Mitarbeiter festgelegt)
- Umfang der Verarbeitung: Niedriges Risiko (es erfolgt keine Offenlegung von Daten; mit jeder Übertragung werden die am Mobilgerät gespeicherten Daten automatisch bereinigt, womit dieser auf das Notwendige reduziert ist)
- Umstände der Verarbeitung: Niedriges Risiko (die Festlegung der zu übertragenden Daten erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und nur durch die dazu berechtigte Person; es besteht zu

	keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
• Zwecke der Verarbeitung:	Niedriges Risiko (es wird auf den Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“ verwiesen; das mobile Arbeiten dient einer effizienten Bearbeitung und ist allgemein anerkannt)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.2.1.9 Spezifische TOMs

Die Übertragung von Daten auf das Mobilgerät setzt die Festlegung der zu übertragenden Daten und der Übertragung selbst in der Anwaltssoftware „ADVOKAT“ voraus. Der dafür nötige Zugang zur Mobilgeräteverwaltung, die auch zur Verwaltung und Registrierung neuer Mobilgeräte dient, kann nur für einzelne Benutzer/innen freigeschalten werden. Eine sichere HTTPS-Verbindung sowie ein gesicherter VPN-Tunnel sorgen für eine hohe Sicherheit beim Transport der Daten. Eine Übertragung erfolgt nur nach erfolgter Authentisierung und Authentifizierung mit Benutzerkennung (eindeutige Geräte-ID) und Kennwort.

Alle Übertragungen werden protokolliert.

Jede Übertragung bereinigt die am Mobilgerät gespeicherten Daten automatisch auf das in der Kanzlei für das jeweilige Mobilgerät definierte Soll, womit die Daten immer auf das Minimum reduziert sind (siehe dazu bei „Lösch- und Aufbewahrungsfristen“).

Die am Mobilgerät gespeicherten Daten sind verschlüsselt. Nur durch Anmeldung am Mobilgerät (Codesperre) werden die Daten entschlüsselt. Bei Verlust oder Diebstahl, wofür bei Mobilgeräten eine erhöhte Gefahr besteht, sind die Daten daher nicht entzifferbar.

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.2.2 Kommunikation via ADVOCOM

1.2.2.1 Kurzbeschreibung

Ein wesentlicher Bestandteil der anwaltlichen Tätigkeit ist der Austausch mit Klient/innen sowie anderen kanzleiexternen Personen (z.B. Beklagte, Vertragspartner, Nebenintervenienten, Privatankläger, Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige).

ADVOCOM ist ein Online-Dienst zur vertraulichen und DSGVO-konformen Kommunikation. Über diesen Dienst erfolgt ein Austausch mit kanzleiinternen und -externen Personen. Der Austausch beinhaltet Schriftverkehr und Dateien aller Art wie z.B. Dokumente, Bilder, Videos, u.a.m.

1.2.2.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist der Austausch mit kanzleiinternen und -externen Personen (Informationsbeschaffung und -verteilung) zur Erfüllung der Zwecke anderer Verarbeitungsvorgänge, für welche dieser Verarbeitungsvorgang in dienender Funktion steht (insb. der Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“).

1.2.2.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	<u>Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO):</u> Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. <u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	**Sonstige Kommunikationsparteien inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der anwaltlich-operativen Tätigkeit und der unternehmerischen Führung des Kanzleibetriebes kann es auch zur Kommunikation mit anderen als den zuvor genannten Personenkategorien (z.B. Steuerberatung, externe Buchhaltung) kommen. In diesen Fällen werden auch deren Daten entsprechend verarbeitet.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Die Kommunikation dient in irgendeiner Weise der Kommunikationsgegenpartei, die in Ihrer geschäftlichen Funktion kontaktiert wird. Dies kann Teil einer bestehenden Geschäftsbeziehung oder geschäftsanbahnend sein (Vertragserfüllung) oder es gibt sonstige berechtigte Gründe, die Person geschäftlich zu kontaktieren (berechtigtes Interesse).
Erfüllung der Informations-pflichten für diese Personenkategorie	Bei Vertragserfüllung erfolgt die Erfüllung der Informationspflicht im entsprechenden Vertrag. Bei berechtigtem Interesse sind zwei Fälle zu unterscheiden: <u>Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO):</u> Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. <u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie D	Kanzleimitarbeiter/innen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit Bearbeitungen und Korrespondenzen zur jeweiligen Causa werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.2.2.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger										
				Kommunik.-Teiln.[2)]	Provider[3)]	Ggf. IT-Support[4)]								
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X	X								
C	2	Kontaktdaten (Tel., Mail)	Nein	X	X	X								
	3	Kontaktpersonen und deren Kontaktdaten	Nein	X	X[5)]	X[5)]								
	4	Verschiedenste, für den geschäftlichen Austausch erforderliche oder jedenfalls relevante Daten und Dateien	Ja[1)]	X	X[5)]	X[5)]								
D	5	Name	Nein	X	X	X								
	6	Foto	Nein	X	X	X								
	7	Dienstliche Kontaktdaten (Tel., Mail)	Nein	X	X	X								

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Datenkategorien im Sinne der Artikel 9 und 10 DSGVO werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

[2)] Kommunikationsteilnehmer: Alle in Kommunikationen via ADVOCOM eingeladene und dadurch involvierte Personen (entspricht den Personenkategorien A, B, C und D)

[3)] Provider = ADVOKAT Unternehmensberatung Greiter & Greiter GmbH

[4)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

[5)] Diese Datenkategorien sind aufgrund der zur Anwendung kommenden, mehrschichtigen Verschlüsselungslösungen nur den Kommunikationsteilnehmern einsichtig. Technisch betrachtet erfolgt aber eine Übermittlung auch an Provider (in verschlüsselter Form) und ggf. IT-Support (direkt am Gerät).

1.2.2.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Kommunikationsteilnehmer	Im Ausnahmefall[1)]	Im Ausnahmefall[2)]
Provider	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

[1)] Sofern eine aktbeteiligte Person in einem Drittstaat ansässig ist, erfolgt die Übermittlung in diesen Drittstaat.

[2)] Sofern eine aktbeteiligte Person eine internationale Organisation ist, erfolgt die Übermittlung an diese internationale Organisation.

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Die Übermittlung an Drittstaaten und an internationale Organisationen erfolgt ausschließlich unter Gewährleistung des durch die Datenschutzgrundverordnung normierten Schutzniveaus. Weil die ganze Welt und jede Person dieser Welt als Adressat in Frage kommen, kann dieser Aspekt nicht global für den Verarbeitungsvorgang, sondern nur im Einzelfall sichergestellt werden.

Im Einzelfall wird geprüft,
- ob ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, welcher ein angemessenes Schutzniveau bei der adressierten Person konstatiert (Art. 45 DSGVO)
- ob geeignete Garantien vorliegen oder geschaffen werden können (Art. 46f DSGVO)
- ob ein Ausnahmetatbestand, welcher die Übermittlung erlaubt, erfüllt ist (Art. 49 DSGVO) Vor allem diese Ausnahmetatbestände können zur Anwendung kommen:
  - Ausdrückliche Einwilligung nach Unterrichtung (Art. 49 Abs. 1 lit. a)
  - Im Interesse der betroffenen Person aufgrund eines Vertrages des verantwortlichen Parteimit einer anderen Person (Art. 49 Abs. 1 lit. c)
  - Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich (Art. 49 Abs. 1 lit. e)

1.2.2.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Lösch- und Aufbewahrungsfristen ergeben sich aus jenen Verarbeitungsvorgängen, zu denen dieser in dienender Funktion steht, das ist insbesondere der Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“.

In ADVOCOM können Kommunikationen angehalten werden, womit eine gewisse Einschränkung der Verarbeitung möglich ist. Weiters können Kommunikationen gelöscht werden, wodurch diese unmittelbar und unwiderruflich beim Provider vernichtet werden. Weiters unterstützt ADVOCOM eine „Löschung bei Vergessen“, wodurch alle Daten gelöscht werden, wenn ein Benutzer für drei Jahr nicht aktiv war (keine Anmeldung).

1.2.2.7 Datenminimierung

Die Grundsätze zur Datenminimierung ergeben sich aus jenen Verarbeitungsvorgängen, zu denen dieser in dienender Funktion steht, das ist insbesondere der Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“.

1.2.2.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen

- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen
- Übertragung über das Internet
- Der Dienst ADVOCOM kann auf allen möglichen Geräten verwendet werden (z.B. Smartphones)

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine automatisierte Verarbeitung von Daten
- Bei der Verarbeitung der Daten kommt ein mehrschichtiges Verschlüsselungskonzept zum Einsatz. Zunächst werden alle Nachrichten (Nachrichtentext und Dateien) am absendenden Gerät verschlüsselt und erst am empfangenden Gerät entschlüsselt. Weiters erfolgt die Übermittlung von Daten ausschließlich über eine sichere HTTPS-Verbindung mit TLS-Transport-Verschlüsselung. Schließlich werden die Inhaltsdaten (Nachrichtentext, Dateinamen und Dateitypen) vom ADVOCOM-Server beim Ablegen in die Datenbank zusätzlich nochmal verschlüsselt.
- Die Verwendung von ADVOCOM erfordert eine Authentifizierung am Anmeldedienst gemäß dem hochmodernen Open ID Connect Standard.
- Die Weitergabe von Daten erfolgt ausschließlich an solche Empfänger/innen, welche ihrerseits ein hohes Schutzniveau bieten, zumal diese selbst ein Interesse an einem hohen Schutzniveau haben.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (mehrschichtiges Verschlüsselungskonzept; sicheres Authentisierungs- und Authentifizierungsverfahren gemäß dem hochmodernen Standard Open ID Connect)
- Art der Verarbeitung: Niedriges Risiko (die Verarbeitung wird ausschließlich manuell initiiert und wird über einen vertrauenswürdigen Anbieter mit mehrschichtigem Verschlüsselungskonzept abgewickelt)
- Umfang der Verarbeitung: Niedriges Risiko (der Umfang der Verarbeitung wird ausschließlich manuell durch berechtigte Mitarbeiter festgelegt)
- Umstände der Verarbeitung: Niedriges Risiko (die Festlegung der zu übertragenden Daten erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und nur durch die dazu berechtigte Person; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (es wird auf den Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“ verwiesen; die Verwendung des Dienstes ADVOCOM dient gerade dazu, im Sinne der Datensicherheit anderen Kommunikationsdiensten wie z.B. E-Mails auszuweichen)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.2.2.9 Spezifische TOMs

Ein mehrschichtiges Verschlüsselungskonzept sorgt für besonders hohe Datensicherheit. Alle Nachrichten (Nachrichtentext und Dateien) werden am absendenden Gerät verschlüsselt und erst am empfangenden Gerät entschlüsselt (symmetrische AES-256-Verschlüsselung und asymmetrische Verschlüsselung der symmetrischen Schlüssel entsprechend RFC447, RSA-OAEP 2048). Weiters erfolgt die Übermittlung von Daten ausschließlich über eine sichere HTTPS-Verbindung mit TLS-

Transport-Verschlüsselung. Schließlich werden die Inhaltsdaten (Nachrichtentext, Dateinamen und Dateitypen) vom ADVOCOM-Server beim Ablegen in die Datenbank zusätzlich nochmal verschlüsselt. Dazu verwendet das System zertifikatbasierte, rotierende symmetrische Schlüssel der Onboard-Kryptographie.

Die Verwendung von ADVOCOM erfordert eine Authentifizierung am Anmeldedienst gemäß dem hochmodernen Open ID Connect Standard, basieren auf dem OAuth 2.0 Protokoll.

In ADVOCOM können Kommunikationen angehalten werden, womit eine gewisse Einschränkung der Verarbeitung möglich ist. Weiters können Kommunikationen gelöscht werden, wodurch diese unmittelbar und unwiderruflich beim Provider vernichtet werden. Weiters unterstützt ADVOCOM eine „Löschung bei Vergessen“, wodurch alle Daten gelöscht werden, wenn ein Benutzer für drei Jahr nicht aktiv war (keine Anmeldung).

Personen der Empfängerkategorien „Provider“ und „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.2.3 Synchronisation (Personen, Terminen und Aufgaben) und Scandienst

1.2.3.1 Kurzbeschreibung

Zur Steigerung der organisatorischen Effizienz werden Dienstprogramme eingesetzt. Diese tragen dazu bei, den manuellen Aufwand zu reduzieren, indem einfache Abläufe (teil-)automatisiert verrichtet werden. Es werden folgende Dienstprogramme eingesetzt:

Outlook- / Exchange-Synchronisation
Personen, Termine und Aufgaben werden durch ein Dienstprogramm mit Microsoft Outlook oder einem Microsoft Exchange Server synchron gehalten. Durch ein Zusammenwirken mit den Synchronisierungsfunktionen dieser Microsoft Programme wird so Synchronität von Personen, Terminen und Aufgaben auf allen Geräten und der Anwaltssoftware „ADVOKAT“ hergestellt.

Scandienst
Für bestimmte Scan-Anbieter ermöglicht ein Dienstprogramm ein direktes Scannen in den digitalen Akt hinein.

1.2.3.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die Steigerung der Effizienz bei Erfüllung der Zwecke anderer Verarbeitungsvorgänge, für welche dieser Verarbeitungsvorgang in dienender Funktion steht (insb. der Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“).

1.2.3.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	<u>Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO):</u> Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. <u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	Kanzleimitarbeiter/innen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit Bearbeitungen und Korrespondenzen zur jeweiligen Causa werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.2.3.4 <u>Kategorien der verarbeiteten Daten und Empfänger</u>

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein										
	2	Anschrift	Nein										
	3	Kontaktdaten (Tel., Mail, Fax)	Nein										
	4	Geburtsdatum	Nein										
	5	Spezifische Daten zu Terminen und Aufgaben (z.B. Datum, Uhrzeit, Bezeichnung)	Nein										
	6	Scandaten	Ja[1)]										
C	7	Namenskurzbezeichnung	Nein										

* Kategorie bP = Kategorie betroffener Personen

** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Diese Datenkategorien werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

1.2.3.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Keine	-	-

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.2.3.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Bei Verwendung des Scandienstes werden die Scandaten nur für einen kurzen Moment zwischengespeichert, um sodann in den digitalen Akt übernommen zu werden. Mit Übernahme in den Akt werden die zwischengespeicherten Daten gelöscht. Im Vergleich zu einer ausschließlich manuellen Verrichtung ist die Aufbewahrungsdauer der zwischengespeicherten Daten (Scanordner) kürzer.

Bei Verwendung der Outlook- / Exchange-Synchronisation erfolgt keine gesonderte Aufbewahrung von Daten, sondern nur ein Datenvergleich und erforderlichenfalls ein Datenaustausch.

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.2.3.7 Datenminimierung

Im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang erfolgt keine Datenerhebung. Zum Umfang der Verarbeitung wurde oberhalb ausgeführt (siehe dazu bei „Lösch- und Aufbewahrungsfristen“).

Die zu synchronisierenden Daten werden durch die/den jeweilige/n Mitarbeiter/in selbst definiert. In einer Arbeitsanweisung bzw. im Dienstvertrag ist festgehalten, dass nur jene Daten der Synchronisation unterworfen werden dürfen, welche für die Erfüllung konkreter Verarbeitungszwecke erforderlich sind.

Im Zusammenhang mit dem Scan-Dienst werden nur jene Daten verarbeitet, welche für die Erfüllung des Zweckes notwendig sind. Überhaupt werden die Daten unmittelbar in den digitalen Akt übernommen und sofort anschließend aus dem Scan-Ordner gelöscht.

1.2.3.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:

- Die Weitergabe von Daten erfolgt ausschließlich an Mitarbeiter/innen der Kanzlei.
- Die Verarbeitung im Zusammenhang mit dem Scan-Dienst erfolgt gänzlich innerhalb der Kanzleiräumlichkeiten.
- Die Übermittlung von Daten im Zusammenhang mit Synchronisierungsdiensten erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten. Durch Synchronisierungsdienste von Microsoft kann eine weitere Übertragung z.B. an Mobilgeräte erfolgen.
- Es werden nur jene Daten verarbeitet, welche zum aktuellen Zeitpunkt zur Erreichung konkreter Verarbeitungszwecke erforderlich sind.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (der Umfang der Verarbeitung wird ausschließlich manuell durch berechtigte Mitarbeiter festgelegt)
- Umfang der Verarbeitung: Niedriges Risiko (es erfolgt keine Offenlegung von Daten; durch Begrenzung der zu übertragenden Daten anhand des Zweckes ist der Umfang auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (die Festlegung der zu übertragenden Daten erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und nur durch die dazu berechtigte Person; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (es wird auf den Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“ verwiesen; die Dienste dienen einer effizienten Bearbeitung und sind allgemein anerkannt)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.2.3.9 Spezifische TOMs

Bei Verwendung von ADVOKAT Security: In der Anwaltssoftware „ADVOKAT“ kann die Synchronisation nur für einzelne Benutzer/innen freigeschalten werden.

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.2.4 Automatisierte Adressaktualisierung (z.B. durch ADVOKAT)

1.2.4.1 Kurzbeschreibung

Die Anwaltssoftware „ADVOKAT“ enthält ein Standard-Set ausgewählter Adressen, welche vom Softwarehersteller – ADVOKAT Unternehmensberatung Greiter & Greiter GmbH – laufend aktualisiert werden. Die Aktualisierung erfolgt durch Aufruf der entsprechenden Funktion.

Bei dem Standard-Set handelt es sich um öffentlich bekannte Adressen, welche für die rechtsanwaltliche Tätigkeit relevant sind. Diese sind Gerichte, Rechtsanwält/innen und Rechtsanwaltskanzleien, Notar/innen, Behörden, Kammern, Gläubigerschutzverbände und Versicherungen.

1.2.4.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die Steigerung der Effizienz bei Erfüllung der Zwecke anderer Verarbeitungsvorgänge, für welche dieser Verarbeitungsvorgang in dienender Funktion steht (insb. der Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“).

1.2.4.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Branchenrelevante Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Für die Ausübung rechtsanwaltlicher Tätigkeiten relevante Personen. Zu diesen zählen Gerichte, Rechtsanwält/innen und Rechtsanwaltskanzleien, Notar/innen, Behörden, Kammern, Gläubigerschutzverbände und Versicherungen.
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Die Verarbeitung der veröffentlichten Adress- und Kontaktdaten dieser Personenkategorie erfolgt, um Rechtsanwält/innen einerseits und die Personen dieser Kategorie andererseits in der Erfüllung Ihrer jeweiligen Aufgaben zu unterstützen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Das Erfüllen der Informationspflicht gegenüber allen betroffenen Personen wäre mit einem enormen Aufwand verbunden, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. b DSGVO nicht anzuwenden sind. Der Aufwand wird als unverhältnismäßig eingestuft, da die Daten, welche Gegenstand der Verarbeitung sind, von den jeweils betroffenen Personen veröffentlichte Daten sind und weil es sich dabei nicht um in irgendeiner Art schützenswerte Daten handelt, zumal die öffentliche Bekanntheit dieser Daten von den betroffenen Personen gewollt ist.

1.2.4.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
A	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein										
	2	Anschrift	Nein										
	3	Kontaktdaten (Tel., Mail, Fax)	Nein										
	4	Kontaktpersonen und deren Kontaktdaten	Nein										

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

1.2.4.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Keine	-	-

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.2.4.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt unbeschränkt für die Dauer der Ausübung rechtsanwaltlicher Tätigkeiten.

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.2.4.7 Datenminimierung

Es wird nur das Minimum an Daten verarbeitet, welches für die entsprechende Verwendung erforderlich ist (Name, Anschrift, Kontaktdaten).

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

1.2.4.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Keine

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Keine Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen
- Keine Weitergabe von Daten bei diesem Verarbeitungsvorgang
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:
- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (manuelle Ausführung der Adressaktualisierung)
- Umfang der Verarbeitung: Niedriges Risiko (keine Weitergabe von Daten; die Verarbeitung dient ausschließlich der Aktualisierung)
- Umstände der Verarbeitung: Niedriges Risiko (es werden ausschließlich von den betroffenen Personen öffentlich bekanntgemachte Daten verarbeitet; die Adressaktualisierung wird manuell und innerhalb der Kanzleiräumlichkeiten und durch qualifiziertes Kanzleipersonal vorgenommen; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)

- Zwecke der Verarbeitung: Niedriges Risiko (es wird auf den Verarbeitungsvorgang „Aktbearbeitung und Aktkorrespondenz“ verwiesen; die Adressaktualisierung dient einer effizienten Bearbeitung)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.2.4.9 Spezifische TOMs

Bei Verwendung von ADVOKAT Security: Die Funktion der Adressaktualisierung kann auf einzelne Benutzer/innen eingeschränkt werden.

Personen schützen

Bei Verwendung von ADVOKAT Security: Die Anwaltssoftware „ADVOKAT“ ermöglicht die Hinterlegung von berechtigten Benutzergruppen bei Personen im Adressbestand. Nur die auf solche Weise berechtigten Personen können überhaupt feststellen, dass es diese Person im System gibt. Für nicht Berechtigte gibt es die Person nicht.

Als besonderes Feature können Benutzer/innen eine Person ausnahmsweise doch sehen, wenn diese in einem Akt beteiligt ist, auf welchen die/der Benutzer/in zugreifen darf. Das ist nötig, damit Benutzer/innen den Akt, welchen diese (mit)bearbeiten, bearbeiten können. Sobald jedoch der Zugriff auf den Akt verloren geht (idealerweise bei Ablage des Aktes) entfällt damit auch der Zugriff auf die Person, sodass die Person, aus Sicht der Benutzerin / des Benutzers, aus dem System verschwindet.

Um die Erfüllung anderer Aufgaben und Pflichten (z.B. Auskunftsrecht) nicht zu gefährden, kann einzelnen Benutzer/innen das Recht eingeräumt werden, sämtliche Personen sehen zu dürfen. Dieses Recht ist sehr restriktiv handzuhaben.

1.2.5 Aktenupload (Internet-Akteneinsicht für Klient/innen)

1.2.5.1 Kurzbeschreibung

Um Klient/innen über den Verlauf einzelner oder aller Ihrer Causen informiert zu halten, werden definierte Akten samt definierten Inhalten auf einen Web-Server hochgeladen, womit die Einsichtnahme in hochgeladene Akten durch Befugte (Benutzerkennung und Kennwort) möglich ist. Die Zugangsdaten werden von der Kanzlei bestimmt und der befugten Person (den Klient/innen) mitgeteilt. Die Internet-Akteneinsicht ermöglicht ausschließlich einen lesenden Zugang.

1.2.5.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist das Informiert-Halten von Klient/innen über den Verlauf der sie betreffenden Causen, sowie die durch das Schaffen von Transparenz für Klient/innen erwirkte Möglichkeit zur aktiven Teilnahme an der Bearbeitung der Causen.

1.2.5.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebenden erhaltenen Aufträgen eröffneten Causen involviert sind, ausgenommen den Auftraggebenden. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	Gerichte und Behörden inkl. Kontaktpersonen bei diesen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der jeweiligen Causa befasste Gerichte (zuständige Zivil- und Strafgerichte) und Behörden (z.B. Finanzämter, Vermessungsämter, Grundverkehrsbehörden, Bezirkshauptmannschaften, Gemeinden, Kammern).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie D	Kanzleimitarbeiter/innen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit Bearbeitungen und Korrespondenzen zur jeweiligen Causa werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.2.5.4 Kategorien der verarbeiteten Daten und Empfänger

	Datenkategorien		Empfänger

				Auftraggeber[2]	Betreiber[3]	Ggf. IT-Support[4]							
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X	X							
	2	Anschrift	Nein	X	X	X							
	3	Kontaktdaten (Tel., Mail, Fax)	Nein	X	X	X							
	4	Geburtsdatum	Nein	X	X	X							
	5	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein	X	X	X							
	6	Firmenbuch- und Gewerbedaten	Nein	X	X	X							
	7	Grundbuchdaten	Nein	X	X	X							
	8	UID-, FB-, ZVR-Nummer	Nein	X	X	X							
	9	Sozialversicherungsdaten	Nein	X	X	X							
	10	Kontaktpersonen und deren Kontaktdaten	Nein	X	X	X							
	11	Beteiligte Personen (Aktbeteiligte Personen, Gerichte und Behörden)	Nein	X	X	X							
	12	Leistungsnachweise	Nein	X	X	X							
	13	Vertragstexte und Geschäftskorrespondenzen	Nein	X	X	X							
	14	Sachverhaltsdaten und Schriftsätze	Nein	X	X	X							
	15	Gerichtliche / Behördliche Erledigungen	Nein	X	X	X							
	16	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein	X	X	X							
	17	Ggf. Daten zu Bonität / Solvenz, Mahndaten	Nein	X	X	X							
	18	Ggf. Daten woraus die rassische/ethische Herkunft hervorgehen (Art. 9 DSGVO)	Ja[1]	X	X	X							
	19	Ggf. Daten woraus politische Meinungen hervorgehen (Art. 9 DSGVO)	Ja[1]	X	X	X							
	20	Ggf. Daten woraus religiöse/weltanschauliche Überzeugungen hervorgehen (Art. 9 DSGVO)	Ja[1]	X	X	X							
	21	Ggf. Daten woraus eine Gewerkschafts-zugehörigkeit hervorgeht (Art. 9 DSGVO)	Ja[1]	X	X	X							
	22	Ggf. genetische Daten (Art. 9 DSGVO)	Ja[1]	X	X	X							
	23	Ggf. biometrische Daten (Art. 9 DSGVO)	Ja[1]	X	X	X							
	24	Ggf. Gesundheitsdaten (Art. 9 DSGVO)	Ja[1]	X	X	X							
	25	Ggf. Daten zu Sexualleben / sexueller Orientierung (Art. 9 DSGVO)	Ja[1]	X	X	X							
	26	Ggf. strafrechtliche Daten (Art. 10 DSGVO)	Ja[1]	X	X	X							
C	27	Kontaktpersonen und deren Kontaktdaten	Nein	X	X	X							
D	28	Name	Nein	X	X	X							
	29	Funktion in der Kanzlei	Nein	X	X	X							
	30	Dienstliche Kontaktdaten	Nein	X	X	X							

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1] Diese Datenkategorien werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

[2)] Auftraggeber (entspricht der Personenkategorie A)

[3)] Betreiber: Das Online-Portal für die Internet-Akteneinsicht (*https://advokat.at/Akteneinsicht/*) ist eine von der Herstellerin der Anwaltssoftware „ADVOKAT“ – ADVOKAT Unternehmensberatung Greiter & Greiter GmbH – betriebene Website.

[4)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.2.5.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Auftraggeber	Nein	Nein
Betreiber	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.2.5.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Zurverfügungstellung von Aktendaten via Internet-Akteneinsicht erfolgt durch regelmäßige Uploads, wobei je Upload eine Bereinigung der am Web-Server liegenden Daten auf das Soll des jeweiligen Uploadvorgangs erfolgt. Durch Hinterlegung einer Erledigungsschwelle (das ist jene Dauer, für welche Akten nach deren Erledigung noch via Internet-Akteneinsicht zugänglich sein sollen), werden Akten und sämtliche damit verbundenen Daten kurz nach der Erledigung des jeweiligen Aktes vollständig vom Web-Server gelöscht.

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.2.5.7 Datenminimierung

Im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang erfolgt keine Datenerhebung. Der Umfang der Verarbeitung wird detailliert und individuell je Klient festgelegt. Weiters erfolgt eine laufende Bereinigung der Daten am Web-Server (siehe dazu bei „Lösch- und Aufbewahrungsfristen“).

Bei Verwendung von ADVOKAT Security: Das Konfigurieren und Durchführen von Uploads ist durch Rechte auf eine bzw. wenige Personen beschränkt.

Die Protokollierung von Uploads und Zugriffen ermöglicht die Nachvollziehbarkeit aller Verarbeitungsvorgänge inkl. getätigter Einsichtnahmen.

Mitarbeiter/innen der Kanzlei haben keinen Zugang zu den auf den Web-Server hochgeladenen Inhalten.

1.2.5.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen

- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen
- Zugang via Internet

Für ein niedriges Risiko sprechen folgende Faktoren:
- Die Weitergabe von Daten erfolgt ausschließlich an den jeweiligen Auftraggeber.
- Die Übermittlung von Daten im Zusammenhang mit der Internet-Akteneinsicht erfolgt ausschließlich über einen verschlüsselten Kommunikationstunnel (HTTPS). Die Web-Server werden von der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH (staatlich konzessionierte Übermittlungs- und Verrechnungsstelle) betrieben und befinden sich ausschließlich in Österreich. Sie sind in modernsten, hochsicheren Datenzentren untergebracht. Die Authentisierung und Authentifizierung erfolgt via Benutzerkennung und Kennwort.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (sichere HTTPS-Kommunikation; sicheres Authentisierungs- und Authentifizierungsverfahren mit Benutzerkennung und Kennwort)
- Art der Verarbeitung: Niedriges Risiko (der Umfang der Verarbeitung wird ausschließlich manuell durch berechtigte Mitarbeiter festgelegt)
- Umfang der Verarbeitung: Niedriges Risiko (Offenlegung erfolgt nur gegenüber dem Auftraggeber; die Bereitstellung erfolgt auf Wunsch des Klient/innen und nur im gewünschten Umfang samt laufender Datenbereinigung, womit dieser auf das Notwendige reduziert ist)
- Umstände der Verarbeitung: Niedriges Risiko (Uploads erfolgen ausschließlich innerhalb der Kanzleiräumlichkeiten und werden durch qualifiziertes Personal definiert und veranlasst; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (der Zweck dient insbesondere dem datenschutzrechtlichen Transparenzgrundsatz – es sei auf Erwägungsgrund 63 DSGVO „Fernzugang für betroffene Person“ verwiesen –, sodass er als legitim betrachtet werden kann)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.2.5.9 Spezifische TOMs

Alle Uploads und sämtliche Zugriffe werden protokolliert.

Jeder einzelne Upload beinhaltet eine automatische Bereinigung von Daten am Web-Server, womit die Daten immer auf das Minimum reduziert sind (siehe dazu bei „Lösch- und Aufbewahrungsfristen“).

Zugänge zur Internet-Akteneinsicht werden individuell je Auftraggebendem festgelegt und ausschließlich diesen mitgeteilt.

Bei Verwendung von Security: Der Zugang zum Verwaltungsprogramm in der Anwaltssoftware „ADVOKAT“ kann auf einzelne Mitarbeiter/innen beschränkt werden.

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

1.3 Kanzleiverwaltung, Rechnungswesen, Zahlungsverkehr

1.3.1 Fakturierung, Zahlungsverkehr, Buchhaltung

1.3.1.1 Kurzbeschreibung

In Verbindung mit der rechtsanwaltlichen Tätigkeit werden erbrachte Leistungen gegenüber Klient/innen abgerechnet, Anzahlungen (Akonti) angefordert, Honorar- bzw. Akontozahlungen erfasst und zugewiesen, Fremdgeldzahlungen abgewickelt und Zahlungsausgänge durchgeführt (inkl. Electronic Banking).

Weiters wird gemäß den gesetzlichen Anforderungen Buch geführt (Buchhaltung, Registrierkasse) und es werden die verpflichtenden Meldungen erstattet (Treuhand, UVA, ZM). In diesem Zusammenhang werden Daten auch von einer dazu beauftragten Steuerberatungskanzlei verarbeitet.

1.3.1.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die Abrechnung erbrachter Leistungen samt dem Einbringen der verrechneten Beträge sowie die Abwicklung von Zahlungseingängen und -ausgängen (inkl. Fremdgelder).

Weiterer Zweck ist die Erfüllung der gesetzlichen Anforderungen betreffend die Führung von Büchern, deren Aufbewahrung und die Erstattung diverser Meldungen (Treuhand, UVA, ZM).

1.3.1.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei im Sinne des bei „Aktbearbeitung und Aktkorrespondenz“ genannten Verarbeitungszwecks beauftragen. Es kann je Causa einen oder mehrere Auftraggebende geben.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Rechtspflicht (Art. 6 Abs. 1 lit. c DSGVO):** Mandatsvertrag bzw. Auftrag Rechnungslegung gemäß § 11 UstG
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung. Bei Verwendung der ADVOKAT Internet-Akteneinsicht haben Auftraggebende 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).

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund des vom Auftraggebers erhaltenen Auftrages eröffnete Causa und in deren Fakturierung und/oder Zahlungsverkehr involviert sind, ausgenommen dem Auftraggeber. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner), Versicherungen, gesetzliche Vertreter und beauftragte Dritte (z.B. Notare, Sachverständige).
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese Personenkategorie	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO): Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	Kanzleimitarbeiter/innen
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der Fakturierung und Zahlungsabwicklung zur jeweiligen Causa werden auch Daten von Mitarbeiter/innen der Kanzlei (Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc.) verarbeitet. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO) / Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** Dienst- bzw. Werkvertrag. Kanzleimitarbeiter/innen haben ein Interesse am geschäftlichen Erfolg der Kanzlei (*„Geht es der Kanzlei gut, geht es den Mitarbeiter/innen gut."*)
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

1.3.1.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
				Ggf. IT-Support[1)]	Banken[2)]	Steuerberatung[3)]							
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X	X	X							
	2	Anschrift	Nein	X									
	3	Kontaktdaten (Tel., Mail, Fax)	Nein	X									
	4	Bank- und Überweisungsdaten	Nein	X	X								
	5	Kontaktpersonen und deren Kontaktdaten	Nein	X									
	6	Leistungsnachweise	Nein	X									
	7	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein	X		X							
C	8	Name	Nein	X		X							
	9	Funktion in der Kanzlei	Nein	X		X							
	10	Dienstliche Kontaktdaten	Nein	X		X							

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

[2)] Banken: Durchführende Banken

[3)] Steuerberatung: Beauftragte Steuerberatungskanzlei
Zur Erstellung von Jahresabschlüssen erfolgt die Übermittlung von Buchhaltungsdaten (Saldenlisten, Kontoauszüge) an die Steuerberatung.

1.3.1.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Ggf. IT-Support	Nein	Nein
Banken	Nein	Nein
Steuerberatung	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.3.1.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung erfolgt in Erfüllung der rechtsanwaltlichen Aufbewahrungspflichten gemäß § 12 RAO für die Dauer von fünf Jahren ab Abschluss der jeweiligen Causa und umfasst sämtliche Datenkategorien. Der Abschluss wird durch Vergabe eines Ablagedatums je Akt dokumentiert, wodurch ein systemisches Bereinigen (Löschen von alten Akten) möglich ist. Soweit es zur Erfüllung von abgabenrechtlichen Aufbewahrungspflichten erforderlich ist, erfolgt eine Aufbewahrung für die gesetzlich vorgeschriebene Dauer von in der Regel sieben Jahren ab Schluss des Kalenderjahres in welchem das Wirtschaftsjahr endet (§ 132 Abs. 1 BAO).

Soweit es zur Abwehr etwaiger Schadenersatzansprüche erforderlich ist, werden die Daten eines Aktes und der involvierten Personen für die Dauer von 30 Jahren (lange Verjährungsfrist) ab Abschluss der jeweiligen Causa aufbewahrt.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT“ Möglichkeiten, welche den Schutz der Daten, die über den Abschluss einer Causa hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs“).

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.3.1.7 Datenminimierung

Nicht nur zur Sicherung eines hohen Datenschutzniveaus, sondern auch für eine schlanke und effiziente Kanzleiverwaltung werden ausschließlich Daten erfasst, welche für die Bearbeitung der jeweiligen Causa und den zusammenhängenden Verarbeitungsvorgängen, und damit zur Erfüllung der Zwecke dieser Verarbeitungsvorgänge, erforderlich oder zumindest zweckdienlich sind.

Das Erfassen von Daten erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Datenerfassung fördert den Grundsatz der Datenminimierung, zumal das Erfassen jedes einzelnen Datums mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Die genannten Gründe gelten entsprechend auch für den Umfang der Verarbeitung. Im Zusammenhang mit diesem Verarbeitungsvorgang werden keine Daten erhoben.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu den in Akten gespeicherten Daten (insb. Honorarnoten, Zahlungen) haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT“ (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bieten ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung sowie für einschlägige Programmbereiche wie z.B. zur Erstellung von Honorarnoten, zum Erfassen von Fremdgeldbewegungen, zum Erstellen von Überweisungen) und die Verwendung von Microsoft SharePoint (Dokumentenmanagementsystem mit Anbindung an ADVOKAT-Security z.B. zur manipulationssicheren Aufbewahrung von Honorarnoten) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

Der Zugang zur Buchhaltung sowie jener zur Registrierkasse ist durch ein Kennwort gesichert und so nur für dafür zuständige Mitarbeiter/innen zugänglich.

1.3.1.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:

- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:

- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Keine automatisierte Verarbeitung von Daten (z.B. keine automatisierte Rechnungslegung)
- Verarbeitung erfolgt aufgrund gesetzlicher Verpflichtung
- Verarbeitung aller Daten erfolgt nur innerhalb des Kanzleinetzwerks
- Keine Offenlegung von personenbezogenen Daten (ausgenommen durchführende Banken und im Ausnahmefall IT-Support)
- Verarbeitung erfolgt vor allem zur Erfüllung gesetzlicher Pflichten (Rechnungslegung, Buchführung)
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (Übermittlung von Daten ausschließlich an die jeweils betroffene Person; aufgrund ausschließlich manueller Verarbeitung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (die Verarbeitung erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und damit durch qualifiziertes Kanzleipersonal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation; die Kanzlei ist zu dieser Verarbeitung gesetzlich verpflichtet)
- Zwecke der Verarbeitung: Niedriges Risiko (die Verarbeitungszwecke sind gesetzlich legitimiert und inhärenter Teil jeder Unternehmung)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.3.1.9 Spezifische TOMs

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

Bei Verwendung von ADVOKAT Security: Das Berechtigungssystem der Anwaltssoftware „ADVOKAT“ ermöglicht die Verwaltung von Rechten für Benutzer/innen und -gruppen betreffend einzelne Akten, Aktengruppen und einzelne Programmbereiche. Dieses Berechtigungssystem stellt sicher, dass nur jene Kanzleimitarbeiter/innen Zugang zu Daten eines Aktes und zu, für diesen Verarbeitungsvorgang, einschlägigen Programmbereichen und -funktionen haben, welche diesen auch tatsächlich für die Erfüllung der Verarbeitungszwecke benötigen.

Bei Verwendung von Microsoft SharePoint: Das mit der Anwaltssoftware „ADVOKAT“ verbundene Berechtigungssystem stellt sicher, dass Dokumente (insb. Honorarnoten) nur für jene Kanzleimitarbeiter/innen zugänglich sind, welche den Zugang für die Erfüllung der Verarbeitungszwecke benötigen. Die Versionierung von Dokumenten schafft zusätzlich einen Manipulationsschutz für alle Dokumente. Je nach Ausführungsvariante von Microsoft SharePoint stehen weitere Sicherheitsfunktionen zur Verfügung.

1.3.2 Personal- und Benutzerverwaltung (Bewerbungs- und Mitarbeiterunterlagen, Benutzer- und Rechteverwaltung)

1.3.2.1 Kurzbeschreibung

Im Zusammenhang mit der Personalsuche, der Rekrutierung und der Personalverwaltung werden diverse personenbezogenen Daten verarbeitet. Für Mitarbeiter/innen werden Benutzer/innen und Zugangsberechtigungen für verschiedene Systeme festgelegt, installiert und administriert (z.B. Windows, ADVOKAT, SQL Server, SharePoint Server).

1.3.2.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die mit dem Arbeitsrecht konforme und verpflichtende Verarbeitung und Aufbewahrung von Daten, sowie die Suche nach und Anstellung von neuen Mitarbeiter/innen.

1.3.2.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Kanzleimitarbeiter/innen**
Anmerkungen zur Personenkategorie	Mitarbeiter/innen der Kanzlei sind Rechtsanwält/innen, Konzipient/innen, juristische Mitarbeiter/innen, Sekretariat, etc. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Dienst- bzw. Werkvertrag.
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

Kategorie B	**Bewerber/innen**
Anmerkungen zur Personenkategorie	Alle Personen, welche sich für die Anstellung in der Kanzlei bewerben.
Rechtsgrundlage für diese Personenkategorie	**Vorvertragliche Maßnahme (Art. 6 Abs. 1 lit. b DSGVO):** Auf Initiative der sich bewerbenden Person (Zusendung einer Bewerbung) werden personenbezogen Daten mit der beiderseitigen Absicht verarbeitet, ein neues Dienstverhältnis zu begründen (Dienst- bzw. Werkvertrag).
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt mittels Datenschutzmitteilung.

1.3.2.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger										
				Steuerberatung[1)]	Sozialversich.[2)]	Ggf. IT-Support[3)]								
A	1	Name	Nein	X	X	X								
	2	Foto	Nein			X								
	3	Anschrift	Nein	X		X								
	4	Kontaktdaten (Tel., Mail, Fax)	Nein	X		X								
	5	Bank- und Überweisungsdaten	Nein	X		X								
	6	Geburtsdatum	Nein	X	X	X								
	7	Sozialversicherungsdaten	Nein	X	X	X								
	8	Personalunterlagen (Dienst- bzw. Werkvertrag, Gehaltsabrechnungen, Dienstzeugnisse)	Nein	X		X								
B	9	Name	Nein			X								
	10	Foto	Nein			X								
	11	Anschrift	Nein			X								
	12	Kontaktdaten (Tel., Mail, Fax)	Nein			X								
	13	Geburtsdatum	Nein			X								
	14	Bewerbungsunterlagen	Nein			X								

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Steuerberatung: Beauftragte Steuerberatungskanzlei
Zur Lohnverrechnung und für die Anmeldung zur Sozialversicherung erfolgt die Übermittlung der erforderlichen Unterlagen an die Steuerberatung.

[2)] Sozialversich.: Hauptverband der Österreichischen Sozialversicherungsträger
Im Zusammenhang mit der Einstellung von Mitarbeiter/innen muss eine Anmeldung erfolgen.

[3)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.3.2.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Steuerberatung	Nein	Nein
Sozialversich.	Nein	Nein
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.3.2.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Die Aufbewahrung von Bewerbungsdaten erfolgt bis zur erfolgreichen Besetzung der ausgeschriebenen Stelle (inkl. Ablauf einer allfälligen Probezeit). Im Einzelfall kann, nach Zustimmung der Bewerberin / des Bewerbers, eine längere Aufbewahrung für eine mögliche spätere Anstellung erfolgen.

Die Aufbewahrung von Personaldaten erfolgt für die Dauer von 30 Jahren ab Beendigung des Dienstverhältnisses. Grund dafür ist die Erfüllung gesetzlicher Verpflichtungen wie z.B. der Ausstellung von Dienstzeugnissen. Auch die Abwehr etwaiger Schadenersatzansprüche kann ein Grund für eine längere Aufbewahrung sein.

Als kompensatorische Maßnahme bietet die Anwaltssoftware „ADVOKAT“ Möglichkeiten, welche den Schutz der Daten, die über die Beendigung eines Dienstverhältnisses hinaus aufbewahrt werden, zu verstärken (z.B. virtueller versperrter Aktenschrank bei Verwaltung von Personaldaten in Form von Personalakten, Personen schützen). Siehe hierzu bei diesem Verarbeitungsvorgang unter „Spezifische TOMs“).

Das Sperren der Verarbeitung wird durch Hinterlegung in der Anwaltssoftware „ADVOKAT“ sichergestellt. Eine Warnfunktion stellt sicher, dass bei jedem Zugriff auf die Verarbeitungssperre hingewiesen wird.

1.3.2.7 Datenminimierung

Nicht nur zur Sicherung eines hohen Datenschutzniveaus, sondern auch für eine schlanke und effiziente Kanzleiverwaltung werden ausschließlich Daten erfasst, welche für die Personalauswahl und -verwaltung, und damit zur Erfüllung des Zweckes dieses Verarbeitungsvorgangs, erforderlich oder zumindest zweckdienlich sind.

Das Erfassen von Daten erfolgt ausschließlich manuell durch Kanzleipersonal. Das Fehlen einer automatisierten Datenerfassung fördert den Grundsatz der Datenminimierung, zumal das Erfassen jedes einzelnen Datums mit Arbeitszeit und damit auch mit Kosten verbunden ist.

Die genannten Gründe gelten entsprechend auch für den Umfang der Verarbeitung.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten. Auch wird darauf hingewiesen, dass sämtliche Daten nur zur Erfüllung der Zwecke, für die sie erhoben wurden, verarbeitet werden dürfen.

Zugang zu den in Akten (z.B. Personalakten) gespeicherten Daten haben nur jene Mitarbeiter/innen der Kanzlei, welche diesen benötigen, um den Zweck der Verarbeitung erfüllen zu können. Dies wird durch ein etabliertes Windows-Berechtigungssystem (Gesicherter Zugang zu Rechnern) und durch gesicherte Anmeldung in der Anwaltssoftware „ADVOKAT“ (Kennwortanmeldung oder Windows-Authentifizierung) sichergestellt. Bedarfsweise bieten ADVOKAT-Security (Berechtigungssystem der Software ADVOKAT zur akt- und aktgruppenweisen Rechteverwaltung) und die Verwendung von Microsoft SharePoint (Dokumentenmanagementsystem mit Anbindung an ADVOKAT-Security) zusätzliche Sicherheit durch eine Verfeinerung der effektiven Zugangsberechtigungen.

1.3.2.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Keine

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Keine Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen
- Keine automatisierte Verarbeitung von Daten
- Die Verarbeitung aller Daten erfolgt nur innerhalb des Kanzleinetzwerks
- Die Weitergabe von Daten erfolgt ausschließlich an sehr vertrauenswürdige Empfänger (Steuerberatungskanzlei, Hauptverband der österr. Sozialversicherungsträger), welche ihrerseits

ein hohes Schutzniveau bieten, zumal diese selbst ein Interesse an einem hohen Schutzniveau haben.
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:

- Verwendung neuer Technologien: Niedriges Risiko (klassische Desktop-Anwendung; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (nur sehr wenige Datenübermittlungen an einen geschlossenen Empfängerkreis; aufgrund ausschließlich manueller Verarbeitung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (Rekrutierung und Personalverwaltung erfolgt ausschließlich innerhalb der Kanzleiräumlichkeiten und durch qualifiziertes Kanzleipersonal; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (die Verarbeitungszwecke sind natürlicher Bestandteil jeder Unternehmung; diese sind legitim und klar abgegrenzt)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.3.2.9 Spezifische TOMs

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.

Bei Verwendung von ADVOKAT Security: Das Berechtigungssystem der Anwaltssoftware „ADVOKAT“ ermöglicht die Verwaltung von Rechten für Benutzer/innen und -gruppen betreffend einzelne Akten (z.B. Mitarbeiterakt), Aktengruppen (z.B. Personalakten) und einzelne Programmbereiche. Dieses Berechtigungssystem stellt sicher, dass nur jene Kanzleimitarbeiter/innen Zugang zu Personaldaten (Bewerber/innen und Mitarbeiter/innen) haben, welche diesen auch tatsächlich für die Erfüllung der Verarbeitungszwecke benötigen.

Bei Verwendung von Microsoft SharePoint: Das mit der Anwaltssoftware „ADVOKAT“ verbundene Berechtigungssystem stellt sicher, dass Dokumente und andere Dateien nur für jene Kanzleimitarbeiter/innen zugänglich sind, welche den Zugang für die Erfüllung der Verarbeitungszwecke benötigen. Die Versionierung von Dokumenten schafft zusätzlich einen Manipulationsschutz für alle Dokumente. Je nach Ausführungsvariante von Microsoft SharePoint stehen weitere Sicherheitsfunktionen zur Verfügung.

Virtueller versperrter Aktenschrank

Bei Verwendung von ADVOKAT Security: Bei Verwaltung von Personaldaten in Akten können diese, durch Ablegen von Personalakten in der Anwaltssoftware „ADVOKAT“ (z.B. bei Aufbewahrung von Daten nach Beendigung eines Dienstverhältnisses), automatisch in einen virtuellen versperrten Aktenschrank (durch Anlage einer dafür vorgesehenen Aktengruppe) gelegt werden, zu welchem nur definierte Personen Zugang haben (z.B. zuständige/r Partner/in, Abteilungsleiter/in). Zusätzlich kann

die Bearbeitung auch für diese definierte(n) Person(en) durch Setzen entsprechender Rechte gesperrt werden.

Personen schützen

Bei Verwendung von ADVOKAT Security: Die Anwaltssoftware „ADVOKAT“ ermöglicht die Hinterlegung von berechtigten Benutzergruppen bei Personen im Adressbestand. Nur die auf solche Weise berechtigten Personen können überhaupt feststellen, dass es diese Person im System gibt. Für nicht Berechtigte gibt es die Person nicht.

Um die Erfüllung anderer Aufgaben und Pflichten (z.B. Auskunftsrecht) nicht zu gefährden, kann einzelnen Benutzer/innen das Recht eingeräumt werden, sämtliche Personen sehen zu dürfen. Dieses Recht ist sehr restriktiv handzuhaben.

1.3.3 Systemadministration, EDV-Betreuung, Software-Support

1.3.3.1 Kurzbeschreibung

Für die Herstellung, Wartung und laufende Betreuung der IT-Infrastruktur werden Professionist/innen in Anspruch genommen (EDV-Betreuung, Software Support). Bei diesen Arbeiten werden unter Umständen personenbezogene Daten einsichtig (z.B. Support via Fernwartung) und/oder verarbeitet (z.B. Serverwechsel).

1.3.3.2 Zweck(e) der Verarbeitung

Zweck dieses Verarbeitungsvorgangs ist die Herstellung und Erhaltung einer modernen und sicheren IT-Infrastruktur zur Verrichtung der mit dem Betrieb einer Rechtsanwaltskanzlei einhergehenden Tätigkeiten.

1.3.3.3 Kategorien betroffener Personen, Rechtsgrundlagen, Informationspflichten

Kategorie A	**Auftraggebende (Klient/innen) inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Personen, welche die Kanzlei bzw. Rechtsanwält/innen der Kanzlei beauftragen.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Mandatsvertrag bzw. Auftrag
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt bei Beauftragung mittels Datenschutzmitteilung.

Kategorie B	**Aktbeteiligte Personen inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Alle Personen, welche in die aufgrund der von Auftraggebern erhaltenen Aufträge eröffneten Causen involviert sind, ausgenommen der Auftraggeber. Zu diesen gehören insbesondere Parteien (Beklagte, Vertragspartner/innen, Nebenintervenient/innen, Privatankläger/innen, etc.), Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen und Sachverständige
Rechtsgrundlage für diese Personenkategorie	**Berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO):** • Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insb. Causen des Straf-, Zivil-, Außerstreit- und Insolvenzrechts, des Arbeits- und Unternehmensrechts sowie des Verwaltungs- und Verfassungsrechts) • Errichtung, Prüfung, Verhandlung oder Abwicklung von Verträgen und Geschäften (z.B. Bauträgerprojekte, M&A, Unternehmensgründungen, Bestandsverträge, Finanzierungen) • Geschäfts- oder Vertretungsverhältnis mit einer anderen aktbeteiligten Person (Versicherungen, gesetzliche Vertreter/innen, Rechtsanwält/innen, Notar/innen)
Erfüllung der Informations-pflichten für diese	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO): Erfolgt bei Datenerhebung mittels Datenschutzmitteilung.

Personenkategorie	<u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird ein Datenschutzmitteilung übersendet.

Kategorie C	**Alle im System vorhandenen Personen**
Anmerkungen zur Personenkategorie	Alle Personen, welche im Adressbestand des Systems vorhanden sind.
Rechtsgrundlage für diese Personenkategorie	**Rechtliche Verpflichtung (von Rechtsanwält/innen) der Kanzlei (Art. 6 Abs. 1 lit. c DSGVO):** Um das Doppelvertretungsverbot (§ 9 Abs. 1 und § 10 Abs. 1 RAO, §§ 10 und 12a RL-BA) zu achten und zu wahren, ist für alle potentiellen Klient/innen und Gegner/innen einer Causa eine mögliche Interessenkollision zu prüfen. Dies erfolgt durch Abgleich mit den im System (aus früheren Causen) vorhanden Personen.
Erfüllung der Informations-pflichten für diese Personenkategorie	<u>Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DSGVO):</u> Erfolgt bei Datenerhebung mittels Datenschutzmitteilung. <u>Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO):</u> Diese Daten unterliegen in der Regel 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 (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. d DSGVO nicht anzuwenden sind. Im Ausnahmefall wird eine Datenschutzmitteilung übersendet.

Kategorie D	**Gerichte und Behörden inkl. Kontaktpersonen bei diesen**
Anmerkungen zur Personenkategorie	Im Zusammenhang mit der jeweiligen Causa befasste Gerichte (zuständige Zivil- und Strafgerichte) und Behörden (z.B. Finanzämter, Vermessungsämter, Grundverkehrsbehörden, Bezirkshauptmannschaften, Gemeinden, Kammern).
Rechtsgrundlage für diese Personenkategorie	**Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe (Art. 6 Abs. 1 lit. e DSGVO):** Die Gesetzgebung hat Strukturen und Systeme vorgegeben, denen sich die/der Rechtsanwender/in bedienen soll und muss. Die Verwendung dieser ist daher im öffentlichen Interesse gelegen.
Erfüllung der Informations-pflichten für diese Personenkategorie	Gerichte und Behörden sind in jedem Fall keine natürlichen Personen, sodass es für diese keine Informationspflichten gibt (keine personenbezogenen Daten gem. Art. 4 Z. 1 DSGVO). Die Kontaktpersonen (Richter/innen, Rechtspfleger/innen, Sachbearbeiter/innen) sind jedoch natürliche Personen. Die Erhebung von personenbezogenen Daten zu diesen Kontaktpersonen erfolgt bei den Gerichten und Behörden im Zusammenhang mit der Anwendung der gesetzlich vorgegebenen Strukturen und Systeme, d.h., dass die Erlangung durch nationale oder EU-Rechtsvorschriften ausdrücklich geregelt ist, weshalb die Bestimmungen zur Informationspflicht (Art. 14 Abs. 1-4 DSGVO) gem. Art. 14 Abs. 5 lit. c DSGVO nicht anzuwenden sind.

Kategorie E	**Kanzleimitarbeiter/innen**
Anmerkungen zur Personenkategorie	Mitarbeiter der Kanzlei sind Rechtsanwält/innen, Konzipienten, juristische Mitarbeiter, Sekretariat, etc. Auch dienstnehmerähnliche Personen (z.B. beauftragte Jurist/innen) zählen zu dieser Personenkategorie.
Rechtsgrundlage für diese Personenkategorie	**Vertragserfüllung (Art. 6 Abs. 1 lit. b DSGVO):** Dienst- bzw. Werkvertrag.
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt im Dienstvertrag, Werkvertrag bzw. in der Datenschutzvereinbarung.

Kategorie F	**Bewerber/innen**
Anmerkungen zur Personenkategorie	Alle Personen, welche sich für die Anstellung in der Kanzlei bewerben.
Rechtsgrundlage für diese	**Vorvertragliche Maßnahme (Art. 6 Abs. 1 lit. b DSGVO):** Auf Initiative der Bewerberin / des Bewerbers (Zusendung einer Bewerbung) werden

Personenkategorie	personenbezogen Daten mit der beiderseitigen Absicht verarbeitet, ein neues Dienstverhältnis zu begründen (Dienst- bzw. Werkvertrag).
Erfüllung der Informations-pflichten für diese Personenkategorie	Erfolgt mittels Datenschutzmitteilung.

1.3.3.4 Kategorien der verarbeiteten Daten und Empfänger

Kategorie bP*	Lfd. Nr.	Datenkategorien	Sensible Daten**	Empfänger									
				Ggf. IT-Support[2)]									
A B	1	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X									
	2	Foto	Nein	X									
	3	Anschrift	Nein	X									
	4	Kontaktdaten (Tel., Mail, Fax)	Nein	X									
	5	Bank- und Überweisungsdaten	Nein	X									
	6	Geburtsdatum	Nein	X									
	7	Datum von Tod, Insolvenzeröffnung, Entziehung oder Einschränkung der Rechte (Sachwaltung)	Nein	X									
	8	Firmenbuch- und Gewerbedaten	Nein	X									
	9	Grundbuchdaten	Nein	X									
	10	UID-, FB-, ZVR-Nummer	Nein	X									
	11	Sozialversicherungsdaten	Nein	X									
	12	Kontaktpersonen und deren Kontaktdaten	Nein	X									
	13	Beteiligte Personen (Aktbeteiligte Personen, Gerichte und Behörden)	Nein	X									
	14	Leistungsnachweise	Nein	X									
	15	Vertragstexte und Geschäftskorrespondenzen	Nein	X									
	16	Sachverhaltsdaten und Schriftsätze	Nein	X									
	17	Gerichtliche / Behördliche Erledigungen	Nein	X									
	18	Abrechnungs-, Zahlungs- und Buchungsdaten	Nein	X									
	19	Ggf. Daten zu Bonität / Solvenz, Mahndaten	Nein	X									
	20	Ggf. Daten woraus die rassische/ethische Herkunft hervorgehen (Art. 9 DSGVO)	Ja[1)]	X									
	21	Ggf. Daten woraus politische Meinungen hervorgehen (Art. 9 DSGVO)	Ja[1)]	X									
	22	Ggf. Daten woraus religiöse/weltanschauliche Überzeugungen hervorgehen (Art. 9 DSGVO)	Ja[1)]	X									
	23	Ggf. Daten woraus eine Gewerkschafts-zugehörigkeit hervorgeht (Art. 9 DSGVO)	Ja[1)]	X									
	24	Ggf. genetische Daten (Art. 9 DSGVO)	Ja[1)]	X									
	25	Ggf. biometrische Daten (Art. 9 DSGVO)	Ja[1)]	X									
	26	Ggf. Gesundheitsdaten (Art. 9 DSGVO)	Ja[1)]	X									
	27	Ggf. Daten zu Sexualleben / sexueller Orientierung (Art. 9 DSGVO)	Ja[1)]	X									

	28	Ggf. strafrechtliche Daten (Art. 10 DSGVO)	Ja[1)]	X										
C	14	Name, Firma oder sonstige geschäftsmäßige Bezeichnung	Nein	X										
	15	Anschrift	Nein	X										
	16	Kontaktdaten	Nein	X										
	17	Geburtsdatum	Nein	X										
	18	UID, FB-, ZVR-Nummer	Nein	X										
	19	Sozialversicherungsdaten	Nein	X										
D	29	Kontaktpersonen und deren Kontaktdaten	Nein	X										
E	1	Name	Nein	X										
	2	Foto	Nein	X										
	3	Anschrift	Nein	X										
	4	Kontaktdaten (Tel., Mail, Fax)	Nein	X										
	5	Bank- und Überweisungsdaten	Nein	X										
	6	Geburtsdatum	Nein	X										
	7	Sozialversicherungsdaten	Nein	X										
	8	Personalunterlagen (Dienst- bzw. Werkvertrag, Gehaltsabrechnungen, Dienstzeugnisse)	Nein	X										
F	9	Name	Nein	X										
	10	Foto	Nein	X										
	11	Anschrift	Nein	X										
	12	Kontaktdaten (Tel., Mail, Fax)	Nein	X										
	13	Geburtsdatum	Nein	X										
	14	Bewerbungsunterlagen	Nein	X										

* Kategorie bP = Kategorie betroffener Personen
** Sensible Daten = Besondere Datenkategorien iSd. Art. 9 DSGVO, strafrechtlich relevant iSd. Art 10 DSGVO

[1)] Diese Datenkategorien werden verarbeitet, wenn dies für die Bearbeitung der jeweiligen Causa erforderlich ist (z.B. Gesundheitsdaten im Zusammenhang mit einer Verkehrsunfall-Causa oder strafrechtliche Daten im Zusammenhang mit einer Strafverteidigungs-Causa).

[2)] Ggf. IT-Support: Die Instandhaltung und Wartung von IT-Systemen (Hardware und Software) erfolgt durch dafür beauftragte Unternehmer/innen (EDV-Betreuer/in, Softwarehersteller/in)

1.3.3.5 Kategorien von Empfängern (inkl. Auftragsverarbeitung, Übermittlung an Drittland)

Empfängerkategorien	Drittstaaten*	Int. Organisation**
Ggf. IT-Support	Nein	Nein

* Drittstaaten: Angabe des Drittstaats / der Drittstaaten (= Staaten außerhalb der EU); Nein = Keine Übermittlung an Drittstaaten
** Int. Organisation: Angabe der internationalen Organisation(en); Nein = Keine Übermittlung an internationale Organisationen

Garantien für die Übermittlung an Drittstaaten / internationale Organisationen:

Keine Übermittlung an Drittstaaten oder internationale Organisationen.

1.3.3.6 Lösch- und Aufbewahrungsfristen (Speicherbegrenzung), Verarbeitungssperren

Im Zusammenhang mit diesem Verarbeitungsvorgang werden keine personenbezogenen Daten erhoben, sondern werden solche nur einsichtig bzw. verarbeitet (z.B. Kopieren auf einen neu angeschafften Server), sodass es auch keine eigenständige Aufbewahrung bei diesem Verarbeitungsvorgang gibt.

1.3.3.7 Datenminimierung

Die Inanspruchnahme von IT-Dienstleistungen im Bereich EDV-Betreuung und Support erfolgt nach Bedarf (z.B. bei Bestehen von Problemen oder bei veränderten Anforderungen an Systeme) und ist in der Regel mit Zeitaufwand und/oder Kosten verbunden, sodass Verarbeitungen nur im notwendigen bzw. zweckmäßigen Umfang erfolgen.

Im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag werden alle Mitarbeiter/innen darauf hingewiesen, dass ausschließlich zweckdienliche Daten erfasst werden sollen, um nur das Minimum an personenbezogenen Daten zu verarbeiten.

1.3.3.8 Risikobewertung

Nachfolgend wird das Risiko für die Rechte und Freiheiten natürlicher Personen bei Verarbeitung von Daten im Zusammenhang mit dem gegenständlichen Verarbeitungsvorgang bewertet.

Für ein hohes Risiko sprechen folgende Faktoren:
- Teilweise Verarbeitung sensibler Daten gemäß Art. 9 und 10 DSGVO
- Verarbeitung geheimer Daten im Sinne der aktbeteiligten Personen
- Verarbeitung von Daten, welche der rechtsanwaltlichen Verschwiegenheitspflicht gem. § 9 RAO unterliegen

Für ein niedriges Risiko sprechen folgende Faktoren:
- Keine automatisierte Verarbeitung von Daten
- Verarbeitung aller Daten erfolgt zum überwiegenden Teil nur innerhalb des Kanzleinetzwerks
- Die Verarbeitung erfolgt nur sehr selten
- Die Weitergabe von Daten erfolgt ausschließlich an sorgfältig ausgewählte Professionisten
- Branchentypisch ist das Bewusstsein für Verschwiegenheit und Datenschutz vergleichsweise sehr hoch.
- Aufgrund der seit Alters bestehenden und in Österreich sehr streng ausgelegten und sehr streng praktizierten Verschwiegenheitspflicht gem. § 9 RAO erfolgt die Verarbeitung von Daten bisher schon auf einem sehr hohen Schutzniveau.

Bewertung der risikorelevanten Aspekte gemäß Art. 35 DSGVO:
- Verwendung neuer Technologien: Niedriges Risiko (Klassische EDV-Systeme, Windows Betriebssysteme, klassische Desktop-Anwendungen; Verarbeitung von Daten in klassischen Datenbanken- und Dateisystemen innerhalb des Kanzleinetzwerks)
- Art der Verarbeitung: Niedriges Risiko (ausschließlich manuelle Verarbeitung)
- Umfang der Verarbeitung: Niedriges Risiko (Verarbeitung erfolgt nur im Bedarfsfall; aufgrund ausschließlich manueller Verarbeitung auf das Notwendige reduziert)
- Umstände der Verarbeitung: Niedriges Risiko (die Verarbeitung erfolgt durch sorgfältig ausgewählte Professionisten und vornehmlich innerhalb der Kanzleiräumlichkeiten; es besteht zu keinem Zeitpunkt eine Not-, Stress- oder Verführungssituation)
- Zwecke der Verarbeitung: Niedriges Risiko (die Verarbeitungszwecke sind in unserer Informationsgesellschaft Teil fast jeder Unternehmer und daher allgemein anerkannt und legitim)

Das im Zusammenhang mit diesem Verarbeitungsvorgang bestehende Risiko für die Rechte und Freiheiten natürlicher Personen wird daher nicht als hoch bewertet. Die Durchführung einer Datenschutz-Folgeabschätzung ist daher nicht erforderlich.

1.3.3.9 Spezifische TOMs

Personen der Empfängerkategorie „IT-Support“ wird Zugang zu Systemen und Daten nur unter Beisein von Kanzleipersonal gewährt. Alle Kanzleimitarbeiter/innen werden auf diese Regel im Dienstvertrag bzw. in einer Datenschutzvereinbarung als Zusatz zum Dienstvertrag hingewiesen. Eine Ausnahme gilt für den Fall, dass notwendige Servicearbeiten durchgeführt werden müssen, welche

den Kanzleibetrieb maßgeblich stören würden. Diese Arbeiten werden ausschließlich von vertrauenswürdigen und dazu beauftragten Personen vorgenommen.