Leistungsbeschreibung fino KanzleiDrive Funktionsumfang Steuerberater

1. Leistungsmerkmale für die fino KanzleiDrive Lösung Funktionsumfang Steuerberater

Begriffsbestimmungen:

Cloud-Lösungen der fino kanzleidrive: Software für das Arbeiten in der fino-Cloud

Die Begriffe fino oder fino kanzleidrive bezeichnen die fino kanzleidrive GmbH.

1.1. Technische Rahmenbedingungen

Zu Nutzung des Dienstes ist ein Internetzugang sowie eine aktuelle Browser-Software notwendig.

1.2. Entfällt

1.3. Verfügbarkeit

Der Auftragnehmer unterhält über seinen Provider für die Internetpräsenzen ein ständig überwachtes Server-System unter den Zertifikatsvoraussetzungen nach DIN 27001.

Leistungsübergabepunkt ist der Router-Ausgang des von fino genutzten Rechenzentrums zum Internet. Für die Anbindung an das Internet, das Bereitstellen oder das Aufrechterhalten der Netzverbindung zum Rechenzentrum sowie das Beschaffen und Bereitstellen von Netzzugangskomponenten für das Internet auf Kundenseite muss der Kunde selbst Sorge tragen.

Der fino-Service steht 24 Stunden am Tag und 365 Tage pro Jahr mit einer Verfügbarkeit von 98% im Monatsmittel („SLA“) zur Verfügung. Hiervon ausgenommen sind folgende Zeiten:

a) Zeiten, in denen die Leistungen aufgrund von technischen oder sonstigen Problemen, die nicht in Einflussbereich des Betreibers liegen, nicht zu erreichen sind. Hierzu gehören unter anderem höhere Gewalt, Verschulden Dritter, sofern diese nicht Erfüllungsgehilfen iSd §278 BGB sind, sowie Ursachen im Einflussbereich des Kunden oder dem des Drittanbieters; Höhere Gewalt im Sinne dieses Absatzes bezeichnet dabei schwerwiegende Ereignisse wie insbesondere Feuer, militärische Gewalt, Aufruhr oder Unruhen, Arbeitsstreiks oder kriegsbedingte Embargos, Unwetter, Engpässen, Pandemien und Epidemien (z.B. Ausbreitung von COVID-19) oder sonstige Umstände und Ursachen, die außerhalb der zumutbaren Kontrolle der betroffenen Partei liegen, die unvermeidbar und unvorhersehbar sind und die die Partei nicht zu vertreten hat; und
b) Zeiten der Nichtverfügbarkeit wegen geplanter und angekündigter Wartungsarbeiten sowie kurzfristig erforderlich werdender Wartungsarbeiten (insbesondere zur Behebung von Sicherheitslücken). Der Betreiber ist darum bemüht, diese Wartungsarbeiten so

einzurichten, dass diese die Nutzung von fino KanzleiDrive möglichst wenig beeinträchtigen, etwa zu Zeiten erfahrungsgemäß geringer Nutzung des Services; und

c) Zeiten der Nichtverfügbarkeit die auf vertragswidrige Nutzungshandlungen des Nutzers zurückzuführen sind.

Der Betreiber wird in diesen Fällen alle angemessenen Anstrengungen tätigen, um die Verfügbarkeit schnellstmöglich wiederherzustellen. Vorbeugende Maßnahmen sind unter Ziffer 3.4 normiert. Bei einem Systemausfall, der weder auf vorsätzliches noch grob fahrlässiges Verhalten seitens des Auftragnehmers oder seinen Mitarbeitern beruht, bestehen keine Ansprüche des Auftraggebers auf Rücktritt, Minderung, Kündigung oder Schadensersatz.

Der Auftragnehmer darf den Service zum Zwecke der Wartung vorübergehend abschalten (im Folgenden „geplante Wartungszeiten“ genannt). Der Auftragnehmer wird dem Nutzer geplante Wartungszeiten mindestens fünf (5) Arbeitstage im Voraus ankündigen. Geplante Wartungsarbeiten, die eine Nichtverfügbarkeit beinhalten, sind grundsätzlich an Wochenenden bzw. außerhalb der üblichen Geschäftszeiten (Mo-Fr 7:30-20:30 Uhr, Sa 7:30-14 Uhr) durchzuführen. Der Ausfall von sechs (6) Stunden Nutzungszeit pro Kalendermonat im Jahresdurchschnitt für Wartungsarbeiten mit Nichtverfügbarkeit des Systems ist nicht Bestandteil der zugesicherten Erreichbarkeit.

Wartungsarbeiten und Störungen:

Informationen zu Wartungsarbeiten und Störungen finden Sie unter https://status.kanzleidrive.de/.

1.4. Nutzungsrechte und Berechnung von Leistungen

Das Nutzungsrecht an der fino-Lösung erlischt durch deren Kündigung.

Die Berechnung erfolgt gemäß aktueller Preisliste, jederzeit einsehbar auf der Webseite des Betreibers unter https://kanzleidrive.de/preise/.

1.5. Pflege und Weiterentwicklung

Im Leistungsumfang enthalten sind nach dem Stand der Technik erforderliche Änderungen bzw. Anpassungen zur Instandhaltung der Software. Im Übrigen besteht eine Verpflichtung zu einer Änderung, Anpassung und Weiterentwicklung der Software nur bei einer gesonderten Vereinbarung.

1.6. Bereitstellung neuer Funktionalitäten (testweise oder dauerhaft)

fino kann ausgewählten Kunden im Rahmen der Nutzung neue Funktionalitäten– ggf. temporär – bereitstellen. Daraus entsteht kein Anspruch für den Kunden auf dauerhafte Erbringung der jeweiligen Leistungen. Erfahrungen im Kontext der Nutzung der neuen Funktionalität übermittelt der Kunde in elektronischer oder mündlicher Form. Wird die neue Funktionalität dauerhaft bereitgestellt, behält sich fino eine Bepreisung vor.

1.7. Datenaustausch mit Drittsystemen

fino kann ihren Kunden die geschuldeten Leistungen ordnungsgemäß nur dann vollständig erbringen, wenn Dritte die in Kooperationsverträgen oder vergleichbaren Vereinbarungen vorgesehenen funktionalen und sonstigen Anforderungen gegenüber fino erfüllen. fino hat keinen Einfluss auf Änderungen bzw. Wegfall, vorübergehende Aussetzungen und vorübergehende technische Nichtverfügbarkeit von Services von Dritten.

1.8. Service und Support

Produktsupport- und Serviceleistungen sind nicht Bestandteil des Leistungsumfangs.

Die Berechnung erfolgt – wo anwendbar – gemäß aktueller Preisliste.

2. Leistungskatalog

fino KanzleiDrive ermöglicht die Erfassung von Mandantenstammdaten und den DSGVO-konformen Datenaustausch (Dokumente / Nachrichten) zwischen Steuerberatern und Mandanten.

2.1. Digitale Signaturen

fino KanzleiDrive ermöglicht es, Dokumente rechtsgültig zu signieren bzw. signieren zu lassen. Signierende können digitale Dateien elektronisch signieren und sichern damit die Integrität und die Authentizität einer Datei. fino KanzleiDrive bietet die folgenden Signaturarten an:

Einfache elektronische Signatur (EES): Für die einfache elektronische Signatur wird ein Fortgeschrittenes elektronisches Siegel gemäß Art. 3 Ziff. 26 eIDAS-VO mit der Rechtswirkung gemäß Art. 35 eIDAS-VO und gemäß ETSI Standard 319 411 “NCP+” verwendet. Das Siegel verfügt über einen qualifizierten elektronischer Zeitstempel im Sinn von Art. 3 Ziff. 34 eIDAS-VO. Die EES hat nicht die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift, eine FES oder QES.

Fortgeschrittene elektronische Signatur: (FES) Für die fortgeschrittene elektronische Signatur wird ein fortgeschrittenes elektronisches Siegel gemäß Art. 3 Ziff. 26 eIDAS-VO mit der Rechtswirkung gemäß Art. 35 eIDAS-VO und gemäß ETSI Standard 319 411 “NCP+” verwendet. Das Siegel verfügt über einen qualifizierten elektronischer Zeitstempel im Sinn von Art. 3 Ziff. 34 eIDAS-VO. Das Siegel wird allerdings erst auf dem Dokument angebracht, wenn die Signierenden eine Willensbekundung per OTP abgeben (siehe 2.1 (c)). Die FES hat nicht die gleichen Rechtswirkungen wie eine handschriftliche Unterschrift oder eine QES.

Qualifizierte elektronische Signatur (QES): Die über den Signing Service erstellte QES erfüllt die in der CP / CPS definierten Eigenschaften und die Definition gemäß Art. 3 Ziff. 12 eIDAS-VO mit den Rechtswirkungen gemäß Art. 25 eIDAS-VO.

Je nach Situation benötigen gewisse Dokumente also die handschriftliche Unterschrift oder die QES ggfs. mit einem elektronischen Zeitstempel, damit beabsichtigte Rechtswirkungen überhaupt eintreten können.

Über einen Signing Service gemäß den Zertifikatsrichtlinien (CP/CPS) zur Ausstellung von Zertifikaten ausgestellte elektronische Signaturen von den Issuing CAs "Diamant“ (qualifiziert) und „Saphir“ (fortgeschritten) können bei Anwendbarkeit anderen Rechts als dem EU-Recht abweichende, allenfalls weitergehende oder weniger weitgehende Wirkungen entfalten als dies nach EU-Recht der Fall ist.

Der Austausch verschlüsselter Daten und die Ausstellung von Signaturzertifikaten unterliegt zudem in/mit gewissen Staaten gesetzlichen Restriktionen.

Grundsätzlich wird bei den Signaturen zwischen einfachen, fortgeschrittenen und qualifizierten elektronischen Signaturen unterschieden. Qualifizierte elektronische Signaturen haben die höchste Rechtswirkung und sind in zahlreichen Fällen der eigenhändigen Unterschrift gleichgestellt. Damit können grundsätzlich auch Geschäftserfordernisse erfüllt werden, die vom Gesetz her eine eigenhändige Unterschrift erfordern.

Der durch uns ausgewählte qualifizierte Vertrauensdienst erzeugt und verwaltet für den Signierenden treuhänderisch das Signaturzertifikat und stellt dieses für die Fernsignaturdienstleistung über einen verschlüsselten Kanal zur Verfügung. Der Signierende benötigt für diese Funktion keine weiteren Betriebsmittel, wie z.B. Token oder Signaturkarte. Vor der Auslösung einer qualifizierten Signatur muss der Teilnehmer sich authentifizieren und den Willen zur Signatur bekunden. Der Signing Service nutzt ein zuvor registriertes Signaturfreigabemittel (Mobile ID).

Die Signierenden können sich vorgängig durch ein nach eIDAS zugelassenes Verfahren identifizieren (BankIdent, Ausweis-Ident eID oder Video-Identverfahren) und anschließend bei jeder Signatur eine damit verbundene Authentifizierung nutzen.

Der durch fino KanzleiDrive ausgewählte Vertrauensdienstleister ist für die Ausstellung qualifizierter Zertifikate für elektronische Signaturen und elektronischer Siegel qualifizierte Vertrauensdiensteanbieter gemäß eIDAS-Verordnung und österreichischem Signatur- und Vertrauensdienstegesetz (SVG) anerkannt. Eine Konformitätsbewertungsstelle prüft regelmäßig, ob die Anforderungen, die das europäische und österreichische Recht und / oder anerkannte technische Normen an einen Vertrauensdiensteanbieter stellen, auch erfüllt werden. Die Aufsichtsstelle erteilte den Qualifikationsstatus als qualifizierte Vertrauensdiensteanbieterin. Der Vertrauensdienstleister ist auf den Vertrauenslisten gemäß Art. 22 eIDAS-Verordnung aufgenommen und berechtigt, das EU-Vertrauenssiegel zu verwenden.

Allgemein bietet der Signing Service nach Vertragsgestaltung und nach Wahl des Teilnehmers fortgeschrittene elektronische Signaturen sowie qualifizierte elektronische Signaturen für natürliche Personen fortgeschrittene elektronische Siegel für juristische Personen an.

(a) Tools zur Personenidentifikation

Bevor eine Authentifizierung möglich ist, muss der Signierende sich entsprechend den Anforderungen der jeweiligen Art der elektronischen Signatur identifizieren. Der Identifikationsprozess kann losgelöst vom Signaturprozess durch eine sogenannte Registrierungsstelle erfolgen.

1. Die zu identifizierende Person kann den Videoidentifikationsdienst aufrufen. Hierfür ist es notwendig, einen PC mit Webcam oder ein mit Kamera und einer auf der Webseite angezeigten App ausgestattetes Smartphone zu haben. Im Rahmen einer Websession muss die zu identifizierende Person benutzergeführt durch einen Operator des Videoidentifizierers seinen Ausweis zeigen und Fragen zur Bestätigung der Ausweisdaten und der Lebendigkeit im Video beantworten. Anschließend werden die so ermittelten Daten an den Vertrauensdiensteanbieter übertragen.

2. Nach Aufruf der URL wird der Signierende gebeten, eine App auf seinem Android oder Apple Smartphone zu installieren und zu nutzen, mit welcher folgende Schritte durchgeführt wurden:
   - Foto der Vorder- und Rückseiten des deutschen Personalausweises oder eines elektronischen deutschen Aufenthaltstitels/eID Card mit eID Funktion
   - Freigabe zum Auslesen und Auslesen über NFC der Chipinformationen des Ausweisdokumentes in Bezug auf die Identität

- Die Mobilnummer wird bestätigt mittels eines Einmalpasswortes, welches per SMS übergeben wird.
  Der Ergebnisdatensatz der Identitätsprüfung wird dann dem Vertrauensdiensteanbieter zur Verfügung gestellt.

3. Die zu identifizierende Person ruft nun den Bankidentifikationsdienst auf, der zunächst die Identifikationsdaten der zu identifizierenden Person inklusive Mobilnummer für zukünftige Willensbekunden erfragt. Anschließend gibt die zu identifizierende Person das Konto ihrer e-Banking fähigen Hausbank ein. Sie loggt sich auf ihr Bankkonto ein und bestätigt die von der Bank gestellten Anfragen zur Authentisierung und führt eine Referenzüberweisung durch. Die Mobilnummer wird nun noch durch ein SMS Einmalpasswort bestätigt. Nach diesem Login verlässt die zu identifizierende Person wieder ihr Bankkonto und ist damit identifiziert. Die Identifikationsdaten, die Mobilnummer und Referenz auf den Bankloginvorgang werden an den Vertrauensdiensteanbieter übertragen. Der Identifizierer verwahrt in diesem Fall die genauen Vorgangsdaten als delegierte Registrierungsstelle.

Nach erfolgreicher Durchführung des jeweiligen Identifikationsverfahrens archiviert der Vertrauensdienstleister die Identifikationsdaten für die gesetzlich vorgeschriebene Dauer und verwaltet die Annahme der Nutzungsbestimmungen. Die identifizierte Person kann fortan auf Basis des während des Identifikationsverfahrens geprüften Authentisierungsmittels (z.B. Mobilnummer) und bis zum Ablauf der Gültigkeit der Identifikation über den Vertrauensdienst des Dienstleisters – je nach Identifikationsmethode – fortgeschrittene oder qualifizierte elektronische Signaturen erstellen ("Repetitive Signing").

(b) Datenablage und Verantwortlichkeiten

Mit der Nutzung der RA-App oder des Smart Registration Service werden die Daten zur identifizierten Person sowie die Identifikationsunterlagen und der Nachweis der Annahme der Nutzungsbestimmungen auf Servern der Registrierungsstelle, des Vertrauensdienstleisters, in der Schweiz gespeichert und entsprechend den in der CP/CPS oder Gesetz genannten Fristen aufbewahrt. Das gilt nicht für die Daten eines IdP – hier gelten die Regeln des IdPs.

Bei projektspezifischen Verfahren wird die Speicherung und der Speicherort in der gesonderten Vereinbarung zur Delegation der Personenidentifikation mit Umsetzungskonzept festgehalten.

(c) Willensbekundung

Jede persönliche Signatur bedingt die Abgabe einer Willensbekundung durch den Signierenden. Für die Willensbekundung wird die Authentisierungsmethode verwendet, die bei der Identifikation des Signierenden angegeben wurde, oder es wurde im Rahmen der Identifizierung bereits eine Willensbekundung geleistet.
Für die Abgabe der Willensbekundung selbst stehen verschiedene Verfahren zur Verfügung:

- OTP: Bei diesem Verfahren entfällt die Authentisierung des Signierenden beim Signing Service, sondern der Signierende sendet direkt an den Signing Service einen Einmalcode, der

ihm zuvor via SMS übersendet wurde. Dieses Verfahren kann nur für fortgeschrittene Signaturen verwendet werden.

- Mobile ID App: Der Signierende löst eine 2-Faktor Authentisierung mittels eines vom Gerät ermöglichten biometrischen Merkmals oder eines PINs/Passwords. Hierfür muss die App vor dem ersten Einsatz, z.B. vor der Bestätigung der Nutzungsbestimmungen, installiert werden und mit der Mobilnummer initialisiert werden. Es ist ein Smartphone notwendig, welches mit dem Internet verbunden ist.

3. Regelungen zur Auftragsverarbeitung nach EU-Datenschutzgrundverordnung (DS-GVO)

Die in dieser Ziffer 3 getroffenen Regelungen zur Auftragsverarbeitung finden Anwendung für alle Leistungen der fino in Bezug auf personenbezogene Daten, die in der Anwendung fino KanzleiDrive erbracht werden.

Verantwortlicher nach Art. 4 Nr. 7 DS-GVO ist der Kunde als direkter Vertragspartner der fino, im Folgenden „Kunde“ genannt.

Die Leistungsbeschreibung ist Bestandteil der zwischen fino und dem Kunden abgeschlossenen Vereinbarung zur Auftragsverarbeitung. Bei Widersprüchen geht diese Leistungsbeschreibung der Vereinbarung zur Auftragsverarbeitung vor.

3.1. Gegenstand und Dauer der Verarbeitung

Gegenstand der Verarbeitung: fino ist im Rahmen dieser Leistung als Auftragsverarbeiter tätig.

fino stellt dem Kunden die Nutzung der in dieser Leistungsbeschreibung beschriebenen Leistung zur Verfügung und verarbeitet im Rahmen der Leistungserbringung sowie für gesondert vereinbarte Service- und Supportleistungen und bei Fernbetreuung personenbezogene Daten im Auftrag des Kunden.

Dauer der Verarbeitung: Die Verarbeitung erfolgt zeitlich unbefristet. Die in den Geschäftsbedingungen der fino geregelten Kündigungsfristen bleiben unberührt.

3.2. Art und Zweck der Verarbeitung

Der Leistungskatalog beschreibt Art und Zweck der Verarbeitung.

3.3. Kategorien betroffener Personen und Art der personenbezogenen Daten

Personenbezogene Daten sind alle Arten personenbezogener Daten, die fino im Auftrag des Kunden verarbeitet.

Im Programm werden personenbezogene Daten, die der Kunde im Programm eigenverantwortlich speichert, verarbeitet. Das Programm ermöglicht die Verarbeitung folgender Arten personenbezogener Daten zu Kategorien betroffener Personen im Rahmen der Auftragsverarbeitung:

Art der personenbezogenen Daten

Es werden die folgenden Datenarten/-kategorien verwendet:

- ☒ Personenstammdaten (Anrede, Vorname, Nachname, etc.)
- ☒ Mandantendaten (Name, Adresse, Kontaktdaten, …)
- ☒ Kontaktdaten (Telefon, E-Mail, …)

Kategorien betroffener Personen

Die betroffenen Personen sind:

- ☒ Mandanten
- ☒ Interessenten
- ☒ Mitarbeiter des Verantwortlichen (sofern sie von der verantwortlichen Person als Benutzer eingerichtet werden)
- ☒ Sonstige Dritte

3.4. Weitere Auftragsverarbeiter

Wenn im Rahmen der in dieser Leistungsbeschreibung beschriebenen Leistung weitere Auftragsverarbeiter im Sinne des Art. 28 DS-GVO eingesetzt werden, sind diese in der Übersicht der eingesetzten weiteren Auftragsverarbeiter zu finden, https://kanzleidrive.de/weitere-auftragsverarbeiter/.

3.5. Übermittlung personenbezogener Daten in ein Drittland

Wenn im Rahmen der in dieser Leistungsbeschreibung beschriebenen Leistung personenbezogene Daten an ein Drittland übermittelt werden, sind

a) das Drittland,
b) der Empfänger in dem Drittland
c) und die Information, für welche Zwecke dieser Empfänger die Daten erhält,

in der Übersicht der eingesetzten weiteren Auftragsverarbeiter zu finden.

3.6. Datenlöschung

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht fino nach Wahl des Kunden entweder alle personenbezogenen Daten oder gibt sie dem Kunden zurück, sofern nicht nach dem Unionsrecht oder nach nationalem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

fino ist berechtigt, den Kunden auf die im Programm vorhandenen Löschmöglichkeiten zur Löschung der personenbezogenen Daten zu verweisen. Weist der Kunde fino an, die Daten zu löschen, obwohl der Kunde die personenbezogenen Daten auch selbst löschen kann, so ist fino berechtigt, für diese Leistungen eine angemessene Vergütung vom Kunden zu verlangen.

Im Übrigen löscht fino personenbezogene Daten im Rahmen der Auftragsverarbeitung auf Weisung der Kunden.

3.7. Vereinbarung weiterer Vertragszwecke

fino ist berechtigt, die personenbezogenen Daten zum Zweck der Fehlerbehebung in dem fino -Produkt, in dem die Daten gespeichert sind, zu verarbeiten. Die Verarbeitung findet nur nach ausdrücklicher Anweisung des Supports durch den Kunden statt, um den Fehler des jeweiligen Einzelfalles zu beheben. Eine Massenverarbeitung durch fino erfolgt nicht.

fino ist berechtigt, die personenbezogenen Daten in anonymisierter oder gehashter Form zum Zweck der Qualitätssicherung für das fino -Produkt, in dem die Daten gespeichert sind bzw. einer neueren Version des fino -Produkts zu verarbeiten.

fino ist berechtigt, die personenbezogenen Daten zu verarbeiten,

a) soweit sie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig erachtet,
b) soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit dem vereinbarten Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängen-der Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.

Dies umfasst insbesondere auch, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern ("Denial of service"-Angriffe) und Schädigungen von Computer- und elektro-nischen Kommunikationssystemen abzuwehren.

3.8. Auftragsverarbeitung hinsichtlich gesondert vereinbarter Service- und Supportleistungen

Sofern vom Kunden angefordert, greift fino im Rahmen der Programmeinrichtung, der Service-Erbringung oder der Service-Erbringung per Remote-Zugriff auf die im Programm und im Rechenzentrum / in der Cloud gespeicherten personenbezogenen Daten gemäß Kap. 3.3 zu.

Die Verarbeitung durch fino im Rahmen des Remote-Zugriffs umfasst die durch den Kunden jeweils angewiesenen Verarbeitungsschritte.

Version: 23. Februar 2023