Datenschutzerklärung der wealthpilot GmbH

Version: 2.2

Stand: 22.02.2019

Autor: Daniel Juppe

wealthpilot GmbH
Geschäftsführer: Daniel Juppe, Marco Richter, Stephan Schug
Registergericht München, HRB 232064
USt-IdNr: DE311827540

Dachauer Straße 15 B
80335 München
Tel.: +49 (0)89 809 119 20
datenschutz@wealthpilot.de
www.wealthpilot.de

Bankverbindung:
Commerzbank München
IBAN: DE19 7004 0041 0225 3359 00
BIC: COBADEFFXXX

1. Vorbemerkung

Die wealthpilot GmbH, Dachauer Straße 15 B in 80335 München (wealthpilot) betreibt und stellt dem Kunden über das Produkt wealthpilot eine Software zur Erfassung und Aufbereitung der Konto- und Depotbestände, sowie sonstigen Vermögenswerten von Endkunden (Mandanten) bereit.

wealthpilot ermöglicht es den Kunden (Vermögensberatern) und Endkunden (Mandanten) deren Bankdaten (Bestände von Konten und Depots sowie Depotumsätze) von B2C- und/oder B2B-Bankservern zu laden und in aufbereiteter Form über den wealthpilot zu betrachten und zu analysieren. Die Bankdaten des Endnutzers werden hierfür auf dem wealthpilot-Server bei der DATEV eG verschlüsselt gespeichert und durch weitere Datenauswertung aufbereitet (z.B. Zuordnung in die Vermögensbilanz).

Die vorliegende Übersicht beschreibt den aktuellen Stand der Regelungen und des Umfangs der Verarbeitung kundenspezifischer Informationen und Geschäftsprozesse.

2. Regelungen der Verantwortlichen im Datenschutz

2.1. Geschäftsführung und sonstige Personen, insbesondere berufene Leiter, die mit der Datenverarbeitung betraut sind

(1) Vertretungsberechtigte Geschäftsführer

Herr Daniel Juppe (Geschäftsführer), Stephan Schug (Geschäftsführer), Marco Richter (Geschäftsführer)

(2) Leiter der mit der Datenverarbeitung im Bereich der Servicedienstleistung beauftragt ist

Herr Robert Fink (Leiter Entwicklung)

(3) Mitarbeiter, die Zugriff auf Kundendaten haben

Grundsätzlich haben Mitarbeiter keinen Zugriff auf Kundendaten und Daten von Endnutzern. Sollte zur Erfüllung des Geschäftszwecks der Zugriff auf Kundendaten erforderlich sein, darf der selektive und temporäre Zugriff auf die Kundendaten mit Einwilligung des Kunden erfolgen. Sollte zur Erfüllung des Geschäftszwecks der Zugriff auf Daten von Endnutzern erforderlich sein, darf der selektive und temporäre Zugriff auf diese Daten nur durch einen Geschäftsführer und mit Einwilligung des Endnutzers erfolgen.

2.2. Ansprechpartner für Datenschutz / Verantwortlicher für IT-Sicherheit

(1) Ansprechpartner für Datenschutz

Zur Beantwortung datenschutzrechtlicher Fragen kann sich der Kunde an folgenden Ansprechpartner wenden:

Herr Daniel Juppe, datenschutz@wealthpilot.de

(2) Verantwortlicher für IT-Sicherheit

Für die Einhaltung der Regelungen zur Sicherheit der informationstechnischen Systeme ist der folgende Ansprechpartner zuständig:

Herr Christof Dallermassl, c.dallermassl@wealthpilot.de

2.3. Sicherheitskonzept/ Datenschutzbericht

wealthpilot beabsichtigt über die erforderlichen Maßnahmen und Umsetzungen regelmäßige unternehmensinterne Statusberichte zu erstellen. Diese haben mindestens zu enthalten:

(1) die Durchführung einer Bestandsaufnahme zur Feststellung der Erfüllung gesetzlicher Anforderungen
(2) Ermittlung, Feststellung und Kontrolle des Handlungs- bzw. Änderungsbedarfs in Bezug auf notwendige Schutzmaßnahmen, sowie Festlegung der Zielstellungen
(3) Entwicklung / Anpassung von (internen) Richtlinien und Arbeitsanweisungen sowie Formularen zur Realisierung der Anforderungen
(4) Beurteilung / Bewertung der Angemessenheit der getroffenen technischen und organisatorischen Maßnahmen
(5) Überwachungsmaßnahmen der ordnungsgemäßen Anwendung von Datenverarbeitungs-programmen
(6) Überblick über aufgetretene Problemfelder und deren Bearbeitung

3. Umfang und Verwendung personenbezogener Daten

3.1. Rechtsgrundlage der Verarbeitung

Personenbezogene Daten dienen ausschließlich der Vertragsbegründung, inhaltlichen Ausgestaltung, Durchführung oder Abwicklung des Vertragsverhältnisses (Rechtsgrundlage hierfür ist Art. 6 I b DSGVO). Soweit Sie uns Ihre Einwilligung zur Verarbeitung erteilt haben, ist Rechtsgrundlage Art. 6 Abs. I lit. a) DSGVO.

3.2. Umfang und Art der Verwendung personenbezogener Daten

wealthpilot erhebt, verarbeitet und/oder nutzt personenbezogene Daten im Rahmen der Bereitstellung und des Betriebs einer Software zur Erfassung und Aufbereitung der Konto- und Depotbestände, sowie sonstigen Vermögenswerten von Nutzern. Umfang der Datenerhebung, -verarbeitung und/oder -nutzung personenbezogener Daten durch wealthpilot ergeben sich aus dem zugrundeliegenden Vertrag.

3.3. Zweck(e) der Verwendung

Die Verwendung personenbezogener Daten durch wealthpilot erfolgt zu folgenden Zwecken:

(1) Dokumentation und Verwaltung von Kundenbeziehungen
(2) Rechnungstellung und Inkasso
(3) Bereitstellung einer Software mit folgenden, wesentlichen Leistungsinhalten:
    - Der Nutzer gibt ausgewählte Nutzerdaten an wealthpilot.
    - Die Nutzerdaten werden von wealthpilot dafür benutzt, um selbst oder mit Hilfe von Schnittstellenanbietern (unter Punkt 9. genannt) Kontoinformationen, Bestände von Konten und Depots und Depottransaktionen des Nutzers abzurufen.
    - Die generierten Daten werden sodann von wealthpilot für Analysen aufbereitet, in der Software angezeigt und verschlüsselt gespeichert.

- Weitere Daten (wie beispielsweise Immobilienwerte), die der Auftraggeber bei wealthpilot manuell erfasst, werden jederzeit verschlüsselt gespeichert und nur für Analysen innerhalb der Anwendung weiterverarbeitet.

(4) Bereitstellung einer Oberfläche für den Zugang des Nutzers zu den abgerufenen Nutzer-Daten bzw. für die Nutzung der oben genannten Software.
(5) Ordnungsgemäße Speicherung der Kunden-Daten (Art der erhobenen Daten siehe Punkt 3.5)
(6) Ordnungsgemäße Speicherung der Nutzer-Daten (Art der erhobenen Daten siehe Punkt 3.5) bzw. der Daten, die im Rahmen der Nutzung der Software entstehen.
(7) Betrieb und Wartung der zur Verfügung gestellten Software.
(8) Jegliche personenbezogenen Daten werden rein zum Zweck verarbeitet, dem Nutzer einen bestmöglichen Service zur Verfügung zu stellen. Wealthpilot wird die Daten niemals für eigene Marketing- oder Vertriebszwecke verarbeiten.

3.4. Zweckbindung und Weitergabe personenbezogener Daten

Personenbezogene Daten werden ausschließlich zu vorgenanntem Zweck verarbeitet. Die Daten des Kunden und des Endnutzers können an die folgenden Dritten, bei der Vorlage eines rechtlichen Erlaubnistatbestandes weitergegeben werden:

(1) Öffentliche Stellen, sofern vorrangige Rechtsvorschriften bzw. Erlaubnissätze existieren (z.B. Ermittlungsbehörden, Finanzbehörden, Sozialversicherungsträger usw.)
(2) Auftragnehmer, insbesondere Auftragsverarbeiter jeweils zur Erfüllung der vorstehenden Zwecke und / oder hoheitlicher Vorgaben. Diese sind unter 9. aufgeführt.

3.5. Art der Daten, die wealthpilot verarbeitet

(1) Kunde-Daten zur Dokumentation, Verwaltung, Rechnungsstellung und Inkasso:
   a. Zur Dokumentation und Verwaltung: Name, Adresse, Telefonnummer, Email, Homepage, Kontakthistorie, Vertragsdaten
   b. Rechnungsstellung und Inkasso: Name, Adresse, Telefonnummer, Email, Bankverbindung, Rechnungshistorie
(2) Nutzer-Daten bei der Nutzung der Software:
   a. Kontoverbindungs-Daten der Nutzerkonten: Name der Bank, BLZ, BIC
   b. Zugangsdaten zu den Berater-/Verwalter-Zugängen zu den Nutzer-Konten: Depotbank-Zugangsdaten des Beraters/Verwalters (Kunden)
   c. Zugangsdaten zu den Nutzer-Konten: Online-Banking Zugangsdaten und PIN aller eingebundenen Nutzer-Konten.
   d. Konto-Daten der Nutzerkonten: Name des Kontoinhabers, Kontotyp (z.B. Depot, Giro-, Sparkonto), Kontobezeichnung, Kontonummer, Kontostand
   e. Wertpapierinformationen bei Depots: z.B. Name des Wertpapiers, ISIN, WKN, aktueller Kurs, Ankaufskurs, Anzahl Wertpapiere

f. Informationen zu Vermögenswerten, die der Nutzer manuell erfasst: Wert, Bezeichnung und individuelle Informationen zu einem Vermögenswert, wie beispielsweise eine Immobilie.
g. Alle Daten werden verschlüsselt im sicheren Rechenzentrum der DATEV gespeichert und verschlüsselt übermittelt

3.6. Kreis der Betroffenen

(1) Kunden, die ein Vertragsverhältnis mit wealthpilot eingegangen sind.
(2) Nutzer, die im Rahmen des Serviceangebots von wealthpilot einen Zugang zur Software besitzen.

3.7. Einhaltung von Datensparsamkeit, Datenvermeidung

wealthpilot hat sich dem Grundsatz der Datenvermeidung und Datensparsamkeit verpflichtet. Die Mitarbeiter sind angewiesen, sofern nicht anders angeordnet, dafür Sorge zu tragen, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

3.8. Empfänger von Daten

An die im Folgenden aufgeführten Stellen können die vorstehenden Daten mitgeteilt werden:

(1) Öffentliche Stellen, sofern vorrangige Rechtsvorschriften bzw. Erlaubnissätze existieren (z.B. Ermittlungsbehörden, Finanzbehörden, Sozialversicherungsträger usw.)
(2) Auftragnehmer, insbesondere Auftragsverarbeiter jeweils zur Erfüllung der vorstehenden Zwecke und / oder hoheitlicher Vorgaben. Diese sind unter 9. aufgeführt.

3.9. Rechte der betroffenen Person

(1) **Recht auf Bestätigung:** Jede betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber eingeräumte Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Möchte eine betroffene Person dieses Bestätigungsrecht in Anspruch nehmen, kann sie sich hierzu jederzeit an einen Mitarbeiter des für die Verarbeitung Verantwortlichen wenden.
(2) **Recht auf Auskunft:** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, jederzeit von dem für die Verarbeitung Verantwortlichen unentgeltliche Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten und eine Kopie dieser Auskunft zu erhalten. Ferner hat der Europäische Richtlinien- und Verordnungsgeber der betroffenen Person Auskunft über folgende Informationen zugestanden:
    a. die Verarbeitungszwecke
    b. die Kategorien personenbezogener Daten, die verarbeitet werden
    c. die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen

d. falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
e. das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
f. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
g. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden: Alle verfügbaren Informationen über die Herkunft der Daten
h. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Abs.1 und 4 DS-GVO und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person
i. Ferner steht der betroffenen Person ein Auskunftsrecht darüber zu, ob personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt wurden. Sofern dies der Fall ist, so steht der betroffenen Person im Übrigen das Recht zu, Auskunft über die geeigneten Garantien im Zusammenhang mit der Übermittlung zu erhalten.
j. Möchte eine betroffene Person dieses Auskunftsrecht in Anspruch nehmen, kann sie sich hierzu jederzeit an einen Mitarbeiter des für die Verarbeitung Verantwortlichen wenden.

(3) **Recht auf Berichtigung:** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Ferner steht der betroffenen Person das Recht zu, unter Berücksichtigung der Zwecke der Verarbeitung, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen. Möchte eine betroffene Person dieses Berichtigungsrecht in Anspruch nehmen, kann sie sich hierzu jederzeit an einen Mitarbeiter des für die Verarbeitung Verantwortlichen wenden.

(4) **Recht auf Löschung (Recht auf Vergessen werden):** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, von dem Verantwortlichen zu verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern einer der folgenden Gründe zutrifft und soweit die Verarbeitung nicht erforderlich ist:

a. Die personenbezogenen Daten wurden für solche Zwecke erhoben oder auf sonstige Weise verarbeitet, für welche sie nicht mehr notwendig sind.
b. Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 Buchstabe a DS-GVO oder Art. 9 Abs. 2 Buchstabe a DS-GVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
c. Die betroffene Person legt gemäß Art. 21 Abs. 1 DS-GVO Widerspruch gegen die Verarbeitung ein, und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Art. 21 Abs. 2 DS-GVO Widerspruch gegen die Verarbeitung ein.
d. Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e. Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
f. Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DS-GVO erhoben.

Sofern einer der oben genannten Gründe zutrifft und eine betroffene Person die Löschung von personenbezogenen Daten, die bei der wealthpilot GmbH gespeichert sind, veranlassen möchte, kann sie sich hierzu jederzeit an einen Mitarbeiter des für die Verarbeitung Verantwortlichen wenden. Der Mitarbeiter der wealthpilot GmbH wird veranlassen, dass dem Löschverlangen unverzüglich nachgekommen wird.

Wurden die personenbezogenen Daten von der wealthpilot GmbH öffentlich gemacht und ist unser Unternehmen als Verantwortlicher gemäß Art. 17 Abs. 1 DS-GVO zur Löschung der personenbezogenen Daten verpflichtet, so trifft die wealthpilot GmbH unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um andere für die Datenverarbeitung Verantwortliche, welche die veröffentlichten personenbezogenen Daten verarbeiten, darüber in Kenntnis zu setzen, dass die betroffene Person von diesen anderen für die Datenverarbeitung Verantwortlichen die Löschung sämtlicher Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat, soweit die Verarbeitung nicht erforderlich ist. Der Mitarbeiter der wealthpilot GmbH wird im Einzelfall das Notwendige veranlassen.

(5) **Recht auf Einschränkung der Verarbeitung:** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

a. Die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen.
b. Die Verarbeitung ist unrechtmäßig, die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten.
c. Der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
d. Die betroffene Person hat Widerspruch gegen die Verarbeitung gem. Art. 21 Abs. 1 DS-GVO eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Sofern eine der oben genannten Voraussetzungen gegeben ist und eine betroffene Person die Einschränkung von personenbezogenen Daten, die bei der wealthpilot GmbH gespeichert sind, verlangen möchte, kann sie sich hierzu jederzeit an einen Mitarbeiter des für die Verarbeitung Verantwortlichen wenden. Der Mitarbeiter der wealthpilot GmbH wird die Einschränkung der Verarbeitung veranlassen.

(6) **Recht auf Datenübertragbarkeit: J**ede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, die sie betreffenden personenbezogenen Daten, welche durch die betroffene Person einem Verantwortlichen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie hat außerdem das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf der Einwilligung gemäß Art. 6 Abs. 1 Buchstabe a DS-GVO oder Art. 9 Abs. 2 Buchstabe a DS-GVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 Buchstabe b DS-GVO beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt, sofern die Verarbeitung nicht für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, welche dem Verantwortlichen übertragen wurde.
Ferner hat die betroffene Person bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Art. 20 Abs. 1 DS-GVO das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist und sofern hiervon nicht die Rechte und Freiheiten anderer Personen beeinträchtigt werden.
Zur Geltendmachung des Rechts auf Datenübertragbarkeit kann sich die betroffene Person jederzeit an einen Mitarbeiter der wealthpilot GmbH wenden.

(7) **Recht auf Widerspruch:** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 Buchstaben e oder f DS-GVO erfolgt, Widerspruch einzulegen. Dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.
Die wealthpilot GmbH verarbeitet die personenbezogenen Daten im Falle des Widerspruchs nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
Verarbeitet die wealthpilot GmbH personenbezogene Daten, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung der personenbezogenen Daten zum Zwecke derartiger Werbung einzulegen. Dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widerspricht die betroffene Person gegenüber der wealthpilot GmbH der Verarbeitung für Zwecke der Direktwerbung, so wird die wealthpilot GmbH die personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.
Zudem hat die betroffene Person das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung personenbezogener Daten, die bei der wealthpilot GmbH zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Art. 89 Abs. 1 DS-GVO erfolgen, Widerspruch einzulegen, es sei denn, eine solche Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.
Zur Ausübung des Rechts auf Widerspruch kann sich die betroffene Person direkt jeden Mitarbeiter der wealthpilot GmbH oder einen anderen Mitarbeiter wenden. Der betroffenen Person steht es ferner frei, im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft, ungeachtet der

Richtlinie 2002/58/EG, ihr Widerspruchsrecht mittels automatisierter Verfahren auszuüben, bei denen technische Spezifikationen verwendet werden.

(8) **Automatisierte Entscheidungen im Einzelfall einschließlich Profiling:** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung — einschließlich Profiling — beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, sofern die Entscheidung (1) nicht für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist, oder (2) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder (3) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.
Ist die Entscheidung (1) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich oder (2) erfolgt sie mit ausdrücklicher Einwilligung der betroffenen Person, trifft die wealthpilot GmbH angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.
Möchte die betroffene Person Rechte mit Bezug auf automatisierte Entscheidungen geltend machen, kann sie sich hierzu jederzeit an einen Mitarbeiter des für die Verarbeitung Verantwortlichen wenden.

(9) **Recht auf Widerruf einer datenschutzrechtlichen Einwilligung:** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, eine Einwilligung zur Verarbeitung personenbezogener Daten jederzeit zu widerrufen.
Möchte die betroffene Person ihr Recht auf Widerruf einer Einwilligung geltend machen, kann sie sich hierzu jederzeit an einen Mitarbeiter des für die Verarbeitung Verantwortlichen wenden. Vermeidung von Rechtsverletzungen und ihrer Folgen
Sowohl die Mitarbeiter als auch die für die wealthpilot tätigen Dienstleister sind, respektive werden bezüglich der Einhaltung der spezifischen datenschutzrechtlichen Regelungen belehrt und nach § 5 BDSG auf das Datengeheimnis verpflichtet.
Sofern Rechtsverletzungen bekannt werden und / oder derartige von Dritten glaubhaft gemacht werden, ist die Geschäftsleitung unverzüglich zu informieren.

(10) **Recht auf Beschwerde:** Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das Recht, Beschwerde bei der zuständigen Aufsichtsbehörde einzureichen.

3.10. Löschung von Daten

Der für die Verarbeitung Verantwortliche verarbeitet und speichert personenbezogene Daten der betroffenen Person nur für den Zeitraum, der zur Erreichung des Speicherungszwecks erforderlich ist oder sofern dies

durch den Europäischen Richtlinien- und Verordnungsgeber oder einen anderen Gesetzgeber in Gesetzen oder Vorschriften, welchen der für die Verarbeitung Verantwortliche unterliegt, vorgesehen wurde.

Entfällt der Speicherungszweck oder läuft eine vom Europäischen Richtlinien- und Verordnungsgeber oder einem anderen zuständigen Gesetzgeber vorgeschriebene Speicherfrist ab, werden die personenbezogenen Daten routinemäßig und entsprechend den gesetzlichen Vorschriften gesperrt oder gelöscht.

Die Löschung von Daten erfolgt unverzüglich, sofern ein derartiges Verlangen bei wealthpilot eingeht.

An die Stelle einer Löschung tritt eine Sperrung, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist. Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

4. Regelungen zur IT-Sicherheit

Informationsverarbeitung spielt eine Schlüsselrolle für die Aufgabenerfüllung von wealthpilot. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von Systemen muss insgesamt kurzfristig kompensiert werden können. Alle Mitarbeiter von wealthpilot halten die einschlägigen Gesetze (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für den Kunden sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden. Alle Mitarbeiter und die Geschäftsführung sind sich ihrer Verantwortung beim Umgang mit den Dienstleistungen bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

Zum Schutz, zur Aufrechterhaltung und Gewährleistung der IT-Sicherheit und Servicequalität hat sich wealthpilot zur Einhaltung der Wahrung eines Release und Deployment Management Prozesses verpflichtet.

5. Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes sind Anlage 1 zu entnehmen.

6. Allgemeine Belehrungen zum Thema Datenschutz

wealthpilot legt Wert darauf, dass ihre Mitarbeiter und / oder die für sie tätigen Dritten im ausreichenden Maß über die datenschutzrelevanten Bestimmungen informiert und in regelmäßigen Abständen hierüber belehrt werden.

Neben den ausdrücklichen in den Arbeitsverträgen enthaltenden datenschutzrechtlichen Regelungen sowie den Bestimmungen zur Wahrung der Vertraulichkeit sind die Mitarbeiter von wealthpilot in ihrer praktischen Arbeit auf die Wahrung des Datenschutzes und der Datensicherheit sensibilisiert. Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu

verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

wealthpilot ist zudem bestrebt sämtlichen Mitarbeitern und / oder Dritten, welche die IT-Systeme, respektive die vorhandene Infrastruktur, nutzen, die Wahrung des Datenschutzes und der Datensicherheit zu gewährleisten. Hierfür wurden diverse Richtlinien (insbesondere zur Nutzung von Ressourcen) veröffentlicht.

Zur Erfüllung der vorgenannten Verpflichtungen verpflichtet sich jeder Mitarbeiter durch eine gesonderte Erklärung zur Wahrung des Datenschutzes.

7. Regelungen zur IT-Nutzung

wealthpilot ist bestrebt sämtlichen Mitarbeitern und / oder Dritten, welche die IT-Systeme, respektive die vorhandene Infrastruktur, nutzen, die Wahrung des Datenschutzes und der Datensicherheit zu gewährleisten. Hierfür hat wealthpilot diverse Richtlinien veröffentlicht. Jeder Nutzer hat die Kenntnis der geltenden Bestimmungen regelmäßig zu bestätigen.

8. Schulungen und Zusammenarbeit

Alle Mitarbeiter werden in regelmäßigen Abständen über die Einhaltung der Grundsätze des Datenschutzes und der Datensicherheit belehrt.

wealthpilot stellt alle zur Erbringung der Leistungen erforderlichen Informationen, und soweit dies zur Erfüllung der Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung.

Es ist gewährleistet, dass sich Betroffene jederzeit an die Geschäftsleitung wenden können.

9. Externe Dienstleister

wealthpilot bedient sich zu ihrer Aufgabenerfüllung externer Dienstleister. Insbesondere da wesentliche Vorgänge der Datenverarbeitung, der IT-Infrastruktur sowie spezieller kundenspezifischer Anwendungen hiervon betroffen sind, werden mit den Dienstleistern vertragliche Regelungen schriftlich festgehalten.

wealthpilot verpflichtet alle externen Dienstleistungserbringer zur Wahrung des Datengeheimnisses und der Vertraulichkeit. Der Dienstleister hat eine Hilfsfunktion, er leistet dem Auftraggeber in einer oder mehreren Phasen der Datenerhebung, -verarbeitung oder -nutzung weisungsgebundene Unterstützung. Er übernimmt keine Aufgabe in ihrer Vollständigkeit, sondern lediglich ihre technische Ausführung. Sofern eine Auftragsverarbeitung vorliegt, schließen die Parteien eine gesonderte Vereinbarung gem. Art. 28 DSGVO. wealthpilot setzt derzeit die folgenden Dienstleistungsunternehmen ein:

(1) Zur Dokumentation und Verwaltung von Kundenbeziehungen:
   a. Als CRM: HubSpot, Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141
   b. Als Hoster für CRM und Homepage: 1&1 Internet SE, Elgendorfer Str. 57, 56410 Montabaur
   c. Als Servicedesk: JIRA Service Desk von Atlassian, Inc., 1098 Harrison Street, San Francisco, CA 94103, USA

d. Als Dokumentenmanagementsystem: Sharepoint von Microsoft Corporation, One Microsoft Way, Redmond, WA, USA 98052
e. Als Mailprogramm: Outlook von Microsoft Corporation, One Microsoft Way, Redmond, WA, USA 98052

(2) Zur Rechnungstellung und Inkasso:
a. Zur Rechnungsstellung: FastBill GmbH, Wildunger Str. 6, 60487 Frankfurt am Main
b. Für den Einzug der Lastschriftvereinbarungen: Commerzbank Aktiengesellschaft, Kaiserplatz, 60311 Frankfurt/Main

(3) Für den Abruf von Kontoinformationen in der Software:
a. FinAPI GmbH, Ainmillerstr. 11, 80801 München, BSDI Grundschutz, ISO 27001, ISO 20000, ITIL, Eco Datacenter Star Audit 5 Sterne und Qualys SSL Labs Security Report Rating A (Bestnote) zertifiziert.
b. NDGIT GmbH, Ridlerstraße 35a, 80339 München, ISO 27001.

(4) Zur ordnungsgemäßen Speicherung der Nutzer-Daten in der Software:
a. Hoster des Servers: DATEV eG, Paumgartnerstraße 6-14, 90429 Nürnberg, zertifiziert nach ISO 27001. Datenspeicherung erfolgt ausschließlich unter deutschem Recht.
b. Service und Wartung des Servers: Schuster & Walther IT-Business GmbH, Schwabacher Straße 3, 90439 Nürnberg

Anlage 1: Technische und organisatorische Maßnahmen der wealthpilot GmbH

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind.

wealthpilot erklärt, dass die technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DS-GVO dem Grunde nach eingehalten werden.

1. Rechenzentrum der Software:

Die schützenswerten Daten der Software werden in den Rechenzentren der DATEV eG gespeichert und verarbeitet.

Informationen über Zertifizierungen der DATEV eG sind hier festgehalten:

https://www.datev.de/web/de/aktuelles/datev-news/maximale-sicherheit-datev-rechenzentrum-nach-iso-27001-zertifiziert/

Die technischen und organisatorischen Maßnahmen der DATEV eG sind im Dokument „AVV_unterschrieben_DATEV.pdf“ festgehalten.

2. Maßnahmen der wealthpilot GmbH

Folgende Maßnahmen werden von wealthpilot getroffen:

2.1. Pseudonymisierung und Verschlüsselung der Daten der Software:

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, die ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Folgende Maßnahmen werden getroffen:

- Ersetzen von Teilen der Daten
- Vollständige Verschlüsselung aller Daten

2.2. Zutrittskontrolle

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen mit denen personenbezogene Daten verarbeitet werden, sowie vertraulichen Akten und Datenträgern physisch verwehren.

Folgende Maßnahmen werden getroffen:

- Revisionssichere Schließanlage mit überwachter Schlüsselausgabe
- Türsicherung zusätzlich mittels elektronischer Token
- Beaufsichtigung oder Begleitung von Fremdpersonen
- Zutritt zu den Büroräumen wird Unbefugten verwehrt
- Türzutrittsprotokolle und Zutrittskontrollsysteme an allen Eingängen

- Objektsicherung mittels Überwachungseinrichtungen (Videoüberwachung)

Folgende Maßnahmen werden zusätzlich in den Rechenzentren getroffen:

- Besetzter Empfang während der regulären Bürozeiten
- Gebäudeüberwachung durch Pförtner und externen Wachschutz
- Serverraum zusätzlich mit eigenem Schließkreis gesichert

2.3. Zugangskontrollen

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.

Folgende Maßnahmen werden getroffen:

- Zugangsberechtigungen für alle Datenverarbeitungssysteme
- IT-Systeme und Endbenutzergeräte erfordern Authentifizierung mittels Kennwortverfahren, d.h. persönlicher und individueller User Log-In bei jeder Anmeldung im System
- Einrichtung eines Benutzerstammsatzes pro User
- Passwortrichtlinie für Standards für individuelle Passwörter
- Access-Control-Listen
- Abkapselung von sensiblen Systemen durch getrennte Netzbereiche
- Protokollierung der Anmeldungen und Anmeldeversuche
- Einrichten von kontinuierlich aktualisierten Antiviren- und Spywarefiltern
- mehrfach redundante Firewalls

2.4. Zugriffskontrollen

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Folgende Maßnahmen werden getroffen:

- Berechtigungskonzepte (Profile, Rollen, etc.) und deren Dokumentation
- eingeschränkte Berechtigungen durch Gruppen- und Hierarchieberechtigungen streng nach dem Need-to-know-Prinzip
- Benutzeraccounts werden nur durch die Geschäftsführung eingerichtet
- Protokollierungen: automatische Monitoring-Prozesse protokollieren die Zugriffe
- Geordnete Verfahren und Abläufe für Security-Patches und gemeldete Schwachstellen
- Blockieren von Ein- und Ausgabeschnittstellen an allen Systemen, die personenbezogene Daten verarbeiten
- Nach Ausscheiden eines Mitarbeiters wird dessen Benutzeraccount, einschließlich aller Berechtigungen sofort gesperrt

2.5. Nichtverkettbarkeit/Zweckbindung

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Folgende Maßnahmen werden getroffen:

- Berechtigungskonzepte
- Verschlüsselte Speicherung von personenbezogenen Daten
- Softwareseitige Mandanten- und Kundentrennung
- Trennung von Entwicklungs-, Test- und Produktivsystemen

2.6. Weitergabeprotokolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

Folgende Maßnahmen werden getroffen:

- Alle Mitarbeiter sind zur Einhaltung der datenschutzrechtlichen Vorschriften und auf das Datengeheimnis gemäß § 53 BDSG (neu) verpflichtet
- Übermittlung von Daten über verschlüsselte Datennetze oder Tunnelverbindungen, Daten werden serverseitig grundsätzlich SSL-verschlüsselt übertragen
- sicherer Transportbehälter für Datenträger
- Daten dürfen auf allen mobilen Devices (USB-Stick, DVDs) nur nach kryptographischer Verschlüsselung abgelegt werden
- umfassende Protokollierungsverfahren
- fachgerechte und sichere Entsorgung von Datenträgern und Dokumenten

2.7. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in EDV-Systeme eingegeben, verändert oder entfernt worden sind.

Folgende Maßnahmen werden getroffen:

- Protokollierung der Systemaktivitäten
- Mitarbeiter haben grundsätzlich keine Rechte zum Eingeben, Verändern oder Entfernen personenbezogener Daten.
- Alle Mitarbeiter werden auf das Datengeheimnis nach § 53 BDSG (neu) verpflichtet und es werden in regelmäßigen Abständen Veranstaltungen und Fortbildungen zum Thema Datensicherheit durchgeführt.
- Die effektive Zugangskontrolle (vgl. 2.3) sichert ebenfalls die Eingabekontrolle.

2.8. Verfügbarkeitskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Folgende Maßnahmen werden getroffen:

- Es existieren redundante Datensicherungsverfahren, die jederzeit ein vollständiges Back-Up und Recovery gewährleisten
- Notfall- und Sicherungskonzept

Folgende Maßnahmen werden zusätzlich in den Rechenzentren getroffen:

- Backups werden in eigenen Brandabschnitten verwahrt
- vollständig redundant ausgelegtes Rechenzentrum, einschl. USV
- präventiver Brandschutz: OxyReduct-Anlage/Argon-Löschanlage mit Brandfrüherkennung
- Alarmanlage
- Hardware-Monitoring
- zertifizierte Serverraum- und IT-Sicherheit nach modernsten Standards

2.9. Transparenz und Intervenierbarkeit

Maßnahmen, die sicherstellen, dass jederzeit bekannt ist, welche Daten von Betroffenen sich wo im Unternehmen und IT-Systemen befinden (Transparenz), und dass diese Daten ggf. rasch verändert und herausgegeben werden können (Intervenierbarkeit).

Folgende Maßnahmen werden getroffen

- Sicherstellung des Grundsatzes der Datenminimierung
- Definition klarer Prozessabläufe und Überwachen deren Einhaltung
- Maßnahme zur Gewährleistung der Identifizierbarkeit und Zuordnung von Daten (insbesondere im Fall der Pseudonymisierung und Verschlüsselung)

2.10. Datenschutzfreundliche Voreinstellungen

Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Folgende Maßnahmen werden getroffen

- Pseudonymisierung von Daten
- Verschlüsselung von Daten
- Maßnahmen gemäß 2.2. bis 2.6.
- Einschränkung der Verarbeitung von Daten
- Umfassendes Löschkonzept

2.11. Auftragskontrolle

Maßnahmen, die gewährleisten, dass in einem Auftragsverarbeitungsverhältnis jede Verarbeitung von personenbezogenen Daten nur im Rahmen der ergangenen Weisungen und Vorgaben des Auftraggebers erfolgt.

Folgende Maßnahmen werden getroffen

- vertragliche Regelungen mit externen Dienstleistern zur Auftragsverarbeitung gem. Art. 28 DSGVO
- Sicherstellung, dass Abweichungen von den Weisungen des Auftraggebers nicht vorkommen können, hierzu gehört der Ausschluss unzulässiger Verarbeitungsschritte oder das nicht erlaubte Kopieren von personenbezogenen Daten
- Alle Mitarbeiter werden auf das Datengeheimnis nach §53 BDSG (neu) verpflichtet und es werden in regelmäßigen Abständen Veranstaltungen und Fortbildungen zum Thema Datensicherheit durchgeführt.

3. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen

3.1. Datenschutz-Management

wealthpilot hat ein Datenschutz-Konzept aufgestellt, welches regelmäßig aktualisiert und überprüft wird.

3.2. Incident-Response-Management

Im Datenschutz-Konzept ist auch ein „Prozess für die Meldung von Datenschutzverstößen“ enthalten.