Vereinbarung zur Auftragsdatenverarbeitung gemäß Artikel 28 DSGVO

zwischen

XPS-Finanzsoftware GmbH Zugspitzstraße 6, 81541 München (nachfolgend "Auftragnehmer" genannt)	und	dem Lizenznehmer der XPS-Finanzsoftware GmbH (nachfolgend "Auftraggeber" genannt)

1. Gegenstand
Der Auftraggeber ist Lizenznehmer von XPS-Privatfinanz, einer webbasierten Anwendung mit optionalen Modulen für die private Finanzplanung, Ruhestandsplanung, Generationen-Tool sowie verschiedenen Finanztools für Standardaufgaben von Finanzberatern. Der Auftraggeber kann Analysemodule von XPS-Privatfinanz nutzen und ggfls. seinen Kunden und Interessenten über eine Verlinkung auf seiner Webseite zur Verfügung stellen. In diesem Rahmen werden Daten durch den Auftragsgeber oder durch seine Kunden und Interessenten in XPS-Privatfinanz erfasst und entsprechend des Analysezwecks verarbeitet. Außerdem kann der Lizenznehmer XPS-Privatfinanz nutzen, um Kunden- und Vertragsdaten online zu speichern und zu verwalten („CRM“).

2. Dauer der Auftragsdatenverarbeitung
Der Auftrag zur Datenverarbeitung ist wesentlicher Teil des zwischen Auftraggeber und Auftragnehmer geschlossenen Lizenzvertrags über XPS-Privatfinanz. Die hier vorliegende Vereinbarung zur Auftragsdatenverarbeitung beginnt und endet mit dem zwischen Auftragnehmer und Auftraggeber geschlossenen Lizenzvertrag über XPS-Privatfinanz.

3. Kategorien der betroffenen Personen
Es sind folgende Personengruppen von der Auftragsdatenverarbeitung betroffen: Kunden und Interessenten des Auftraggebers.

4. Art der Daten
Es werden folgende Arten von Daten gespeichert und verarbeitet: Geburtsdaten, Einkommens- und Vermögensdaten, Daten zu Versicherungsverträgen, Adress- und Kommunikationsdaten (letzteres falls XPS-Privatfinanz als Verwaltungssystem und CRM-Tool genutzt wird).

5. Zweck der Auftragsdatenverarbeitung
Die Auftragsdatenverarbeitung dient folgenden Zwecken: Erstellung einer privaten Finanzplanung, Ruhestandsplanung, Generationenplanung, Analyse von speziellen Problemstellungen (z.B. Kauf einer Immobilie), Verwaltung und CRM.

6. Ort
Die Auftragsdatenverarbeitung findet ausschließlich in Deutschland statt.

7. Technische und organisatorische Maßnahmen
Der Auftragnehmer trifft für seinen Verantwortungsbereich die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten. Der Auftraggeber gestattet dem Auftragnehmer, Maßnahmen zu ergreifen, die sich aus dem technischen Fortschritt ergeben und zur Verbesserung des Sicherheitsniveaus beitragen. Die Darlegung der Technische und organisatorische Maßnahmen (TOM, Stand 03.12.2025) sind Vertragsbestandteil.

8. Auskunft, Berichtigung, Einschränkung und Löschung von Daten
Der Auftragnehmer darf Daten, die vom Auftraggeber oder seinen Kunden und Interessenten erfasst und im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Der Auftragnehmer hat technisch und konzeptionell das Recht auf Löschen, Berichtigung und Auskunft zu personenbezogenen Daten sicher zu stellen.

9. Sonstige Pflichten des Auftragnehmers
Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Insbesondere gewährleistet der Auftragnehmer folgende Vorgaben:

- Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Mitarbeiter ein, die auf Vertraulichkeit verpflichtet und zuvor mit allen für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
- Der Auftragnehmer unterstützt den Auftraggeber nach besten Kräften, wenn dieser von Kontrollen, Haftungsansprüchen oder einem anderen Anspruch im Zusammenhang mit dieser Vereinbarung ausgesetzt ist.
- Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

10. Pflichten des Auftraggebers
Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO und insoweit zur Umsetzung der gesetzlichen Vorschriften verpflichtet.

- Der Auftraggeber ist alleine für die Beurteilung der Zulässigkeit der Auftragsdatenverarbeitung sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Der Auftraggeber trägt Sorge dafür, dass die gesetzlich notwendigen Voraussetzungen geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.
- Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrags bestehen.

11. Unterauftragsverhältnisse
Unterauftragnehmer, die der Auftragnehmer für Nebenleistungen einsetzt, wie z.B. Serveradministrator oder freie Softwareentwickler werden vom Auftragnehmer nur dann eingesetzt, wenn mit ihnen eine entsprechende vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO geschlossen wurde. Eine sorgfältige Auswahl erfolgt durch den Auftragnehmer. Die tatsächliche Auftragsdatenverarbeitung als Hauptleistung geschieht ausschließlich durch den Auftragnehmer. Der Auftraggeber stimmt der Beauftragung der in der Anlage „TOM“ genannten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.
Die Hinzunahme eines Unterauftragnehmers oder der Wechsel eines bestehenden Unterauftragnehmers sind zulässig, wenn der Auftragnehmer dies vorab schriftlich anzeigt und der Auftraggeber nicht innerhalb von zwei Wochen schriftlich Einspruch erhebt. Eine weitere Unterbeauftragung durch einen Unterauftragnehmer ist nicht zulässig.
Im Rahmen von besonderen Nutzungen wird KI von Drittanbietern eingesetzt. Vor der Nutzung wird der konkrete KI-Anbieter benannt und es erfolgen weitere Hinweise und der Anwender muss der Verarbeitung durch die KI aktiv zustimmen.

12. Kontrollrechte des Auftraggebers
Der Auftragnehmer gestattet dem Auftraggeber oder dessen Datenschutzbeauftragten, sich nach Anmeldung zu Prüfzwecken in den Betriebsräumen zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung relevanten Datenschutzgesetze zu überzeugen. Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er z.B. bei der Prüfung Fehler oder Unregelmäßigkeiten feststellt.

13. Mitteilungspflichten des Auftragnehmers
Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen und Datenschutzfolgeabschätzungen.
Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

14. Weisungsbefugnis des Auftragsgebers
Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen schriftlich. Mündliche Weisungen werden erst beachtet, wenn sie schriftlich vom Auftraggeber bestätigen wurden. Wenn der Auftragnehmer der Ansicht ist, dass eine Weisung gegen Vorschriften zum Schutz personenbezogener Daten verstößt, hat der Auftragnehmer den Auftraggeber unverzüglich darauf hinzuweisen.

15. Kopien, Löschung und Rückgabe von personenbezogenen Daten
Kopien der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind Sicherheitskopien, soweit sie für die Gewährleistung einer ordnungsgemäßen Datenverarbeitung notwendig sind, sowie Daten, die im Hinblick auf die Einhaltung der gesetzlichen Aufbewahrungspflichten erforderlich sind.
Nach Beendigung der Auftragsdatenverarbeitung hat der Auftragnehmer sämtliche in seinem Besitz befindliche Unterlagen, Verarbeitungs- und Nutzungsergebnisse sowie aktive Datenbestände datenschutzgerecht zu vernichten, soweit dem keine gesetzlichen Pflichten entgegenstehen.

16. Salvatorische Klausel / Anwendbares Recht / Gerichtsstand
Änderungen und Ergänzungen dieser Vereinbarung bedürfen, bei sonstiger Ungültigkeit, der Schriftform. Diese Formvorschrift kann nur schriftlich außer Kraft gesetzt werden. Sollte eine der Bestimmungen dieses Vertrages unwirksam sein oder werden, so bleiben die übrigen Bestimmungen davon unberührt. Die unwirksame Bestimmung ist durch eine solche zu ersetzen, die der gewünschten Zielsetzung der unwirksamen Bestimmung am nächsten kommt.
XPS-Privatfinanz ist abgestellt auf Produkte und Steuerrecht der Bundesrepublik Deutschland, weshalb für die Nutzung bzw. auf diese Vereinbarung, bzw. auf die Frage des Zustandekommens der Vereinbarung und alle damit zusammenhängenden Fragen ausschließlich deutsches Recht Anwendung finden – die Anwendbarkeit des UN-Kaufrechts wird jedenfalls ausdrücklich ausgeschlossen; bei Streitigkeiten ist das sachlich zuständige Gericht in München anzurufen.

_____

Auftraggeber / Lizenznehmer: Firma, Name, Vorname | Datum | Stempel/Unterschrift

_____

Straße, Ort

Vertragsannahme:

_____

Datum | Auftragnehmer / XPS-Finanzsoftware GmbH