starfinanz

Auftragsformular SFirm
Durchführung von Auftragsarbeiten
E-Mail: fk-service@starfinanz.de
Faxnummer: 040 23728 - 169

Rechnungsanschrift

Instituts- / Firmenname	
Kundennummer (Bankleitzahl)	Abteilung
Ansprechpartner	Straße + Hausnummer
Postleitzahl + Ort	Telefon
E-Mail-Adresse	

Weitere Daten zu Ihrem Auftrag

Diese Angaben ermöglichen es unseren Supportmitarbeitern, Ihnen den bestmöglichen Service zu gewährleisten.

Falls der Auftrag auf einen **bereits bestehendes Ticket** zurückgeht, geben Sie bitte die Ticket-ID an:	

Falls dem Auftrag **KEIN** Ticket zugrunde liegt, beschreiben Sie bitte kurz das Problem bzw. den Grund des Auftrages:

Star Finanz-Software Entwicklung und Vertriebs GmbH
Grüner Deich 15 • 20097 Hamburg • Telefon +49 40 23728-0 • Telefax +49 40 23728-350 • www.starfinanz.de
Sitz der Gesellschaft: Hamburg • Amtsgericht Hamburg HRB 64916
Geschäftsführer: Jochen Balas (Vorsitzender der Geschäftsführung), Jens Rieken, Martin Tobies
Kreissparkasse Walsrode • BIC: NOLADE21WAL • IBAN: DE22251523750045259199
Sparkasse Harburg-Buxtehude • BIC: NOLADE21HAM • IBAN: DE13207500000000072702
Sparkasse Hildesheim Goslar Peine • BIC: NOLADE21HIK • IBAN: DE31259501300000785736
Sparkasse Hannover • BIC: SPKHDE2HXXX • IBAN: DE17250501800000225320

Ein Unternehmen der Finanz Informatik

starfinanz

Vertragsunterzeichnung

☐ Hiermit beauftragen wir verbindlich, unter Anerkennung der AGB die Durchführung der vereinbarten Arbeiten für **131,25 € pro angefangener Arbeitsstunde zuzüglich ges. MwSt**.

Es gelten die Geschäftsbedingungen der Star Finanz GmbH, die unter https://www.starfinanz.de/index.php?id=agb einsehbar sind.

Die für den Auftrag ggf. erforderlichen Kunden-Dateien werden zwischen dem Kunden und der Star Finanz per Upload / Download zur Verfügung gestellt. Die Zugangsdaten werden nach Auftragseingang durch die Star Finanz gesondert per E-Mail mitgeteilt.

Wir bestätigen darüber hinaus, die Leistungsbeschreibung für die Durchführung von Auftragsarbeiten gelesen zu haben und akzeptieren diese vollumfänglich.

Datum, Ort Unterschrift

Leistungsbeschreibung für die Durchführung von Auftragsarbeiten

- Werden für die Durchführung des Auftrages Datensicherungen des Kunden benötigt, müssen diese mindestens SFirm-Version 4.x entsprechen (es muss ggf. vorher ein Programmupdate durchgeführt werden)
- Beauftragte Arbeiten werden von uns mit größter Sorgfalt durchgeführt und nach dem Stand der Technik auf Korrektheit überprüft. Datenverluste sind trotzdem nicht auszuschließen.
- Für Schäden und Datenverluste, die sich aus der Leistung ergeben, sowie für beiläufige Schäden oder Folgeschäden sind alle Haftungsansprüche ausdrücklich ausgeschlossen.
- Die Berechnung erfolgt nach Aufwand pro Stunde.
- Wir übernehmen keinerlei Kosten, die auf Ihrer Seite, z.B. durch Hinzuziehen eines externen Dienstleisters, entstehen.

Wichtiger Hinweis zum Datenschutz

Wenn wir von Ihnen im Rahmen einer beauftragten Supportleistung Kenntnis von personenbezogenen Daten erhalten bzw. einsehen könnten, ist es in einem solchen Fall und in Übereinstimmung mit den datenschutzrechtlichen Bestimmungen nötig, einen AVV (Auftragsverarbeitungsvertrag) mit uns abzuschließen.

Im Hinblick auf einen solchen Supportfall haben wir uns erlaubt, den notwendigen Auftragsverarbeitungsvertrag („AVV“) nebst Anlagen („AVA“) diesem Formular als Anlage beizufügen. Bitte ergänzen Sie in der Anlage AVA-Kommunikation unter den Punkten 1, 3 und 5 vor dem Rückversand an uns die notwendigen Angaben, fügen die Adresse Ihres Hauses auf den Seiten 1 und 6 ein, unterschreiben Sie bitte die Dokumente und schicken Sie uns diese entweder postalisch in zweifacher Ausfertigung oder digital per E-Mail zu. Wir werden diese gegenzeichnen und Ihnen ein Exemplar zukommen lassen.

Auftragsverarbeitungsvertrag

Zwischen

(kurz: „**Auftraggeber**“)

und

Star Finanz-Software Entwicklung und Vertriebs GmbH
Grüner Deich 15, 20097 Hamburg

(kurz: „**Auftragnehmer**“)

Präambel

P.1. Auftraggeber und Auftragnehmer sehen sich den hohen Standards verpflichtet, die innerhalb der Sparkassen-Finanzgruppe im Hinblick auf den Datenschutz gelten.

P.2. Der vorliegende **A**uftrags**v**erarbeitungs**v**ertrag (kurz: „**AVV**“) konkretisiert für alle Verarbeitungen die Rechte und Pflichten der Parteien auf dem Gebiet des Datenschutzes, welche sich aus den zwischen den Parteien bereits oder künftig bestehenden rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnissen (kurz: „**Hauptvertrag**“) ergeben.

§ 1 Auftrag und Spezifika der Verarbeitung

1.1. Der AVV kommt mit all seinen Teilen zur Anwendung, sofern und soweit der Auftraggeber den Auftragnehmer zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (kurz: „**Daten**“) verpflichtet hat.

1.2. Der AVV bildet den Rahmen für eine Vielzahl unterschiedlicher Vorgänge der Auftragsverarbeitung.

1.3. Bei etwaigen Widersprüchen gehen die Regelungen dieses AVV und all seiner Teile den Regelungen des zugehörigen Hauptvertrages vor.

1.4. Die für einzelne Verarbeitungen geltenden spezifischen datenschutzrechtlichen Festlegungen (kurz: „**Spezifika**“) werden vor Beginn der Verarbeitung in Anlagen zum AVV (kurz: „**AVA**“) geregelt. Dies sind insbesondere Gegenstand und Dauer sowie Art und Zweck der Verarbeitung, die Kategorie der Daten und die Kategorien betroffener Personen sowie die technischen und organisatorischen Maßnahmen (kurz: „**TOM**“).

1.5. Die AVA sind Teil des AVV. Bei etwaigen Widersprüchen gehen die Regelungen der AVA der allgemeineren Regelung im AVV vor. Wird im Folgenden oder in den AVA auf den AVV Bezug genommen, so ist der AVV mit allen seinen Teilen gemeint.

§ 2 Verantwortlichkeit und Verarbeitung auf Weisung

2.1. Der Auftraggeber ist im Rahmen dieses AVV für die Einhaltung der anwendbaren gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Offenlegung gegenüber dem Auftragnehmer sowie für die Rechtmäßigkeit der Verarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

2.2. Der Auftragnehmer handelt ausschließlich weisungsgebunden, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a DSGVO vor (anderweitige gesetzliche Verarbeitungspflicht). Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

2.3. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten oder schränkt deren Verarbeitung ein (kurz: „**Sperrung**“), wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist.

2.4. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Vorschriften über den Datenschutz verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis diese vom Auftraggeber in Textform bestätigt oder abgeändert wurde. Die Ausführung offensichtlich datenschutzrechtswidriger Weisungen darf der Auftragnehmer jederzeit ablehnen.

2.5. Die Parteien benennen in Textform gegenseitig einen oder mehrere Ansprechpartner in datenschutzrechtlichen Angelegenheiten, einschließlich der bestellten Datenschutzbeauftragten. Ergeben sich bei den Ansprechpartnern Änderungen, haben sich die Parteien hierüber in Textform zu informieren.

2.6. Der Auftragnehmer gewährleistet, dass die zur Verarbeitung der Daten befugten Personen die Weisungen des Auftraggebers kennen und diese beachten.

2.7. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits- und Verschwiegenheitspflicht besteht auch nach Beendigung der Verarbeitung fort.

2.8. Der Auftragnehmer hat bei der Verarbeitung im Auftrag das Bankgeheimnis zu wahren, soweit der Auftraggeber dem Bankgeheimnis unterworfen ist. Hierauf wird der Auftraggeber den Auftragnehmer hinweisen, sofern dies für den Auftragnehmer aus dem Hauptvertrag nicht ersichtlich ist. Das Bankgeheimnis erstreckt sich auf alle personenbezogenen Daten und anderen Informationen, die dem Auftraggeber über seine Kunden, Interessenten oder über Dritte aus der Geschäftsbeziehung zu diesen bekannt werden. Unter das Bankgeheimnis fällt auch die Angabe, ob der Auftraggeber überhaupt eine Geschäftsbeziehung zu einem Kunden unterhält.

§ 3 Sicherheit der Verarbeitung

3.1. Die Parteien vereinbaren TOM gemäß Art. 32 DSGVO zum angemessenen Schutz der Daten, (kurz: „**AVA TOM**“).

3.2. Änderungen der vereinbarten TOM bleiben dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau insgesamt nicht unterschritten wird. Wesentliche Änderungen sind dem Auftraggeber in Textform mitzuteilen.

3.3. Trifft der Auftraggeber eigene technische und organisatorische Maßnahmen für eine auf den Auftragnehmer übertragene Datenverarbeitung, so hat ihn der Auftragnehmer im Rahmen seiner Möglichkeiten hierbei zu unterstützen.

§ 4 Unterrichtung bei Datenschutzverletzungen und Fehlern der Verarbeitung

4.1. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der ihm vom Auftraggeber offengelegten Daten im Sinne des Art. 4 Nr. 12 DSGVO in seinem Organisationsbereich bekannt werden oder ein konkreter Verdacht einer solchen Datenschutzverletzung beim Auftragnehmer besteht.

4.2. Stellt der Auftraggeber Fehler bei der Verarbeitung fest, hat er den Auftragnehmer unverzüglich hierüber zu unterrichten.

4.3. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Behebung der Datenschutzverletzung gemäß § 4.1 oder der Fehler gemäß § 4.2 sowie zur Minderung möglicher nachteiliger Folgen, insbesondere für die betroffenen Personen. Hierüber stimmt er sich mit dem Auftraggeber ab. Mündliche Unterrichtungen gemäß § 4.1 oder § 4.2 sind unverzüglich in Textform nachzureichen.

§ 5 Übermittlung von Daten an einen Empfänger in einem Drittland

Die Übermittlung von Daten an einen Empfänger in einem Drittland außerhalb von EU und EWR ist unter den in Art. 44 ff. DSGVO geschriebenen Bedingungen zulässig. Einzelheiten werden in einem oder mehreren AVA geregelt.

§ 6 Unterbeauftragung weiterer Auftragsverarbeiter

6.1. Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (kurz: „**Unterauftragnehmer**“) erbringen lassen.

6.2. Der Auftragnehmer informiert den Auftraggeber in Textform rechtzeitig vorab über die Beauftragung von Unterauftragnehmern oder Änderungen in der Unterbeauftragung. Der Auftraggeber kann bei Vorliegen eines wichtigen Grundes der Unterbeauftragung innerhalb von vier Wochen nach Kenntnisnahme in Textform widersprechen. Ein wichtiger Grund liegt insbesondere vor, wenn ein begründeter Anlass zu Zweifeln besteht, dass der Unterauftragnehmer die vereinbarte Leistung entsprechend den anwendbaren gesetzlichen Bestimmungen zum Datenschutz oder gemäß dieser AVV erbringt.

6.3. Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden technischen und organisatorischen Maßnahmen mindestens dasselbe Schutzniveau aufweisen.

6.4. Keine Unterbeauftragungen im Sinne dieser Regelung sind Leistungen, die der Auftragnehmer als reine Nebenleistung zur Unterstützung seiner geschäftlichen Tätigkeit außerhalb der Auftragsverarbeitung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes der Daten auch für solche Nebenleistungen angemessene Vorkehrungen zu ergreifen.

§ 7 Sonderkündigungsrecht des Auftraggebers bei Widerspruch der beauftragenden Stelle

Erfolgt die Beauftragung des Auftragnehmers als Unterauftragsverarbeitung des Auftraggebers, so steht der beauftragenden Stelle des Auftraggebers ein Widerspruchsrecht nach Art. 28 (2) DSGVO zu. Dieses Widerspruchsrecht besteht für einen Zeitraum von 4 Wochen ab Kenntnisnahme der beauftragenden Stelle über die Unterbeauftragung des Auftragnehmers. Sollte die beauftragende Stelle binnen der vorgenannten Frist von diesem Widerspruchsrecht gegenüber dem Auftraggeber Gebrauch machen, so steht dem Auftraggeber ein fristloses Sonderkündigungsrecht dieses Vertrages und der zugehörigen Beauftragung des Auftragnehmers zu.

§ 8 Rechte betroffener Personen und Unterstützung des Auftraggebers

Macht eine betroffene Personen Ansprüche gemäß Kapitel III der DSGVO bei einer der Parteien geltend, so informiert sie die jeweils andere Partei darüber unverzüglich. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Bearbeitung solcher Anträge sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

§ 9 Kontroll- und Informationsrechte des Auftraggebers

9.1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung seiner Pflichten mit geeigneten Mitteln nach. Der Auftraggeber überprüft die Geeignetheit.

9.2. Für die Überprüfung der Einhaltung der vereinbarten Schutzmaßnahmen nach § 9.1 und deren geprüfter Wirksamkeit kann der Auftragnehmer auf angemessene Zertifizierungen oder andere geeignete Prüfungsnachweise verweisen. Angemessen sind insbesondere Zertifizierungen nach Art. 40 DSGVO oder Nachweise nach Art. 42 DSGVO. Daneben kommen unter anderem in Betracht: eine Zertifizierung nach SITB (Sicherer IT-Betrieb der Sparkassen-Finanzgruppe), eine Zertifizierung nach ISO 27001 oder ISO 27017, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, eine Zertifizierung nach anerkannten und geeigneten Branchenstandards oder ein Prüfungsnachweis gemäß SOC / PS 951. Die Zertifizierungs- und Prüfungsverfahren sind von einem anerkannten unabhängigen Dritten

durchzuführen. Der Auftragnehmer hat seine Zertifikate oder Prüfungsnachweise zur Verfügung zu stellen. Des Weiteren können andere geeignete Mittel (z.B. Tätigkeitsberichte des Datenschutzbeauftragten oder Auszüge aus Berichten der Wirtschaftsprüfer) zum Nachweis der Einhaltung der vereinbarten Schutzmaßnahmen dem Auftraggeber zur Verfügung gestellt werden. Das Inspektionsrecht des Auftraggebers aus § 9.3 bleibt hiervon unberührt.

9.3. Der Auftraggeber ist berechtigt, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs, regelmäßig nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit, Inspektionen beim Auftragnehmer zur Prüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durchzuführen. Der Auftragnehmer darf die Inspektion von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der von ihm getroffenen technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen die Beauftragung dieses Prüfers ein Einspruchsrecht.

9.4. Zur Behebung der bei einer Inspektion getroffenen Feststellungen stimmen die Parteien umzusetzende Maßnahmen ab.

9.5. Macht eine Aufsichtsbehörde von Befugnissen nach Art. 58 DSGVO Gebrauch, so informieren sich die Parteien hierüber unverzüglich. Sie unterstützen sich in ihrem jeweiligen Verantwortungsbereich, bei Erfüllung der gegenüber der jeweiligen Aufsichtsbehörde bestehenden Verpflichtungen.

§ 10 Haftung und Schadenersatz

10.1. Macht eine betroffene Person gegenüber einer Partei Schadenersatzansprüche wegen Verstoßes gegen datenschutzrechtliche Bestimmungen geltend, so hat die beanspruchte Partei die andere Partei hierüber unverzüglich zu informieren.

10.2. Auftraggeber und Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

10.3. Die Parteien unterstützen sich wechselseitig bei der Abwehr von Schadenersatzansprüchen betroffener Personen, es sei denn, dies würde die Rechtsposition der einen Partei im Verhältnis zur anderen Partei oder zur Aufsichtsbehörde gefährden.

§ 11 Laufzeit

11.1. Der AVV wird auf unbestimmte Zeit geschlossen. Die Laufzeit einer AVA wird in der AVA selbst geregelt; ohne eine solche Regelung entspricht die Laufzeit einer AVA derjenigen des AVV.

11.2. Der AVV kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden, wenn gleichzeitig oder zuvor alle AVA beendet wurden.

11.3. Eine AVA endet mit Beendigung des zugehörigen Hauptvertrags, ohne dass es einer gesonderten Kündigung dieser AVA bedarf. Der Auftragnehmer hat in diesem Fall nach Wahl des Auftraggebers unverzüglich die nach der AVA verarbeiteten Daten herauszugeben oder datenschutzkonform zu löschen und dies dem Auftraggeber in Textform (z. B. durch ein Löschprotokoll) zu bestätigen. Sofern der Auftragnehmer eine eigene gesetzliche Pflicht zur Speicherung dieser Daten hat, hat er dies dem Auftraggeber in Textform anzuzeigen.

§ 12 Schlussbestimmungen

12.1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber in Textform zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich in Textform darüber informieren, dass die Verantwortung für die Daten ausschließlich beim Auftraggeber liegt.

12.2. Mündliche Nebenabreden wurden nicht getroffen. Änderungen und Ergänzungen des AVV bedürfen zu ihrer Wirksamkeit der Textform und der ausdrücklichen Bezugnahme auf die AVV. Abweichende mündliche Abreden der Parteien sind unwirksam. Dies gilt auch für Änderungen dieser Klausel.

12.3. Sollte auch nur eine Bestimmung dieser Vereinbarung ganz oder teilweise rechtsunwirksam oder nichtig sein oder werden, bleibt dieser AVV im Übrigen gleichwohl aufrechterhalten und gültig. An Stelle der rechtsunwirksamen oder nichtigen Bestimmung gilt das Gesetz, sofern die hierdurch entstandene Lücke nicht durch ergänzende Vertragsauslegung gemäß §§ 133, 157 BGB geschlossen werden kann. Beide Parteien sind jedoch insoweit verpflichtet, unverzüglich eine rechtswirksame und datenschutzkonforme Vertragsergänzung abzustimmen und zu erstellen.

12.4. Es gilt deutsches Recht.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer (Star Finanz)
_____	_____
Name, Funktion Unterzeichner (in Druckbuchstaben)	Name, Funktion Unterzeichner (in Druckbuchstaben)

Auftragsverarbeitungsvertrag Anlage (AVA): Kommunikation

zwischen

(kurz: „**Auftraggeber**“)

Und

Star Finanz-Software Entwicklung und Vertriebs GmbH
Grüner Deich 15, 20097 Hamburg

(kurz: „**Auftragnehmer**“)

Die Parteien treffen zum Vertrag über die Auftragsverarbeitung (nachfolgend „**AVV**“) mit dieser AVA ergänzend für die Kommunikation der Parteien untereinander folgende Festlegungen:

1 Datenschutzbeauftragter beim Auftraggeber

☐ Datenschutzbeauftragter des Auftraggebers ist:

Name, Vorname:	
Anschrift:	
Telefon-Nummer:	
Fax-Nummer:	
E-Mail-Adresse:	

Vorrangiger Kommunikationsweg ist:

☐ E-Mail ☐ Post ☐ Fax ☐ Telefon

☐ Der Auftraggeber hat keinen Datenschutzbeauftragten benannt.

2 Datenschutzbeauftragter beim Auftragnehmer

☒ Datenschutzbeauftragter des Auftragnehmers ist:

Name, Vorname:	RA/StB Brigitte Colberg
Anschrift:	Star Finanz GmbH, Grüner Deich 15, 20097 Hamburg
Telefon-Nummer:	040/23728-343
Fax-Nummer:	040/23728-350
E-Mail-Adresse:	brigitte.colberg.extern@starfinanz.de

Vorrangiger Kommunikationsweg ist:

☒ E-Mail ☐ Post ☐ Fax ☐ Telefon

☐ Der Auftragnehmer hat keinen Datenschutzbeauftragten benannt.

3 Operativer und fachlicher Ansprechpartner und Stellvertreter beim Auftraggeber für den AVV[1]

☐ Ansprechpartner des Auftraggebers für die operative und fachliche Betreuung des AVV ist:

Name, Vorname:	
Anschrift:	
Telefon-Nummer:	
Fax-Nummer:	
E-Mail-Adresse:	

☐ Stellvertretender Ansprechpartner des Auftraggebers für die operative und fachliche Betreuung des AVV ist:

Name, Vorname:	
Anschrift:	
Telefon-Nummer:	
Fax-Nummer:	
E-Mail-Adresse:	

Vorrangiger Kommunikationsweg ist jeweils:

☐ E-Mail ☐ Post ☐ Fax ☐ Telefon ☐ Ticketsystem nach dem Hauptvertrag

4 Operativer und fachlicher Ansprechpartner und Stellvertreter beim Auftragnehmer für den AVV[2]

☒ Ansprechpartner des Auftragnehmers für die operative und fachliche Betreuung des AVV ist:

Name, Vorname:	Krukemeyer, Oliver
Anschrift:	Star Finanz GmbH, Grüner Deich 15, 20097 Hamburg
Telefon-Nummer:	040/23728-599
Fax-Nummer:	040/23728-169
E-Mail-Adresse:	oliver.krukemeyer@starfinanz.de

☒ Stellvertretender Ansprechpartner des Auftragnehmers für die operative und fachliche Betreuung des AVV ist:

Name, Vorname:	Hamela, Martin
Anschrift:	Star Finanz GmbH, Grüner Deich 15, 20097 Hamburg
Telefon-Nummer:	040/23728-500
Fax-Nummer:	040/23728-169
E-Mail-Adresse:	martin.hamela@starfinanz.de

Vorrangiger Kommunikationsweg ist jeweils:

☒ E-Mail ☐ Post ☐ Fax ☐ Telefon ☐ Ticketsystem nach dem Hauptvertrag

---

[1] Der Datenschutzbeauftragte hat gemäß Art. 39 Abs. 1 DSGVO vornehmlich eine beratende und überwachende Funktion. Deshalb sollte der Datenschutzbeauftragte in der Regel nicht der Ansprechpartner für vertragliche Fragen sein. Ansprechpartner für den AVV sollte stattdessen jeweils eine Person sein, die operativ und fachlich für die Betreuung des AVV zuständig ist. Deshalb werden die Daten zum Datenschutzbeauftragten einerseits sowie zum fachlichen und operativen Ansprechpartner andererseits (nebst Stellvertreter) separat erfasst. Zur Abgrenzung wird auf die kommenden Ausführungen im ROLF zum Datenschutzmanagement verwiesen.

[2] Siehe Fußnote 1.

5 Weisungsberechtigte Personen beim Auftraggeber[3]

☐ Weisungsberechtigt sind die in Ziff. 3 genannten Ansprechpartner.

☐ Weisungsberechtigt sind die folgenden Personen:

Name, Vorname:	
Anschrift:	
Telefon-Nummer:	
Fax-Nummer:	
E-Mail-Adresse:	

Name, Vorname:	
Anschrift:	
Telefon-Nummer:	
Fax-Nummer:	
E-Mail-Adresse:	

Vorrangiger Kommunikationsweg für die Erteilung von Weisungen ist:

☐ E-Mail ☐ Post ☐ Fax ☐ Ticketsystem nach dem Hauptvertrag

6 Weisungsempfänger beim Auftragnehmer[4]

☒ Weisungsempfänger sind die in Ziff. 4 genannten Ansprechpartner.

Der vorrangige Kommunikationsweg für den Empfang von Weisungen ergibt sich aus Ziff. 5.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer (Star Finanz)
_____	_____
Name, Funktion Unterzeichner (in Druckbuchstaben)	Name, Funktion Unterzeichner (in Druckbuchstaben)

[3] Sollen mehrere Ansprechpartner weisungsberechtigt sein, sind mehrere Checkboxen anzukreuzen. Anderenfalls ist jeweils nur die passende Checkbox anzukreuzen.

[4] Siehe Fußnote 3

AVA-Formblatt

1. Gegenstand der Verarbeitung (des Auftrags)

☐ Der Gegenstand des Auftrags ergibt sich aus dem schriftlichen Hauptvertrag [**Bezeichnung**] vom [**Datum**].

☐ Der Gegenstand des Auftrags ergibt sich aus [**sonstigen schriftlichen Dokumenten**] vom [**Datum**].

☒ Gegenstand des Auftrags ist: Umsetzung der beauftragten Support-Leistung

2. Dauer des Auftrags

☒ Die Dauer des Auftrags ergibt sich aus der schriftlich beauftragten Supportleistung**.**

☐ Der Auftrag beginnt am **[Datum]** und endet am **[Datum]**.

☐ Der Auftrag beginnt mit Unterzeichnung dieses Vertrags und wird auf unbestimmte Zeit geschlossen. Er ist mit einer Frist von [**Angabe einer Frist**] kündbar. Die Möglichkeit zur fristlosen Kündigung aus besonderem Grund bleibt hiervon unberührt.

☐ Der Auftrag wird zur einmaligen Ausführung in folgendem Zeitraum geschlossen: **[Angabe eines konkreten Zeitraums]**

3. Zweck der Verarbeitung

Die Tätigkeit des Auftragnehmers dient folgenden vereinbarten Zwecken:

☒ Unterstützung von Kunden und Geschäftspartnern bei der Durchführung von Verträgen oder Aufträgen

☒ Versand von Waren / Erbringung von Dienstleistungen

☒ Betreuung von Kunden und Geschäftspartnern

☐ Kundenbefragungen im Rahmen von Markt- und Meinungsforschung

<u>Zwecke der Buchhaltung (Finance)</u>

☐ Gewährleistung der ordentlichen und gesetzeskonformen Buchhaltung

☐ Rechnungsstellung für bezogene Waren / Dienstleistungen

<u>Zwecke der Personalverwaltung (HR)</u>

☐ Pflege und Verwaltung von Mitarbeiterdaten

☐ Angestelltenentwicklungsplanung

☐ Dokumentation von Arbeitszeiten

☐ Zahlung von Gehältern und Löhnen

☐ Planung und Verwaltung von Fortbildungs- und Trainingsmaßnahmen

☐ Mitarbeiterbeurteilung / Leistungsbewertung

☐ Verwaltung von Kompetenzen und Qualifikationen der Mitarbeiter/Innen

☐ Verwaltung von Bewerbungen

☐ Dokumentation und Festlegung von Compensations und Benefits

Zwecke des Gebäudemanagements (Facillity)

☐ Überwachung betrieblicher Einrichtungen

☐ Gewährleistung des Zutrittschutzes

☐ Ermöglichung der Verfolgung von Straftaten

☐ Wahrnehmung des Hausrechts

☐ Gewährleistung der ordnungsgemäßen Akten- und Datenträgervernichtung

Zwecke der EDV / IT

☐ Kommunikation mittels elektronischer Medien

☐ Ermöglichung der Kontaktierung von Mitarbeitern/Innen

☐ Dokumentation von Terminen von Mitarbeitern/Innen

☐ Zugangsverwaltung hinsichtlich IUK-Technik und Unternehmensnetzwerk

☐ Verwaltung von Berechtigungen

☐ Verwaltung von Softwarelizenzen

☐ Telekommunikationskostenabrechnung

Sonstige Zwecke

☐ Pflege und Verbesserung von Kommunikationsprozessen

☐ Reisebuchung und –kostenabrechnung

☐ Qualitätssicherung

☒ Weitere: Erbringung von Supportleistungen

4. Datenarten / -kategorien

Folgende Datenarten sind Gegenstand dieses Auftrags:		
☒ Adressdaten	☐ Gesundheitsdaten	☐ Personal- und Identifikationsnummern
☐ Alter	☒ Kreditkartendaten	☐ Reisebuchungs- und -abrechnungsdaten
☐ Arbeitszeitdaten	☐ Kundenverhal-tensdaten	☐ Telekommunikations-abrechnungsdaten
☐ Audiodaten	☒ Lohn- und Gehaltsdaten	☐ Telekommunikations-verbindungsdaten
☒ Bankverbindungsdaten inkl. Zahlungsverkehrsdaten	☐ Mitarbeiter-bewertungen	☒ Telefonnummern
☐ Bewerberdaten	☐ Mitarbeiter-qualifikationen und -eigenschaften	☐ Vertragsdaten
☐ Bilddaten	☒ Namen	☐ Videodaten
☐ Hobbys	☒ Nutzerkennungen	☒ Zahlungsdaten
☒ E-Mails	☒ Passwörter	☒ Zugangsdaten
☒ sonstige: Ggfs. alle, die beim Auftraggeber gespeicherten und die für die Abwicklung des Auftrags benötigten Daten.		

5. Kreis der Betroffenen

Folgende Kategorien von Betroffenen sind Gegenstand des Auftrags:

☒ Beschäftigte

☒ Auszubildende und Praktikanten

☐ Bewerber

☐ ehemalige Arbeitnehmer

☒ freie Mitarbeiter

☐ Gesellschafter

☐ Angehörige von Beschäftigten

☒ Kunden

☐ Interessenten

☒ Lieferanten und Dienstleister

☐ Mieter

☒ Geschäftspartner

☐ externe Berater

☐ Besucher

☐ Pressevertreter

☒ sonstige: Ggfs. alle, die mit dem Aufraggeber geschäftlich zusammenarbeiten

6. Besondere technische und organisatorische Maßnahmen

☐ Besonders abgegrenzte oder geschützte Gebäudeteile

☐ Besonders restriktiver Zugriff (restriktive Rollenvergabe, VAP, …)

☐ Spezielle Protokolle

☐ Besondere Maßnahmen der Verschlüsselung

☐ Trusted Employee-Bereich

☐ Besondere Kameraüberwachung

☐ Zusätzliche Backups / Ausfallrechenzentrum im Salzstock / …

☐ Leckage-System

☐ Sonstiges: [Bitte ergänzen]

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschriften	Unterschriften (Star Finanz)
_____	_____
Name, Funktion Unterzeichner (in Druckbuchstaben)	Name, Funktion Unterzeichner (in Druckbuchstaben)

AVA-TOM

Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Zutrittskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- ☒ Zutrittskontrollsystem, Ausweisleser (Magnet-/Chipkarte)
- ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.)
- ☒ Sicherheitstüren / -fenster
- ☐ Gitter vor Fenstern/Türen
- ☐ Zaunanlagen
- ☒ Schlüsselverwaltung/Dokumentation der Schlüsselvergabe
- ☐ Werkschutz, Pförtner
- ☒ Alarmanlage
- ☒ Videoüberwachung
- ☐ Spezielle Schutzvorkehrungen des Serverraums
- ☒ Spezielle Schutzvorkehrungen für die Aufbewahrung von Back-Ups und/oder sonstigen Datenträgern
- ☒ Nicht-reversible Vernichtung von Datenträgern
- ☐ Mitarbeiter- und Berechtigungsausweise
- ☐ Sperrbereiche
- ☐ Besucherregelung (Bspw. Abholung am Empfang, Dokumentation von Besuchszeiten, Besucherausweis, Begleitung nach dem Besuch bis zum Ausgang)
- ☐ sonstiges:

b) Zugangskontrolle || Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben.

- ☒ Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Unternehmensnetzwerk
- ☒ Autorisierungsprozess für Zugangsberechtigungen
- ☒ Begrenzung der befugten Benutzer
- ☐ Single Sign-On
- ☒ BIOS-Passwörter
- ☒ Kennwortverfahren (Angabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall)
- ☒ Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff
- ☐ Personalisierte Chipkarten, Token, PIN-/TAN, etc.
- ☒ Protokollierung des Zugangs
- ☒ Zusätzlicher System-Log-In für bestimmte Anwendungen
- ☒ Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung)
- ☒ Firewall
- ☒ sonstiges: Verbindlicher Einsatz von ssh public-key Authentisierung für den Zugang zu Linux-Systemen

c) Zugriffskontrolle || Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben.

- ☒ Verwaltung und Dokumentation von differenzierten Berechtigungen
- ☒ Abschluss von Verträgen zur Auftragsdatenverarbeitung für die externe Pflege, Wartung und Reparatur von Datenverarbeitungsanlagen, sofern bei der Fernwartung die Verarbeitung von pbD, also der Umgang mit personenbezogenen Daten, Gegenstand der Dienstleistung ist.
- ☒ Auswertungen/Protokollierungen von Datenverarbeitungen
- ☒ Autorisierungsprozess für Berechtigungen
- ☒ Genehmigungsroutinen
- ☒ Profile/Rollen
- ☒ Verschlüsselung von CD/DVD- ROM, externen Festplatten und/oder Laptops (etwa per Betriebssystem, TrueCrypt, Safe Guard Easy, WinZip, PGP)
- ☐ Maßnahmen zur Verhinderung unbefugten Überspielens von Daten auf extern verwendbare Datenträger (z.B. Kopierschutz, Sperrung von USB-Ports, „Data Loss Prevention (DLP)-System“)
- ☒ „Mobile Device Management-System“
- ☒ Vier-Augen-Prinzip
- ☒ Funktionstrennung „Segregation of Duties“
- ☒ Fachkundige Akten- und Datenträgervernichtung gemäß DIN 66399
- ☒ Nicht-reversible Löschung von Datenträgern
- ☐ Sichtschutzfolien für mobile Datenverarbeitungssysteme
- ☐ sonstiges:

d) Trennungskontrolle || Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- ☒ Speicherung der Datensätze in physikalisch getrennten Datenbanken
- ☒ Verarbeitung auf getrennten Systemen
- ☒ Zugriffsberechtigungen nach funktioneller Zuständigkeit
- ☒ Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen
- ☒ Mandantenfähigkeit von IT-Systemen
- ☒ Verwendung von Testdaten
- ☒ Trennung von Entwicklungs- und Produktionsumgebung
- ☐ sonstiges:

e) Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO) || Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten 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.

Es erfolgt keine Pseudonymisierung, da dies nicht vereinbart ist.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

a) Weitergabekontrolle || Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- ☒ Verschlüsselung von Email bzw.- Email-Anhängen (z.B. WinZip)
- ☒ Verschlüsselung des Speichermediums von Laptops
- ☒ Gesicherter File Transfer (z.B. sftp)
- ☒ Gesicherter Datentransport (z.B. SSL, ftp, ftps, TLS)
- ☒ Verschlüsselung von CD/DVD- ROM, externen Festplatten oder USB-Sticks (z.B. True Crypt, Safe Guard Easy, PGP)
- ☐ Physikalische Transportsicherung
- ☐ Verpackungs- und Versandvorschriften
- ☐ Elektronische Signatur
- ☒ Gesichertes WLAN
- ☒ Fernwartungskonzept (z.B. Verschlüsselung, Ereignisauslösung durch Auftraggeber, Challenge-Response, Rückrufautomatik, Einmal-Passwort)
- ☒ „Mobile Device Management-System“
- ☐ „Data Loss Prevention (DLP)-System“
- ☒ Regelung zum Umgang mit mobilen Speichermedien (z.B. Laptop, USB-Stick, Mobiltelefon)
- ☒ Protokollierung von Datenübertragung oder Datentransport
- ☐ Protokollierung von lesenden Zugriffen
- ☐ Protokollierung des Kopierens, Veränderns oder Entfernens von Daten
- ☒ Getunnelte Datenfernverbindungen (VPN = Virtuelles Privates Netzwerk)
- ☐ sonstiges:

b) Eingabekontrolle || Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat.

- ☒ Zugriffsrechte
- ☒ Systemseitige Protokollierungen
- ☐ Dokumenten Management System (DMS) mit Änderungshistorie
- ☐ Sicherheits-/Protokollierungssoftware
- ☒ Funktionelle Verantwortlichkeiten, organisatorisch festgelegte Zuständigkeiten
- ☒ Mehraugenprinzip
- ☐ „Data Loss Prevention (DLP)-System“
- ☐ sonstiges:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle und Belastbarkeitskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind.

- ☒ Sicherheitskonzept für Software- und IT-Anwendungen
- ☒ Back-Up Verfahren
- ☒ Aufbewahrungsprozess für Back-Ups (brandgeschützter Safe, getrennter Brandabschnitt, etc.)
- ☒ Gewährleistung der Datenspeicherung im gesicherten Netzwerk
- ☒ Bedarfsgerechtes Einspielen von Sicherheits-Updates

- ☒ Spiegeln von Festplatten
- ☒ Einrichtung einer unterbrechungsfreien Stromversorgung (USV)
- ☒ Geeignete Archivierungsräumlichkeiten für Papierdokumente
- ☐ Brand- und/oder Löschwasserschutz des Serverraums
- ☐ Brand- und/oder Löschwasserschutz der Archivierungsräumlichkeiten
- ☒ Klimatisierter Serverraum
- ☒ Virenschutz
- ☒ Firewall
- ☒ Notfallplan
- ☒ Erfolgreiche Notfallübungen
- ☒ Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage)
- ☒ sonstige: Einsatz von Virtualisierungs-Technologie mit automatischem Fail-Over

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

a) Datenschutz-Management || Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- ☐ Datenschutzleitbild der Sparkassen Finanzgruppe
- ☐ Datenschutz-Richtlinie der Sparkassen Finanzgruppe
- ☒ Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit
- ☒ Bestellung eines Datenschutzbeauftragten
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis und Bankgeheimnis
- ☒ Hinreichende Schulungen der Mitarbeiter in Datenschutzangelegenheiten
- ☒ Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- ☒ Durchführung von Datenschutzfolgenabschätzungen, soweit erforderlich (Art. 35 DS-GVO)
- ☐ Ext. Prüfung/Auditierung der Informationssicherheit (etwa im Rahmen von ISO-Zertifizierung, SOX-Compliance)
- ☒ sonstige: Durchführung von internen Audits nach dem Standard Sicherer IT-Betrieb (SITB)

b) Incident-Response-Management ||Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- ☐ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden (Art. 33 DS-GVO)
- ☒ Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Betroffenen (Art. 34 DS-GVO)
- ☐ sonstige:

c) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO) ||

Die default Einstellungen sind sowohl bei den standardisierten Voreinstellungen von Systemen und Apps als auch bei der Einrichtung der Datenverarbeitungsverfahren zu berücksichtigen. In dieser Phase werden Funktionen und Rechte konkret konfiguriert, wird im Hinblick auf Datenminimierung die Zulässigkeit bzw. Unzulässigkeit bestimmter Eingaben bzw. von Eingabemöglichkeiten (z. B. von Freitexten) festgelegt und über die Verfügbarkeit von Nutzungsfunktionen entschieden (z. B. hinsichtlich des Umfangs der Verarbeitung). Ebenso werden die Art und der Umfang des Personenbezugs bzw. der Anonymisierung (z. B. bei Selektions-, Export- und Auswertungsfunktionen, die festgelegt und voreingestellt oder frei gestaltbar zur Verfügung gestellt werden können) oder die Verfügbarkeit von bestimmten Verarbeitungsfunktionen, Protokollierungen etc. festgelegt.

- ☒ Es werden nur die minimal für den Anwendungszweck erforderlichen Daten abgefragt, zusätzliche optionale Daten werden nicht als Pflichtfelder gekennzeichnet.
- ☒ Die Eingabe und Übertragung von Daten in Web-Formularen erfolgt grundsätzlich verschlüsselt.
- ☒ Es werden Integritätsprüfungen implementiert.

d) Auftragskontrolle || Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können.

- ☒ Vereinbarung zur Auftragsverarbeitung mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers
- ☒ Prozess zur Erteilung und/oder Befolgung von Weisungen
- ☒ Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern
- ☒ Kontrolle/Überprüfung weisungsgebundener Auftragsdurchführung
- ☒ Schulungen/Einweisung aller zugriffsberechtigten Mitarbeiter beim Auftragnehmer
- ☐ Unabhängige Auditierung der Weisungsgebundenheit
- ☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis
- ☐ Vereinbarung von Konventionalstrafen für Verstöße gegen Weisungen
- ☐ formalisiertes Auftragsmanagement
- ☐ dokumentiertes Verfahren zur Auswahl des Dienstleisters
- ☒ standardisiertes Vertragsmanagement zur Vor- und Nachkontrolle der Dienstleister
- ☐ sonstiges:

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschriften	Unterschrift Star Finanz
_____	_____
Name, Funktion Unterzeichner (in Druckbuchstaben)	Name, Funktion Unterzeichner (in Druckbuchstaben)