

Sonderbedingungen Datenschutz zum SFirm Nutzungs- und Servicevertrag bzw. StarMoney Business Abonnementvertrag

1. Gegenstand und Dauer des Auftrags

Die Sparkasse übernimmt entsprechend dieser Vereinbarung die Wartung und Pflege der Software SFirm bzw. StarMoney Business.

Gemäß Beschluss der deutschen Datenschutzaufsichtsbehörden sind auch im Falle der Wartung von Datenverarbeitungsanlagen oder automatisierter Verfahren die datenschutzrechtlichen Regeln über eine Auftragsverarbeitung anzuwenden.

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des SFirm Nutzungs- und Servicevertrages bzw. des StarMoney Business Abonnementvertrages.

2. Konkretisierung des Auftragsinhalts

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

Gegenstand der Verarbeitung personenbezogener Daten sind insbesondere Personenstammdaten, Vertragsstammdaten, Bankverbindungen, Konten, Zahlungstransaktionen und Buchungen.

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen insbesondere Kunden, Interessenten, Beschäftigte, Lieferanten und deren Ansprechpartner.

3. Technisch-organisatorische Maßnahmen

Die Sparkasse hat die angemessene Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus.

Die Datenverarbeitung findet ausschließlich auf den Systemen des Kunden statt. Die Sparkasse greift ausschließlich remote auf die Systeme des Kunden zu.

Bei den Zugriffen auf die Systeme des Kunden wird TeamViewer oder ein vergleichbares Remote-Access-System eingesetzt. Alle Mitarbeiter sind angewiesen im Rahmen des Remote-Access auf das SFirm- bzw. StarMoney Business-System des Kunden:

- a) Verbindungen nur unter Beteiligung des Kunden aufzubauen,
- b) nur verschlüsselte Verbindungen zum Kunden aufzubauen,
- c) keine Daten aus der SFirm- bzw. StarMoney Business-Software bzw. -Datenbank des Kunden zu speichern,
- d) keine Screenshots zu fertigen und
- e) Änderungen an Systemdaten nur im Rahmen der Aufgabenstellung vorzunehmen.

4. Berichtigung, Einschränkung und Löschung von Daten

Die Sparkasse darf die personenbezogenen Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Kunden berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die Sparkasse wendet, wird die Sparkasse dieses Ersuchen unverzüglich an den Kunden weiterleiten.

5. Qualitätssicherung und sonstige Pflichten der Sparkasse

Die Sparkasse hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet sie insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten.
- b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO.
- c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO (siehe Punkt 3).
- d) Auf Anfrage des Kunden arbeitet die Sparkasse mit der Aufsichtsbehörde bei der Erfüllung der Aufgaben zusammen.
- e) Die unverzügliche Information des Kunden über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit diese sich auf diesen Auftrag beziehen.

- f) Soweit der Kunde seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei der Sparkasse ausgesetzt ist, hat ihn die Sparkasse nach besten Kräften zu unterstützen.
- g) Die Sparkasse kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in ihrem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

6. Unterauftragsverhältnisse

Die Sparkasse ist berechtigt, Unterauftragnehmer (weitere Auftragsverarbeiter) einzusetzen, sofern sie den Kunden hierüber vorab in Textform unterrichtet und der Kunde hiergegen nicht binnen 7 Tagen berechtigten Einspruch erhebt. Die Sparkasse wird hierzu eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer abschließen.

7. Kontrollrechte des Kunden

- (1) Der Kunde hat das Recht, im Benehmen mit der Sparkasse Überprüfungen durchzuführen.
- (2) Die Sparkasse stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten der Sparkasse nach Art. 28 DS-GVO überzeugen kann. Hierzu stellt die Sparkasse eine alle drei Jahre zu erneuernde Bestätigung des Datenschutzbeauftragten dem Kunden auf dessen Anforderung bereit.
- (3) Für die Ermöglichung von Kontrollen durch den Kunden kann die Sparkasse einen angemessenen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen der Sparkasse

- (1) Die Sparkasse unterstützt den Kunden bei der Einhaltung der, in den Artikeln 32 bis 36 der DS-GVO, genannten Pflichten. Hierzu gehören u.a.:
 - a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen,
 - b) die Verpflichtung, Datenschutzverletzungen unverzüglich an den Kunden zu melden,
 - c) die Verpflichtung, den Kunden im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen.

9. Weisungsbefugnis des Kunden

- (1) Mündliche Weisungen bestätigt der Kunde unverzüglich schriftlich.
- (2) Die Sparkasse hat den Kunden unverzüglich zu informieren, wenn sie der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Die Sparkasse ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten werden von der Sparkasse nicht erstellt.

Die Sparkasse zeichnet zum Zweck der Protokollierung die per TeamViewer oder vergleichbaren Remote-Access-System durchgeführte Fernwartung aufgrund bestehender Rechenschaftspflichten (§76 BDSG) auf. Die Datei zur Aufzeichnung wird seitens der Sparkasse längstens 12 Monate aufbewahrt und anschließend gelöscht.