# Sonderbedingungen Datenschutzvereinbarung zur Auftragsvereinbarung
## der First Cash Solution GmbH (1cs) für und im Namen der Volksbank in der Ortenau eG

**Definitionen**

Auftraggeber: Vertragspartner aus dem jeweiligen Hauptvertrag.

Auftragnehmer: Volksbank in der Ortenau eG, Okenstraße 7, 77652 Offenburg.

Vertragsparteien: Beide Parteien (Auftragnehmer und Auftraggeber) werden gemeinsam in Folge Vertragsparteien genannt.

**1. Gegenstand und Dauer der Vereinbarung**

Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrags. Die Leistungen werden auf Basis der Hauptverträge zwischen den Vertragsparteien (bspw. Auftrag und Mietvertrag für die Nutzung eines kartengestützten Zahlungssystems) erbracht. Aus diesen Hauptverträgen ergibt sich auch der jeweilige Gegenstand der Verarbeitung personenbezogener Daten.
Änderungen des Verarbeitungsgegenstandes ergeben sich ausschließlich aufgrund neuer, angepasster oder gekündigter Hauptverträge zwischen den Vertragsparteien.
Das Auftragsverhältnis beginnt mit dem Datum der Unterzeichnung des Hauptvertrages. Die Dauer dieses Auftrags entspricht der Laufzeit des jeweiligen Hauptvertrags, so dass er automatisch mit Ende der Laufzeit des jeweiligen Hauptvertrags endet, ohne dass es einer Kündigung dieses Auftrags bedarf.

**2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Betroffene**

**2.1** Zweck und Art der Verarbeitung
Zur Erfüllung der vertraglichen Pflichten aus den Hauptverträgen erhält und speichert der Auftragnehmer vom Auftraggeber oder den Vertragspartnern des Auftraggebers Vertragsabrechnungs-, Zahlungs- und Kommunikationsdaten. Darüber hinaus erfasst und speichert der Auftragnehmer personenbezogene Daten von Mitarbeitern des Auftraggebers oder Vertragspartnern des Auftraggebers zur Durchführung der vertragsbedingten Kommunikation.
**2.2** Daten des Auftraggebers
Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten bei Mitarbeitern des Auftraggebers oder Mitarbeitern der Vertragspartner des Auftraggebers (Kreis der Betroffenen) sind folgende Datenkategorien:

- Name und Kommunikationsdaten der Ansprechpartner
- Bankverbindung des Auftraggebers
- Vertragspartnernummer und Vertragsdaten
- Konfigurationsdaten der technischen Schnittstellen (IP-Adressen, PC-Konfigurationen etc.)
- Auskunft über einen Registerauszug des Auftraggebers
- Legitimationsdaten des Auftraggebers

**2.3** Daten der Kunden des Auftraggebers
Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten bei Kunden des Auftraggebers oder Kunden von Vertragspartnern des Auftraggebers (Kreis der Betroffenen) sind folgende Datenkategorien:

- Zahlungsdaten (Umsatzdaten, Transaktionsdaten)
- Vertragsabrechnungsdaten
- Name und Kommunikationsdaten der Kunden

**3. Verarbeitung auf Weisung**

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf durch den Hauptvertrag erteilte Weisung des Verantwortlichen, sofern er nicht durch gesetzliche Vorgaben zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen schriftlich oder in einem dokumentierten, elektronischen Format zu erteilen. Mündliche Weisungen wiederholt der Auftraggeber unverzüglich in Textform. Weisungsberechtigte Personen des Auftraggebers sind jeweils die aktuellen gesetzlichen Vertreter.

Weisungsempfänger beim Auftragnehmer sind die Mitarbeiter des Vertriebes und des Vertriebsinnendienstes (E-Mail: mail@1cs.de).

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind der jeweiligen Vertragspartei unverzüglich schriftlich oder elektronisch die Nachfolger/die Vertreter mitzuteilen.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber nach Überprüfung bestätigt oder geändert wird.

**4. Pflichten des Auftraggebers**

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.
Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

**5. Pflichten des Auftragnehmers**

Der Auftragnehmer verpflichtet sich bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und in geeigneter Weise zur Verschwiegenheit verpflichtet.
Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
Beim Auftragnehmer ist als Beauftragter für den Datenschutz Herr Thomas Göhrig von der FCH Compliance GmbH (E-Mail: thomas.goehrig@fc-heidelberg.de) bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
Der Auftragnehmer unterstützt den Auftraggeber in dem jeweils erforderlichen Umfang dabei, die dem Auftraggeber obliegenden Pflichten, ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen sowie eine Datenschutz-Folgenabschätzung durchzuführen, zu erfüllen.
Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.
Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber wird der Auftragnehmer die jeweils erforderlichen Mitwirkungsleistungen gegenüber dem Auftraggeber erbringen. Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

**6. Kontrollrechte des Auftraggebers**

Der Auftraggeber hat das Recht, regelmäßige Kontrollen (auch vor Ort) im Hinblick auf die Vertragserfüllung durchzuführen, sofern der Auftragnehmer hierdurch nicht Betriebsgeheimnisse gefährdet sieht oder auf Daten Dritter zugegriffen wird. Die Durchführbarkeit einzelner Kontrollhandlungen sind daher im Vorfeld einer Prüfung von beiden Parteien zu klären.
Sieht der Auftragnehmer sein Betriebsgeheimnis gefährdet, werden diesbezügliche Kontrollen nur bei konkreten Verdachtsfällen hinsichtlich eines Verstoßes gegen diese Vereinbarung insofern eingeräumt, dass der Auftraggeber hierfür eine Prüfung von einer von ihm ausgewählten unabhängigen Stelle auf eigene Kosten veranlassen kann. Der Prüfer hat sicherzustellen, dass er im Rahmen seiner Prüfung keine Betriebsgeheimnisse an den Auftraggeber weitergibt.
Der Auftraggeber hat eine Kontrolle mindestens vier Wochen im Voraus anzumelden. Alle Kontrollen finden unter dem Beisein eines Mitarbeiters des Auftragnehmers statt.
Der Auftragnehmer verpflichtet sich unter Beachtung der vorgenannten Voraussetzungen die erforderlichen Auskünfte zu geben und Nachweise zu führen.
Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
Zum Nachweis der in dieser Vereinbarung festgelegten Pflichten stellt der Auftraggeber auf der Webseite www.1cs.de die jeweils aktuellen Zertifizierungen nach PCI DSS und PS 951 zum Download zur Verfügung. Unabhängig davon stellt der Auftragnehmer sicher, dass regelmäßige interne Kontrollen durchgeführt werden.

**7. Mitteilungspflichten des Auftragnehmers bei Datenpannen**

Werden dem Auftragnehmer Verletzungen des Schutzes personenbezogener Daten im Rahmen der Auftragsverarbeitung bekannt, meldet er diese dem Auftraggeber unverzüglich. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen.
Soweit eine Mitwirkungsleistung des Auftragnehmers für die Wahrung von Betroffenenrechten durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Mitwirkungsleistungen nach Weisung des Auftraggebers erbringen. 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.
Die Vertragsparteien arbeiten auf Anfrage der Aufsichtsbehörden nach Artikel 31 DSGVO bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer räumt der Aufsichtsbehörde die gleichen Kontrollrechte ein, wie sie dem Auftraggeber in dieser Vereinbarung zugestanden werden.

**8. Unterauftragsverhältnisse mit Subunternehmern**

Zurzeit sind für den Auftragnehmer die in Anlage 2 mit Namen, Anschrift und Produktzuordnung bezeichneten Subunternehmer tätig. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Die Beauftragung weiterer Subunternehmen zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung der weisungsberechtigten Personen des Auftraggebers gestattet.
Der Auftragnehmer wird die Anlage 2 in regelmäßigen Abständen dem Auftraggeber zu Verfügung stellen. Der Auftraggeber darf seine Zustimmung nicht unbillig verweigern. Sollte eine Verweigerung des Auftraggebers dazu führen, dass geschlossene Hauptverträge durch den Auftragnehmer nicht mehr erfüllt werden können, steht dem Auftragnehmer ein fristloses Kündigungsrecht zu.
Der Auftragnehmer sichert eine sorgfältige Auswahl der Subunternehmer zu. Er hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den auferlegten Datenschutzpflichten nachkommt. Zudem hat er die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig zu überprüfen.
Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen, Wartung und Benutzerservice, Reinigungskräfte, Prüfer oder die Entsorgung von Datenträgern. Der Auftragnehmer ist jedoch verpflichtet, auch hierfür angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

**9. Sicherheit der Datenverarbeitung**

Es wird für diese Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Die konkreten Maßnahmen werden in Anlage 1 festgelegt.
Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.



First Cash Solution GmbH, Okenstr. 7, D-77652 Offenburg,
Telefon: +49 (0) 7805 91696 0, Fax: +49 (0) 7805 91696 4197, mail@1cs.de, www.1cs.de
491 501 Stand 04.2018

**10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags**

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Absprache mit dem Auftraggeber entweder herauszugeben oder zu löschen bzw. zu vernichten, sofern nicht eine gesetzliche Verpflichtung zur Aufbewahrung besteht. Gleiches gilt für Test- und Ausschussmaterial.

**11. Sonstiges**

Zur Haftung und Schadensersatzansprüchen wird auf Art. 82 DSGVO verwiesen.
Erteilte Weisungen, Nebenabreden und Dokumente zum Nachweis der Einhaltung der vertraglichen Pflichten sind für ihre Geltungsdauer und anschließend noch für drei Kalenderjahre aufzubewahren.
Sollten das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahmung), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
Die Parteien vereinbaren die ausschließliche Anwendbarkeit deutschen Rechts. Die Festlegung des Gerichtsstandes obliegt dem Auftraggeber.



First Cash Solution GmbH, Okenstr. 7, D-77652 Offenburg,
Telefon: +49 (0) 7805 91696 0, Fax: +49 (0) 7805 91696 4197, mail@1cs.de, www.1cs.de
491 501 Stand 04.2018

# Sonderbedingungen Datenschutzvereinbarung zur Auftragsvereinbarung
**der First Cash Solution GmbH (1cs) für und im Namen der Volksbank in der Ortenau eG**

## Anlage 1 – Technisch-organisatorische Maßnahmen

Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten. Die Parteien haben das erforderliche Schutzniveau gemeinsam ermittelt und sind zu dem Ergebnis gekommen, dass ein sehr hohes Schutzniveau einzuhalten ist.

Das Schutzniveau wird durch diese Maßnahmen eingehalten:

**a. Vertraulichkeit**

- Alarmanlage/Einbruch-Meldesystem im gesamten Gebäude; Sicherung außerhalb der Arbeitszeit
- Türsicherung: Zutritt in die Räumlichkeiten mit Chipkarten der Mitarbeiter gesichert; der Zutritt ist jeweils beschränkt auf den notwendigen Personenkreis
- Besucherausweise für Firmenfremde
- Serverraum zusätzlich gesichert durch Schließsystem mit Codesperre
- Serverraum in brandschutzgesichertem Bereich
- Gesicherter Eingang für An- und Ablieferung
- Authentifikation mit Benutzer ID und Passwort; Regeln zur Vergabe von Benutzer IDs und Passwörtern; es wird ein regelmäßiger Passwortwechsel erzwungen
- Für den Bereich Zahlungssysteme separate Benutzerberechtigungsverwaltung
- Einsatz von Anti-Viren-Software und Firewalls
- Selbst angestelltes und sorgfältig ausgewähltes Reini-gungspersonal
- Kontrollierte Vernichtung von Datenträgern
- Verpflichtung auf das Datengeheimnis
- Regelungen für die Vergabe von Zugriffsberechtigungen
- Zugriff auf PCs durch Windows-Anmeldung gesichert, automatische Abmeldung bei Abwesenheit vom Arbeitsplatz
- Das Netz des Bereichs Zahlungssysteme ist logisch getrennt (VLAN) vom Kernbanksystem. Somit sind keinerlei unberechtigte Zugriffe von Mitarbeitern außerhalb des Be-reichs Zahlungssystem möglich

**b. Integrität**

- Einsatz von VPN Technologie zur verschlüsselten Übertragung der Zahlungsdaten
- Empfang und Versand von Kundendaten über CryptShare
- Bereitstellung von Kundendaten über SFTP
- Bei Speicherung personenbezogener Daten auf mobilen Datenträgern ist sichergestellt, dass diese stets im Zugriff von berechtigten Personen sind
- Regelmäßige Sicherung des Datenbestandes auf externe Platte, die im Tresor (GIS Data Save) abgelegt wird
- Vollständigkeits- und Richtigkeitsprüfungen bei Datenlieferungen
- Löschung von Datenresten vor Datenträgeraustausch
- Anzeige der benutzerbezogenen Änderungshistorie im CRM-System
- Sofern angelieferte personenbezogene Zahlungsdaten verändert oder entfernt werden müssen, geschieht dies nur in begründeten Fällen und ausschließlich gemäß schriftlichem oder telefonischem Auftrag
- Verpflichtung auf das Datengeheimnis
- Bei der Anlieferung der personenbezogenen Daten besteht immer der Zweck der Transaktionsverarbeitung und/oder des Cash Poolings. Aus Gründen der Wirtschaftlichkeit werden die Kundendaten im Rahmen der Transaktionsverarbeitung und/oder des Cash Poolings gemeinsam verarbeitet, eine Trennung ist nicht vorgesehen. Durch qualitätsgesicherte Anwendungen dieses Prozesses ist sichergestellt, dass sich Daten nicht vermischen und somit stets nacheinander und getrennt verarbeitet werden.
- Die Daten für das Clearing und Reporting werden getrennt verarbeitet und gespeichert
- Trennung von Produktiv- und Testsystem

**c. Verfügbarkeit und Belastbarkeit/Physischer oder technischer Zwischenfall**

- Angelieferte Kundendaten werden redundant gespeichert, so dass beim Ausfall eines Datenspeichers die Daten noch vorhanden sind
- Tägliche Vollsicherung des Datenbestandes
- Anlieferung der Daten über getrennte Zugangskanäle möglich, falls ein Kanal ausfallen sollte
- Notfallkonzeption und Durchführung von Notfalltests

**d. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Maßnahmen**

- Informationssicherheits-Management
- Datenschutz-Management
- Incident-Response-Management
- Auftragskontrolle (Keine Auftragsdatenverarbeitung im Sinne von Artikel 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z. B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.)



First Cash Solution GmbH, Okenstr. 7, D-77652 Offenburg,
Telefon: +49 (0) 7805 91696 0, Fax: +49 (0) 7805 91696 4197, mail@1cs.de, www.1cs.de
491 501 Stand 04.2018