Vereinbarung zur Wartung und Pflege von IT-Systemen per Fernwartung inkl. Datenschutzvereinbarung

Zwischen dem Kunden

- Auftraggeber der Fernwartung - und

der

Volksbank Köln Bonn eG, Heinemannstr. 15, 53175 Bonn - Auftragnehmer -

1. Präambel

Die Volksbank Köln Bonn eG führt beim Kunden eine Wartung und Pflege von IT-Systemen per Fernwartung durch. Die Preise für diese Leistung sind dem Preisverzeichnis der Volksbank Köln Bonn eG zu entnehmen.

Diese Vereinbarung wird als Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG), insbesondere des § 11 BDSG („Auftragsdatenverarbeitung") geschlossen. Den Parteien ist bekannt, dass seit dem 25.05.2018 die Datenschutz-Grundverordnung (DSGVO - EU-Verordnung 2016/679) gilt und sich die Vorgaben der Auftragsdatenverarbeitung dann grundsätzlich nach Art. 28 DSGVO richten.

2. Allgemeines

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers per Fernwartung durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogene Daten bekommt bzw. Kenntnis erlangt oder personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können.

3. Dauer und Beendigung des Auftrags

Der Auftragnehmer führt für den Auftraggeber Leistungen (Wartung und/oder Pflege von IT-Systemen) durch. Die Leistung wird auf Basis der allgemeinen Geschäftsbedingungen der Volksbank Köln Bonn eG durchgeführt. Diese Vereinbarung beginnt ab elektronischer oder schriftlicher Unterzeichnung durch beide Parteien. Die Dokumentation der Fernwartung wird als Videodatei gespeichert und nach 90 Tagen gelöscht, sofern keine zusätzliche Weisung des Auftraggebers erfolgt. Wird diese Vereinbarung elektronisch geschlossen, endet Sie automatisch nach 90 Tagen nach Durchführung der Fernwartung mit der Löschung der Videodateien. Eine gesonderte Information des Auftraggebers erfolgt nicht mehr. Wird dieser Vertrag schriftlich geschlossen, kann er jederzeit ohne Einhaltung einer Kündigungsfrist gekündigt werden. Der Auftraggeber willigt unabhängig von einer Kündigung in die Speicherung der Videodateien für maximal 90 Tagen nach Durchführung der Fernwartung ein.

4. Gegenstand des Auftrags

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- Durchführung einer Fernwartung zur Wartung und Pflege von IT-Systemen.

Hierbei ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf folgende Daten/Datenarten hat:

- Namen
- Anschriften
- Bankdaten
- Kontodaten
- Kontoumsätze

Kreis der von der Datenverarbeitung Betroffenen:

- Kunden
- Lieferanten
- Beschäftigte
- Sonstige Dritte

5. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Wartung und Pflege von IT-Systemen gegenüber dem Auftragnehmer zu erteilen. Weisungen können

- schriftlich
- per Fax
- per E-Mail

erfolgen.

(2) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Wartung und Pflege durch den Auftragnehmer feststellt.

6. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, auf die er im Zusammenhang mit den Wartungs-/Pflegearbeiten Zugriff erhält, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(4) Für den Fall, dass der Auftragnehmer feststellt oder Tatsachen die Annahme begründen, dass von ihm für den Auftraggeber verarbeitete

- besondere Arten bzw. besondere Kategorien personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG bzw. Art. 9 DSGVO oder
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen oder
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig über Zeitpunkt, Art und Umfang des Vorfalls/der Vorfälle in Schriftform oder Textform (Fax/E-Mail) zu informieren. Die Information muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung enthalten. Die Information soll zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung beinhalten. Der Auftragnehmer ist darüber hinaus verpflichtet, unverzüglich mitzuteilen, welche Maßnahmen durch den Auftragnehmer getroffen wurden, um die

unrechtmäßige Übermittlung bzw. unbefugte Kenntnisnahme durch Dritte künftig zu verhindern.

(5) Der Auftragnehmer kommt seit dem 25.05.2018 seinen Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nach.

7. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, sofern die Betriebsabläufe des Auftragnehmers durch die Kontrollen gestört werden.

(4) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. § 38 BDSG bzw. seit dem 25.05.2018 nach Art. 58 DSGVO i.V.m. § 40 BDSG (neu), insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen.

8. Fernwartung

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z.B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o.ä. Gerät zu verfolgen.

(2) Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i.S.d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung i.S.d. § 203 StGB durch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

(3) Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o.ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

9. Unterauftragsverhältnisse

(1) Die Beauftragung von Subunternehmen durch den Auftragnehmer ist nur mit schriftlicher Zustimmung des Auftraggebers zulässig.

(2) Der Auftragnehmer hat das Subunternehmen sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Subunternehmer die nach § 9 BDSG bzw. seit dem 25.05.2018 nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Das Ergebnis der Kontrolle ist vom Auftragnehmer zu dokumentieren und auf Anfrage dem Auftraggeber zu übermitteln. Der Auftragnehmer ist verpflichtet, sich vom Subunternehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten i.S.d. § 4f BDSG bzw. seit dem 25.05.2018 nach Art. 37 DSGVO i.V.m. § 38 BDSG (neu) bestellt hat, soweit dieser gesetzlich zur Bestellung eines Datenschutzbeauftragten verpflichtet ist.

(3) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Subunternehmer gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren.

(4) Die Verpflichtung des Subunternehmens muss schriftlich erfolgen. Dem Auftraggeber ist die schriftliche Verpflichtung auf Anfrage in Kopie zu übermitteln.

(5) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 5 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

10. Datengeheimnis

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 5 BDSG bzw. seit dem 25.05.2018 zur Wahrung der Vertraulichkeit verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 5 BDSG verpflichtet wurden. Seit dem 25.5.2018 wird der Auftragnehmer stattdessen die in Satz 2 genannten Personen in einer dem Art. 28 Abs. 3 lit. b) genügenden Weise zur Vertraulichkeit verpflichten, sofern diese nicht schon anderweitig einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

11. Wahrung von Betroffenenrechten

Der Auftraggeber ist für die Wahrung der Betroffenenrechte alleine verantwortlich.

12. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen (TOM), die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Eine Dokumentation der TOM's ist der Anlage 1 zu entnehmen.

13. Schlussbestimmungen

(1) Es gilt das Recht der Bundesrepublik Deutschland.

(2) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

Anlage 1 – Technisch-organisatorische Maßnahmen

(Stand September 2018)

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle

Das Eindringen Unbefugter in Systeme und Anwendungen, die zur Verarbeitung von personenbezogenen Daten eingesetzt werden, ist zu verhindern.
Es ist kein unbefugter Zutritt zu Datenverarbeitungsanlagen durch Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Alarmanlagen, Videoanlagen möglich.

- Zugangskontrolle

Der unbefugte Zutritt zu Gebäuden, Räumen und Einrichtungen, in denen personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ist zu verhindern. Es ist keine unbefugte Systembenutzung durch (sichere) Kennwörter, automatische Sperrmechanismen und Verschlüsselung von Datenträgern möglich.

- Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen und mit DV-Anwendungen, die zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten dienen, sind zu verhindern.
Es ist kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte möglich.

- Trennungskontrolle

Daten verschiedener Verantwortlicher sind nach ihrem Erhebungszweck zumindest sachlogisch getrennt zu verarbeiten.
Die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, erfolgt durch Mandantenfähigkeit und separate Dateiablage.

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Der Schutz personenbezogener Daten wird insbesondere durch die Pseudonymisierung, die Trennung der die Personen unmittelbar identifizierbar machenden Daten von den weiteren Daten und deren getrennte Aufbewahrung, erreicht.
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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle

Aspekte im Zusammenhang mit der Weitergabe personenbezogener Daten innerhalb und außerhalb der DV-Systeme und DV-Anwendungen sind zu regeln.
Es ist kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport möglich.

- Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverarbeitung ist zu gewährleisten. Es wird festgehalten, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch Protokollierung und Dokumentenmanagement.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle

Personenbezogene Daten sind gegen zufällige oder mutwillige Zerstörung bzw. Verlust zu schützen. Es erfolgt ein Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backups, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne. Eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO) ist gewährleistet.

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

Es ist seitens des Auftragsverarbeiters ein Datenschutzmanagement zu implementieren, das geeignet ist, regelmäßig eine Überprüfung, Bewertung und Evaluierung der Einhaltung der datenschutzrechtlichen Anforderungen, insbesondere der technischen-organisatorischen Maßnahmen zu gewährleisten.

- Datenschutz-Management
- Datenschutzprüfungen durch die Revision
- Auftragskontrolle

Eine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO erfolgt nur mit entsprechender Weisung des Auftraggebers, durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters.