Anlage: Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 BDSG

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Dienstvertrag in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Dienstvertrag in Zusammenhang stehen und bei denen Mitarbeiter der creditPass GmbH oder durch die creditPass GmbH beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrags.

§ 1 Definitionen:
(1) Personenbezogene Daten
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.
(2) Datenverarbeitung im Auftrag
Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch die creditPass GmbH im Auftrag des Auftraggebers.
(3) Weisung
Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) der creditPass GmbH mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 2 Anwendungsbereich und Verantwortlichkeit
(1) Die creditPass GmbH verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an die creditPass GmbH sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („verantwortliche Stelle“ im Sinne des § 3 Abs. 7 BDSG).
(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.
(3) Die Inhalte dieser Vertragsanlage gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird, und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 3 Pflichten der creditPass GmbH
(1) Die creditPass GmbH darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.
(2) Die creditPass GmbH wird in Ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen des Bundesdatenschutzgesetzes (§ 9 BDSG) entsprechen. Dies beinhaltet insbesondere
a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
c) dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
d) dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
e) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
f) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
g) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
h) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).
Eine Maßnahme nach b bis d ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.
Eine Darstellung dieser technischen und organisatorischen Maßnahmen wird als Annex 1 Bestandteil dieser Vereinbarung.
(3) Die creditPass GmbH stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsdatenverarbeitung zur Verfügung. Die Kosten hierfür trägt der Auftraggeber.
(4) Die creditPass GmbH stellt auf Anforderung dem Auftraggeber die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung. Die Kosten hierfür trägt der Auftraggeber.
(5) Die creditPass GmbH stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß § 5 Bundesdatenschutzgesetz (Datengeheimnis) verpflichtet und in die Schutzbestimmungen des Bundesdatenschutzgesetzes eingewiesen worden sind. Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.
(6) Die creditPass GmbH teilt dem Auftraggeber auf Anfrage die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.
(7) Die creditPass GmbH unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.
(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Die creditPass GmbH hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Die creditPass GmbH ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt die creditPass GmbH auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.
(9) Die Erfüllung der vorgenannten Pflichten ist von der creditPass GmbH zu kontrollieren und in geeigneter Weise nachzuweisen.

§ 4 Pflichten des Auftraggebers
(1) Der Auftraggeber und die creditPass GmbH sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.
(2) Der Auftraggeber hat die creditPass GmbH unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
(3) Die Pflicht zur Führung des öffentlichen Verfahrensverzeichnisses (Jedermannverzeichnis) gem. § 4g Abs. 2 S. 2 BDSG liegt beim Auftraggeber.
(4) Dem Auftraggeber obliegen die aus § 42a BDSG resultierenden Informationspflichten.
(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.
(6) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
(7) Erteilt der Auftraggeber Einzelweisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

§ 5 Anfragen Betroffener an den Auftraggeber
Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird die creditPass GmbH den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt:
- der Auftraggeber hat die creditPass GmbH hierzu schriftlich aufgefordert und
- der Auftraggeber erstattet der creditPass GmbH die durch diese Unterstützung entstandenen Kosten.

§ 6 Kontrollpflichten
(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen der creditPass GmbH und dokumentiert das Ergebnis.
Hierfür kann er
a) Selbstauskünfte der creditPass GmbH einholen.
b) sich ein Testat eines Sachverständigen vorlegen lassen.
c) sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich überzeugen.
(2) Die creditPass GmbH verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.
(3) Die der creditPass hierfür entstehenden Kosten trägt der Auftraggeber.

§ 7 Subunternehmer
(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen fachlich qualifizierte Unternehmen oder Unternehmer zur Leistungserfüllung oder für damit zusammenhängende Leistungen (z.B. Wartung, Service etc.) heranzieht, sofern diese Unternehmen ihren Sitz im Europäischen Wirtschaftsraum haben und ihre Leistungen auch innerhalb des Europäischen Wirtschaftsraumes erbringen.
(2) Erteilt die creditPass GmbH Aufträge an Unterauftragnehmer, so obliegt es der creditPass GmbH, ihre Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen. Satz 1 gilt insbesondere für Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages.
(3) Die creditPass GmbH wird dem Auftraggeber auf Anforderung in Textform jederzeit Auskunft über die aktuell bestehenden Unteraufträge erteilen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl
(1) Sollten die Daten des Auftraggebers bei der creditPass GmbH durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die creditPass GmbH den Auftraggeber unverzüglich darüber zu informieren. Die creditPass GmbH wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „verantwortlicher Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.
(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen der creditPass GmbH - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
(3) Es gilt deutsches Recht.

Annex 1 zur Vereinbarung zur Auftragsdatenverarbeitung

Die nachstehend aufgeführten technischen und organisatorischen Maßnahmen gelten für das Produkt „creditPass“ der creditPass GmbH. Mit dem Zusatz [RZ] gekennzeichnete Maßnahmen gelten nur für das Rechenzentrum, nicht für die Büroräume der creditPass GmbH. Von den Büroarbeitsplätzen ist kein Zugriff auf die von den Auskunfteien übermittelten Ergebnisse der creditPass-Anfrage möglich. Maßnahmen, die nur für die Büroräume gelten sind mit dem Zusatz [OF] gekennzeichnet. Maßnahmen ohne Zusatz gelten sowohl für das Rechenzentrum als auch für die Büroräume.
Die creditPass GmbH nutzt Server im Rechenzentrum der **Interlake System GmbH**, Postfach 2269, 88012 Friedrichshafen. Mit der Firma Interlake als Unterauftragnehmer im Sinne von § 7 der Vereinbarung zur Auftragsdatenverarbeitung besteht eine gesonderte Vereinbarung zur Auftragsdatenverarbeitung, in der die nachstehend für das Rechenzentrum festgelegten technischen und organisatorischen Maßnahmen vertraglich vereinbart sind.

1. Zutrittskontrolle
Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:
- [OF] Zutritt zu den Büroräumen besteht nur für Mitarbeiter, Gäste haben nur in Begleitung eines Mitarbeiters und erst nach Registrierung und Identifizierung Zutritt
- [RZ] Zutritt zu den Rechenzentren nur für autorisierte Mitarbeiter – Prüfung erfolgt durch den Sicherheitsdienst
- [RZ] Richtlinie zur Begleitung und Kennzeichnung von Gästen
- [RZ] Vergaberichtlinie für Zutrittsberechtigungen zu den Rechenzentren
- [RZ] Server in abschließbaren Serverschränken
- [RZ] Kennzeichnung der Server durch Aliase
- [RZ] Organisationsanweisung zur Ausgabe von Schlüsseln
- [RZ] Sicherung durch Wachdienst mit regelmäßigen Kontrollgängen
- [RZ] Überwachung/Aufzeichnung des Zutritts durch Kameras

2. Zugangskontrolle
Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:
- Rechner und Serversysteme nur mit Passwort und über passwortgeschützte, verschlüsselte Verbindung durch Benutzer mit Adminstratorrechten nutzbar
- Clientsysteme nur nach passwortgestützter Netzwerk-Authentifizierung nutzbar
- Sperrung des Benutzerkontos nach drei fehlgeschlagenen Anmeldeversuchen
- Automatische, passwortgeschützte Bildschirm- und Rechnersperre
- Verbindliches Verfahren zur Vergabe von Berechtigungen
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern
- [OF] Verbindliche Vorgaben für die Passwortqualität (Mindestlänge 8 Zeichen, muss Sonderzeichen, Zahlen und Groß-/Kleinschreibung enthalten)
- [RZ] Verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter
- [RZ] Richtlinie zum sicheren, ordnungsgemäßen Umgang und Änderung von Passwörtern

3. Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
- Verbindliches Berechtigungsvergabeverfahren
- Trennung von Berechtigungsbewilligung (organisatorisch) durch Abteilungsleitung / Geschäftsleitung / Geschäftsführung und Berechtigungsvergabe (technisch) durch IT-Abteilung
- [OF] Zugriff auf Antworten der Auskunfteien haben nur speziell geschulte und unterwiesene Mitarbeiter von creditPass. Diese sind per Arbeitsanweisung verpflichtet, nur auf ausdrückliche Anforderung des Auftraggebers Zugriff auf die Antworten der Auskunfteien zu nehmen.
- [RZ] Berechtigungsmechanismus mit Möglichkeit zur exakten Differenzierung auf Feldebene
- [RZ] Verbindliches Verfahren zur Wiederherstellung von Daten aus Backup (Restore durch ITAbteilung auf Anweisung von Geschäftsführung)
- [RZ] Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(gruppen)
- [RZ] Einsatz von Application-Firewalls und Intrusion-Detection-Systemen zur Verhinderung und Erkennung von Angriffen. Verbindliche Arbeitsanweisung für Administratoren im Alarmfall
- [RZ] Zugriffsauditierung und Analyse der Auditlogs

4. Weitergabekontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:
- Systemzugriffe werden automatisiert geloggt
- [OF] Nur ausgewählte Mitarbeiter von creditPass haben Zugriff auf das creditPass-System
- [RZ] Einsatz von Verschlüsselung in Aufbewahrung und Transport
- [RZ] Zugriff auf personenbezogene Daten nur über authentifizierte Kanäle
- [RZ] Automatische Sperre bei mehrmaliger fehlerhafter Authentifizierung
- [RZ] Einsatz von Application-Firewalls und Intrusion-Detection-Systemen zur Verhinderung und
- Erkennung von Angriffen. Verbindliche Arbeitsanweisung für Administratoren im Alarmfall
- [RZ] Zugriffsauditierung und Analyse der Auditlogs
- [RZ] Versand personenbezogener Daten per verschlüsselter E-Mail

5. Eingabekontrolle
Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
- [OF] Kein Zugriff auf Antworten der Auskunfteien möglich
- [RZ] Vertragliche Beschränkung der Arbeit mit personenbezogenen Daten des Auftraggebers auf die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeiter des Dienstleisters
- [RZ] Registrierung der Benutzer und Uhrzeit der jeweiligen Änderung im System
- [RZ] Einsatz von Application-Firewalls und Intrusion-Detection-Systemen zur Verhinderung und Erkennung von Angriffen. Verbindliche Arbeitsanweisung für Administratoren im Alarmfall
- [RZ] Zugriffsauditierung und Analyse der Auditlogs

6. Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:
- [RZ] Detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers
- [RZ] Detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Dienstleister außerhalb des schriftlich formulierten Auftrags
- [RZ] Der Dienstleister hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse
- [RZ] Auf Kundenwunsch kann im Vertrag eine verantwortliche Person beim Auftraggeber benannt werden, die in Bezug auf die vereinbarte Auftragsdatenverarbeitung gegenüber dem Dienstleister weisungsbefugt ist

7. Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:
- [RZ] Vollständiges Backup- und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Datenträger
- [RZ] Nachweis der sicheren und ordnungsgemäßen Archivierung in physisch geschütztem Archiv und verbindlicher Regelung der Zugriffsberechtigten
- [RZ] Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) und schriftliche Konzeption ihres Einsatzes
- [RZ] Einsatz von Storage Systemen mit Rendundanz (RAID)
- [RZ] Einsatz unterbrechungsfreier Stromversorgung und von Notstromaggregaten
- [RZ] Richtlinie zur Wartung und Durchführung von Updates
- [RZ] Automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware (z.B. Virenscanner)
- [RZ] Automatisches Monitoringkonzept und permanentes Monitoring zur Erkennung von Störungen
- [RZ] Automatisierter Benachrichtigungsworklfow zur Verbreitung von Wartungs- und Störungsmeldungen

8. Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:
- [OF] Anfragen und Daten unterschiedlicher Auftraggeber werden logisch getrennt voneinander gespeichert und verarbeitet
- [RZ] Die Daten unterschiedlicher Auftraggeber/Projekte werden soweit möglich auf unterschiedlichen Systemen verarbeitet
- [RZ] Die Daten unterschiedlicher Auftraggeber/Projekte werden soweit möglich von unterschiedlichen Mitarbeitern verarbeitet
- [RZ] Abschottung der Systeme unterschiedlicher Projekte in verschiedenen Sicherheitszonen
- [RZ] Die in den verwendeten Systemen verfügbaren Berechtigungsmechanismen ermöglichen die exakte Umsetzung der Vorgaben des Berechtigungskonzeptes
- [RZ] Aufträge an Subunternehmer dürfen nur nach Genehmigung vergeben werden. Der Auftragnehmer hat in diesem Fall vertraglich sicherzustellen, dass die vereinbarten Regelungen auch gegenüber Subunternehmen gelten. Sie haben die Einhaltung dieser Pflichten regelmäßig zu überprüfen. Die Weiterleitung von Daten ist erst zulässig, wenn der Subunternehmer die Verpflichtung nach § 11 BDSG erfüllt hat.