Vereinbarung

über Auftragsdatenverarbeitung i.S.d. Art. 28 Abs. 3
Datenschutz-Grundverordnung (DSGVO)

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragspartner zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit der Zusammenarbeit im Zusammenhang stehen und bei denen Beschäftigte der **ribeka GmbH**, Johann-Philipp-Reis-Str. 9, 53332 Bornheim (nachfolgend „Auftragnehmer“) oder durch den Auftragnehmer beauftragte personenbezogene Daten des Auftraggebers verwalten.

§1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

SchILDcard ist ein Modul zu SchILD zur einfachen Erstellung von Schülerausweisen. Über SchILDcard können alle notwendigen Konfigurationen (Layout, Inhalt, Gültigkeit, etc.) sowie alle notwendigen Daten (Schüler) erstellt, ausgewählt und direkt an die Germancard Technologie GmbH für den Druck übergeben werden. Im Rahmen der Leistungserbringung ist es erforderlich, dass sowohl der Auftragnehmer als auch der mit dem Druck beauftragte Hersteller (Germancard Technologies GmbH) mit personenbezogenen Daten umgeht, für die die Schule als verantwortliche Stelle im Sinne der daten-schutzrechtlichen Vorschriften fungiert.

Diese Vereinbarung richtet sich nach der Laufzeit der Zusammenarbeit, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

§2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen werden anfänglich festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die in der Leistungsbeschreibung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine

Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DSGVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Vereinbarung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Das Datenschutz- und Sicherheitskonzept der ribeka GmbH sowie der Germancard Technologies GmbH ist dieser Vereinbarung beigefügt.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragnehmer unterstützt – soweit vereinbart – den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten. Entstehen hierdurch zusätzliche Kosten, so trägt diese der Auftraggeber.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisungen zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einen angemessenen gesetzlichen Verschwiegenheitspflichten unterliegen. Die Vertraulichkeits- / Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrags fort.

(5) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten bekannt werden.

(6) Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(7) Den aktuellen Ansprechpartner des Auftragnehmers für im Rahmen der Vereinbarung anfallende Datenschutzfragen finden Sie unter www.ribeka.com/datenschutz der Ansprechpartner des Herstellers ist Herr Yahya Zahad (office@germancard.de) sowie der vom Hersteller beauftragte externe Datenschutzbeauftragte. Im Falle eines Wechsels des Ansprechpartners, unterrichtet der Auftragnehmer den Auftraggeber unverzüglich.

(8) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit einzusetzen.

(9) Der Auftragnehmer berichtigt oder löscht die auftragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine

entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien aufgrund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren. Entstehen hierdurch Kosten, so trägt dies der Auftraggeber.

(10) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung nicht erforderlich. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(11) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen. Entstehen hierdurch Kosten, so trägt diese der Auftraggeber.

§4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO, gilt §3, Abs. 10 entsprechend. Entstehen hierdurch Kosten, so trägt diese der Auftraggeber.

(3) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§5 Anfragen betroffener Personen

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angeben der Person möglich ist.

(2) Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung - soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist den Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

(2) Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen Einspruchsrecht.

(3) Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen. Der Aufwand einer Inspektion ist für den Auftraggeber grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

(4) Sollte eine Datenaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Eine Liste der aktuell eingesetzten Subunternehmer (Auftragsverarbeiter) finden Sie in Anlage 2

(2) Der Einsatz weitere Subunternehmer als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(3) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten eine im erforderlichen Umfang Vereinbarungen treffen, um angemessenen Datenschutz- und Informations- Sicherheitsmaßnahmen zu gewährleisten.

(4) Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber.

(5) Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund gegenüber der vom Auftragnehmer bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

(6) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§8 Informationspflichten, Schriftformklausel, Rechtwahl

(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 dem Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen darüber informieren, dass die Hoheit

und das Eigentum an diesen Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen zu dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann 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) Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen der Zusammenarbeit vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage nicht.

(4) Es gilt deutsches Recht.

§9 Haftung und Schadensersatz

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechen der in Art. 82 DSGVO getroffenen Regelung.

Anlage 1

Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Zweck der Datenverarbeitung	Die Verarbeitung erfolgt zum Zweck der vertragsgemäßen Leistung (Herstellung / Druck und Versand von Schülerausweisen)
Art und Umfang der Datenverarbeitung	Die von der Schule über SchILDcard bereitgestellten Daten sind die essentiell, für die vereinbarte Leistungserbringung benötigten Daten (siehe „Art der Daten“).
Art der Daten	Folgende Daten werden zur Erstellung von Schülerausweisen übertragen: Schuldaten (Schulname, Schulnummer, Rechnungs- und Lieferanschrift) Schülerindividualdaten (Vorname und Nachname, Geburtsdatum, Schülerfoto) Klassen- , Kurszugehörigkeit
Kategorien betroffener Personen	Schüler/Schülerinnen

Anlage 2

Weitere Auftragsverarbeiter

Firma, Anschrift	**Art der Verarbeitung**	**Zweck**	**Art der Daten**	**Kategorien der betroffenen Personen**
Germancard Technologies GmbH Ottostraße 5 50170 Kerpen	Bereitstellung der technischen und logistischen Infrastruktur zur Erstellung von Ausweiskarten	Herstellung (Druck) und Versand der bestellten Schülerausweise	siehe Anlage 1	siehe Anlage 1
Germancard Technologies GmbH Ottostraße 5 50170 Kerpen	Bereitstellung einer hochsicheren, DSGVO-Konformen Infrastruktur für den Datenaustausch	Sicherer Austausch von Daten zwischen Auftraggeber, Auftragnehmer und Hersteller	siehe Anlage 1	siehe Anlage 1

Anlage 3

TOM

Datenschutz- und Datensicherheitskonzept

entsprechend Art. 5 Abs. 1 lit. f und Art. 32 DSGVO

Dem Schutz der personenbezogenen Daten der betroffenen Personen kommt höchste Bedeutung zu. Die personenbezogenen Daten sind daher stets in Übereinstimmung mit den anwendbaren Datenschutzvorschriften, insbesondere der Datenschutzgrundverordnung (DSGVO) zu verarbeiten.

Gem. Art. 32 DSGVO sind die zu treffenden technisch organisatorischen Maßnahmen im Einzelnen festzulegen. Dies erfolgt innerhalb dieses Datenschutz- und Datensicherheitskonzepts.

Entsprechend Art. 32 DSGVO hat der Auftragnehmer sowie alle eingesetzten Subunternehmer (siehe Anlage 2) die technischen und organisatorischen Maßnahmen zu treffen, die geeignet sind, um die Ausführung der Vorschriften der DSGVO zu gewährleisten. Geeignet sind Maßnahmen nur, wenn sie eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung. Dazu wurde eine vorangehende Bewertung von Risiko und Folgen für die Rechte und Freiheiten betroffener Personen unter Berücksichtigung der Art der Auftragsdaten, des Umfangs, der Umstände, des Zwecks, der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere des Risikos, des Stand der Technik, der Implementierungskosten sowie der notwendigen Garantien zum Schutz der betroffenen Personen durchgeführt.

Allgemeine Datenschutzgrundsätze

Die ribeka GmbH setzt bei der Verarbeitung personenbezogener Daten nur Personal ein, welches geschult und zur Einhaltung der datenschutzrechtlichen Vorgaben und Verhaltensregeln verpflichtet ist. Dies trifft ebenso Mitarbeiter des Auftragsverarbeiters.

Bei der Identifizierung und Umsetzung von Sicherheitsmaßnahmen der unternehmenseigenen Informationstechnik hält sich die ribeka GmbH und die Germancard Technologie GmbH an den IT-Grundschutz.

ribeka GmbH

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
    1.1 Zutrittskontrolle
        Unbefugten ist der Zutritt zu Räumen zu verwehren, in denen Datenverarbeitungsanlagen untergebracht sind.
        - Realisierung eines wirksamen Zutrittsschutzes
        - Festlegung zutrittsberechtigter Personen
        - Verwaltung von personengebundenen Zutrittsberechtigungen
        - Begleitung von Fremdpersonal

    1.2 Zugangskontrolle
        Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden.
        - Festlegung des Schutzbedarfs
        - Zugangsschutz
        - Umsetzung Authentisierung per Username Passwort
        - Gesicherte (verschlüsselte) Übertragung von Authentisierungsgeheimnissen
        - Sperrung bei Fehlversuchen und Prozess zur Rücksetzung gesperrter Zugangskennungen
        - Festlegung befugter Personen
        - Automatische Zugangssperre und Manuelle Zugangssperre

    1.3 Zugriffskontrolle

Es kann nur auf die Daten zugegriffen, für die eine Zugriffsberechtigung besteht. Daten können bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt
werden.

- Erstellen eines Berechtigungskonzepts
- Umsetzung von Zugriffsbeschränkungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen

1.4 Verwendungszweckkontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Datensparsamkeit im Umgang mit personenbezogenen Daten
- Getrennte Verarbeitung verschiedener Datensätze
- Regelmäßige Verwendungszweckkontrolle und Löschung
- Trennung von Test- und Entwicklungsumgebung

1.5 datenschutzfreundliche Voreinstellungen

Es werden nur Daten erhoben, die zur Erreichung des Verwendungszwecks erforderlich sind.

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

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, zu 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.

- Festlegung Empfangs- /Weitergabeberechtigter Instanzen/Personen
- Prüfung der Rechtmäßigkeit der Übermittlung ins Ausland
- Sichere Übertragung zu externen Systemen
- Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Härtung der Backendsysteme
- Beschreibung der Schnittstellen
- Sichere Ablage von Daten, inkl. Backups
- Gesicherte Speicherung auf mobilen Datenträgern
- Einführung eines Prozesses zur Datenträgerverwaltungen
- Prozess zur Sammlung und Entsorgung
- Datenschutzgerechter Lösch- und Zerstörungsverfahren
- Führung von Löschprotokollen

2.2 Eingabekontrolle

Zweck der Eingabekontrolle ist es, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt
worden sind.

- Protokollierung der Eingaben
- Dokumentation der Eingabeberechtigungen

3. Verfügbarkeit, Belastbarkeit, Desaster Recovery

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

- Brandschutz
- Redundanz der Primärtechnik
- Monitoring
- Datensicherungskonzepte und Umsetzung

3.2 Desaster Recovery – Rasche Wiederherstellung nach Zwischenfall (Art. 32 Abs. 1 lit. c DSGVO)

- Notfallplan
- Datensicherungskonzepte und Umsetzung

4. Datenschutzorganisation

- Festlegung von Verantwortlichkeiten
- Umsetzung und Kontrolle geeigneter Prozesse
- Umsetzung von Schulungsmaßnahmen
- Verpflichtung auf Vertraulichkeit
- Regelungen zur internen Aufgabenverteilung
- Einführung einer geeigneten Vertreterregelung

5. Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl weiterer Auftragnehmer nach geeigneten Garantien
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit weiteren Auftragnehmern
- Abschluss einer Vereinbarung zur Auftragsverarbeitung mit der Schule

Germancard Technologie GmbH

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

- Zutrittskontrolle

Die Germancard Technologie GmbH verwehrt Unbefugten den Zutritt zu den Unternehmensräumen. Dies geschieht durch:

- Einsatz eines Objektschutzes
- Einsatz eines Schließsystems, das einen Zugang nur für Berechtigte ermöglicht
- Permanente Begleitung bzw. Beaufsichtigung von Besuchern
- Baulich separierter Serverraum mit Beschränkung des Zugangs nur für berechtigte Personen

- Zugangskontrolle

Die Germancard Technologie GmbH verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Dies geschieht durch:

- Authentifizierung von Systemanwendern durch Benutzer-/Passwortverfahren
- Einrichten persönlicher Benutzerkonten zur Steuerung individueller Berechtigungen
- Protokollierung von Einwahlversuchen
- Sperrung von Benutzerkonten nach drei Fehlversuchen
- Passwörter müssen folgende Restriktionen erfüllen: Länge mind. acht Zeichen, Gültigkeit 6 Monate, Passwort Historie über die letzten 5 Einträge
- Automatische Bildschirmsperre nach 5 Minuten Inaktivität
- Unverzügliche Sperrung des Benutzers bei Austritt (Verwendung eines Laufzettels)

- Zugriffskontrolle

Die Germancard Technologie GmbH gewährleistet, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenüberprüfung vorgesehen ist. Dies geschieht durch:

- Datenverschlüsselung auf der gesamten Datenverbindungsstrecke, also zwischen Kunde und der Germancard Technologie GmbH
- Erstellung von Übermittlungsprotokollen

- Eine Zugriffsmatrix dokumentiert unter Berücksichtigung eines Berechtigungskonzepts welche Mitarbeiter auf welche Daten und Programme Zugriff haben. Bei Nutzerwechseln erfolgt eine Sperrung des nicht mehr verwendeten Accounts. Der neue Nutzer wird durch das Einsetzen in seinen Funktionsbereich automatisch mit den notwendigen Berechtigungen ausgestattet. Die Zugriffsrechte sind ausreichend differenziert und erfüllen das Need-to-know Prinzip.
- Papierunterlagen werden über geeignete Entsorgungscontainer gesammelt und einem zuverlässigen Entsorgungsunternehmen zur Vernichtung übergeben.

- Trennungskontrolle

Die Germancard Technologie GmbH gewährleistet, dass zu den unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dies geschieht durch:

- Mandantentrennung durch logische Datentrennung auf Basis von Kunden und Mandantennummern
- Vergabe von Zugriffsrechten

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

- Eingabekontrolle

Die Germancard Technologie GmbH gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dies geschieht durch:

- Organisatorische Festlegung von Zuständigkeiten
- Zugriffssteuerung
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines geeigneten Berechtigungskonzepts

3. Verfügbarkeit und Belastung der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle

Die Germancard Technologie GmbH gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dies geschieht durch:

- Regelmäßige Anfertigung von Datensicherungen (tägliche Erstellung von Sicherheitskopien)
- Auslagerung der Backupmedien an einen brandgeschützten Lagerungsort
- Einsatz einer unterbrechungsfreien Stromversorgung für Server
- Klimatisierte Serverräume mit Brandmeldern

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

Die Germancard Technologie GmbH gewährleistet, dass die Wirksamkeit der technisch organisatorischen Maßnahmen (TOM) regelmäßig durch geeignete Verfahren einer kritischen Begutachtung unterzogen und die daraus resultierenden Ergebnisse in regelmäßigen Abständen bewertet sowie die notwendigen Anpassungsmaßnahmen vorgenommen werden. Dies geschieht durch:

- Incident-Responds-Management
- Firewalls regelmäßig auf Updates hin überprüfen und diese auf Systeme laden
- USV regelmäßig kontrollieren
- Überprüfung und Widerherstellbarkeit von Backup-Dateien
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Auftragskontrolle

  Die Germancard Technologie GmbH gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Dies geschieht durch:

  - Abstimmung in der Auftragsorganisation mit dem Auftraggeber
  - Auftragsbezogene Protokollierungen und Kontrollmechanismen (Vollständigkeit, Durchlauf der Produktionskette)
  - Schulung und Information der Mitarbeiter

Für alle Fragen rund um den Datenschutz bei der Germancard Technologie GmbH steht Ihnen zur Verfügung:
Herr Yahya Zahad, Germancard Technologie GmbH Ottostraße 5, 50170 Kerpen
Tel.: 02273/601490, E-Mail: office@germancard.de

ribeka GmbH

Johann-Philipp-Reis-Str. 9
53332 Bornheim/Rheinland
Telefon +49 (0)2222-990600
Fax +49 (0)2222-990601
E-Mail info@ribeka.com
www.ribeka.com

Registergericht: Amtsgericht Bonn
Registernummer: HRB 8423
Vertretungsberechtigte Geschäftsführer:
Erich Berger, Dr. Jürgen Richter