Datenschutzrichtlinien

Inhalt

Einleitung

Diese Richtlinie regelt den Schutz personenbezogener Daten im Rahmen der Geschäftstätigkeit der CHROMOS Group.

Der Schutz personenbezogener Daten ist für die CHROMOS Group ein wichtiges Anliegen. Deshalb verarbeiten die Unternehmen der CHROMOS Group personenbezogene Daten ihrer Mitarbeiter, Kunden und Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

Die CHROMOS Group ist abhängig von Daten und Informationen und den daraus resultierenden elektronischen Geschäftsprozessen. Die Genauigkeit, Integrität und Verfügbarkeit von Daten und Informationen ist für die CHROMOS Group von grosser Wichtigkeit.

1. Räumlicher Anwendungsbereich

Diese Richtlinie findet Anwendung für die gesamte Verarbeitung (vgl. Ziff. 13 m) personenbezogener Daten (vgl. Ziff. 13 k) in der CHROMOS Group, unabhängig vom Ort der Verarbeitung.

2. Adressaten dieser Richtlinie / Verantwortlichkeiten / Sanktionen

Um effektiv eine datenschutzkonforme Informationsverarbeitung, Datensicherheit und angemessene Reaktionen auf Anliegen von der Datenverarbeitung Betroffener (vgl. Ziff. 13 d) sicherzustellen, richtet sich diese Richtlinie an jeden Mitarbeiter der Unternehmen der CHROMOS Group.

Die **Geschäftsführungen** der Unternehmen der CHROMOS Group tragen die Gesamtverantwortung für den Datenschutz und für die Umsetzung der datenschutzrechtlichen Vorgaben in den jeweiligen Unternehmen. Damit sind sie verpflichtet, durch organisatorische, personelle und technische Massnahmen eine ordnungsgemässe Datenverarbeitung unter Beachtung der gesetzlichen sowie der in dieser Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutzkontrollen durch Behörden ist der jeweils zuständige Datenschutzbeauftragte umgehend zu informieren. Soweit nicht abweichend vereinbart, sind alle Mitglieder der jeweiligen Geschäftsführung gemeinsam verantwortlich (Art. 26 Abs. 1 DSGVO).

Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Einhaltung der datenschutzrechtlichen Vorschriften im Rahmen der unternehmerischen Vorgaben verantwortlich, insbesondere die kontinuierliche Umsetzung dieser Richtlinie. Zudem werden alle Mitarbeiter der CHROMOS Group kontinuerlich bezüglich datenschutzrechtlicher Vorschriften geschult.

Die **Bereichsleitungen** haben über die Kontrolle ihres eigenen Verantwortungsbereiches hinaus sicherzustellen, dass ihre Mitarbeiter (ggf. auch temporär Beschäftigte) und/oder an den Prozessen

beteiligte Personen über diese Richtlinie informiert sind. Sie sind darüber hinaus in Bezug auf Datenerhebungen/-verarbeitungen in ihrem Bereich verantwortlich für

- die Bereitstellung erforderlicher sachlicher und personeller Ressourcen für Einhaltung der Richtlinienvorgaben,
- die Sicherstellung ordnungsgemässer Überwachung der Einhaltung der Richtlinienvorgaben,
- Sicherstellung der Erfüllung der Informationspflichten gegenüber Betroffenen,
- die Sicherstellung der vorgeschriebenen Verfahrensbeschreibungen,
- die Sicherstellung der vorgeschriebenen Datenschutzfolgeabschätzungen und
- die regelmässige Information des jeweils zuständigen Datenschutzbeauftragten (vgl. Ziff. 13 j) über die Erhebung und Verarbeitung personenbezogener Daten in ihrem Bereich.

Die **jeweils zuständigen Datenschutzbeauftragten** (vgl. Ziff. 13 j) der Unternehmen der CHROMOS Group beraten die Geschäftsführungen und andere Unternehmensmitarbeiter bei der Umsetzung dieser Richtlinie und prüfen deren Einhaltung. Sie führen ein Verzeichnis von Verarbeitungen des jeweiligen Unternehmens der CHROMOS Group gemäss Art. 30 DSGVO und bearbeiten Auskunfts-/Korrekturanfragen sowie datenschutzrechtliche Widersprüche von Betroffenen. Wenigstens einmal jährlich unterwerfen sie die technischen und organisatorischen Datenschutz-Massnahmen (vgl. Ziff. 11) in Zusammenarbeit mit den IT-Sicherheitsbeauftragten einer Kontrolle (vgl. Ziff. 9).

Der **IT-Sicherheitsbeauftragte** organisiert und unterstützt die Datenschutzbeauftragten bei der Erstellung des Verfahrensverzeichnisses. Der IT-Sicherheitsbeauftragte schlägt technische und organisatorische Massnahmen zur Gewährleistung dieser Richtlinie für die CHROMOS Group vor. Die Massnahmen sind in Abschnitt 11 dokumentiert. Alle Massnahmen gemäss dieser Richtlinie werden durch den IT-Sicherheitsbeauftragen regelmässig kontrolliert und die Kontrolle dokumentiert.

Der **Bereich Personal** erfüllt Auskunfts- und Einsichtsrechte von Mitarbeitern.

Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstösse gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

3. Grundprinzipien für die Verarbeitung personenbezogener Daten

3.1. Fairness und Rechtmässigkeit

Bei der Verarbeitung personenbezogener Daten in der CHROMOS Group werden die Persönlichkeitsrechte der Betroffenen (vgl. Ziff. 13 d) gewahrt. Personenbezogene Daten werden auf rechtmässige Weise und fair erhoben und verarbeitet.

3.2. Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

3.3. Transparenz

Der Betroffene (vgl. Ziff. 13 d) muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden:

- die Identität der verantwortlichen Stelle (vgl. Ziff. 13 n)
- den Zweck der Datenverarbeitung
- Dritte (vgl. Ziff. 13 f) oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

3.4. Datenvermeidung und Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten ist zu prüfen, ob und in welchem Umfang diese notwendig ist, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte (vgl. Ziff. 13 b) oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

3.5. Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich (vgl. Ziff. 13 h) sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde.

3.6. Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Massnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

3.7. Vertraulichkeit und Datensicherheit

Hinsichtlich personenbezogener Daten wird das Datengeheimnis gewahrt. Personenbezogene Daten werden daher im persönlichen Umgang vertraulich behandelt und durch angemessene organisatorische und technische Massnahmen gegen unberechtigten Zugriff, unrechtmässige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert.

4. Zulässigkeit der Verarbeitung von personenbezogenen Daten

4.1. Grundsätze der Datenverarbeitung

Die Verarbeitung personenbezogener Daten innerhalb der CHROMOS Group darf nur im Rahmen des rechtlich Zulässigen erfolgen. Grundsätzlich dürfen nur solche Informationen erhoben, verarbeitet

werden, die zur betrieblichen Aufgabenerfüllung erforderlich (vgl. Ziff. 13 h) sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

Eine Verarbeitung personenbezogener Daten ist nur zulässig bei Vorliegen eines der nachstehend näher dargelegten Erlaubnistatbestände, nämlich

- bei Vorliegen einer Einwilligung des Betroffenen (vgl. Ziff. 4.2),
- zur Erfüllung geäusserter Kundenanliegen und bei Vorliegen einer Werbeeinwilligung (vgl. Ziff. 4.3),
- bei Erforderlichkeit zur Anbahnung/Erfüllung eines Vertrages (vgl. Ziff. 4.4)
- bei Vorliegen einer gesetzlichen Erlaubnis (vgl. Ziff. 4.5) oder
- bei berechtigtem Interesse, ohne dass die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen (vgl. Ziff. 4.6).

Die jeweilige Zweckbestimmung der Daten ist vor Einführung neuer Arten von Verarbeitungen durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungs-Kriterien sind einzeln zu prüfen. Die Prüfung ist darüber hinaus auch zu einem ordnungsgemässen Nachweis zu dokumentieren.

Vor Einführung neuer Arten von Verarbeitungen personenbezogener Daten ist auch zu prüfen, ob bei Anonymisierung (vgl. Absatz 13 b) oder Pseudonymisierung der Daten der Verarbeitungszweck ebenso gut zu erreichen ist, und einer entsprechenden Verarbeitung ggf. der Vorzug zu gewähren.

Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierzu ein gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des erhebenden/verarbeitenden Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der jeweils zuständige Datenschutzbeauftragte zu konsultieren.

Für über das Internet verarbeitete personenbezogene Daten gelten die Bestimmungen in Abschnitt 4.8.

Die Verarbeitung von Mitarbeiterdaten richtet sich nach den Regelungen in Abschnitt 4.9.

4.2. Einwilligung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden.

Die Entgegennahme von Einwilligungen erfolgt stets im Bewusstsein, dass die Einwilligung des Betroffenen in die Verarbeitung personenbezogener Daten freiwillig ist. Vor der Einwilligung muss der Betroffene gemäss Ziff. 3.3 informiert werden. Erforderlich ist eine unmissverständlich abgegebene Willensbekundung des Betroffenen in Form einer Erklärung oder einer sonstigen eindeutigen bestä-

tigenden Handlung, mit der die betroffene Person ihr Einverständnis zur Verarbeitung der sie betreffenden Daten erteilt.

Die Einwilligung muss nachweisbar sein (Art. 7 Abs. 1 DSGVO). Vor diesem Hintergrund sind Einwilligungserklärungen schriftlich oder in elektronischer Textform einzuholen und zu speichern und/oder aufzubewahren. Sollte die Einwilligung in mit dem zuständigen Datenschutzbeauftragen abgestimmten Fällen mündlich, z. B. telefonmündlich, eingeholt werden, muss diese genau dokumentiert und die Dokumentation gespeichert und/oder aufbewahrt werden.

Vor dem 25. Mai 2018 erteilte Einwilligungen wirken fort, soweit sie die Grundsatzanforderungen der DSGVO erfüllen.

4.3. Datenverarbeitung zu Werbezwecken

Kundenbindungs- oder Werbemassnahmen bedürfen weiterer rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Sofern Daten ausschliesslich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene ist über die Freiwilligkeit der Angabe von Daten für diese Zwecke zu informieren. Vom Betroffenen ist eine Einwilligung (vgl. Ziff. 4.2) in die Verarbeitung seiner Daten zu Werbezwecken einzuholen. Der Betroffene soll im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen können.

Wendet sich ein Betroffener mit einem Informationsanliegen an ein Unternehmen der CHROMOS Group (z.B. Wunsch nach Zusendung von Informationsmaterial zu einer Leistung oder einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden.

4.4. Datenverarbeitung für eine vertragliche Beziehung

Rechtmässig ist die Verarbeitung personenbezogener Daten zur Begründung, Durchführung und Beendigung eines Vertrages (Art. 6 Abs. 1 lit. b DSGVO). Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht.

So können zum Beispiel im Rahmen bestehender Verträge regelmässig die Vertrags-, Stammdaten und Abrechnungsdaten des Vertragspartners, wie etwa sein Name und seine Adresse, verarbeitet werden, um beispielsweise die Rechnung oder die Lieferung zu adressieren.

In der Vertragsanbahnungsphase ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Vertragsdokumenten oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Hierzu zählen auch Datenverar-

beitungsvorgänge, die zur Anbahnung oder im Rahmen von Beschäftigungsverhältnissen erforderlich sind.

Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäusserte Einschränkungen sind zu beachten.

Für darüber hinausgehende Werbemassnahmen müssen die in Ziff. 4.3 genannten Voraussetzungen erfüllt sein.

4.5. Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Datenverarbeitungen sind auch rechtmässig, wenn sie die durch oder aufgrund von Rechtsvorschriften erforderlich sind. Rechtsgrundlage dafür können nationale wie auch unionsrechtliche Vorschriften sein, denen wir bzw. die jeweils handelnden Personen unterliegen, (Art. 6 Abs. 1 lit. c DSGVO).

Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

Beispiel hierfür sind die handels- und steuerrechtlichen Vorschriften, welche uns z. T. umfangreiche Dokumentations- und Aufbewahrungspflichten auferlegen.

4.6. Überwiegende berechtigte Interessen

Die Verarbeitung personenbezogener Daten darf auch erfolgen, wenn dies zur Wahrung unserer berechtigten Interessen oder der eines Dritten (vgl. Ziff. 13 f) erforderlich sind. Als „berechtigte Interessen“ sind vor allem rechtliche (z.B. Durchsetzung von offenen Forderungen) und wirtschaftliche (z.B. Vermeidung von Vertragsstörungen) Interessen anzusehen.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf jedoch nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen (Art. 6 Abs. 1 lit. f DSGVO). Es sind also in jedem solchen Fall die schutzwürdigen Interessen der von der Datenverarbeitung betroffenen Personen zu prüfen. Im Rahmen einer umfassenden Interessenabwägung ist sodann festzustellen, welche Interessen überwiegen – unsere oder die der betroffenen Personen. In Zweifelsfällen ist der jeweils zuständige Datenschutzbeauftragte zu konsultieren.

4.7. Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten (vgl. Ziff. 13 c) darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen.

Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der jeweils zuständige Datenschutzbeauftragte (vgl. Ziff. 13 j) zu informieren.

Die Verarbeitung von Kreditkarten-Daten erfolgt unter Einhaltung der PCI-DSS-Compliance-Vorgaben gemäss der beschriebenen Massnahmen in Anhang 1 dieser Richtlinie.

4.8. Nutzerdaten und Internet

Werden auf Internetseiten oder in Apps der CHROMOS Group personenbezogene Daten verarbeitet, so sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

Wenn zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt werden (Tracking), werden die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert. Ein personenbezogenes Tracking darf nur erfolgen, wenn der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out).

Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

4.9. Verarbeitung zur Anbahnung/im Rahmen eines Beschäftigungsverhältnisses

Im Rahmen der Anbahnung und Durchführung von Beschäftigungsverhältnissen dürfen solche personenbezogene Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Beschäftigungsvertrages erforderlich sind.

Bei der Anbahnung eines Beschäftigungsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Unternehmen der CHROMOS Group erforderlich.

Im Rahmen bestehender Beschäftigungsverhältnisse muss die Datenverarbeitung immer auf den Zweck des Beschäftigungsvertrages bezogen sein, sofern nicht ein anderer der vorstehend in diesem Abschnitt 4 genannten Legitimationsgründe gegeben ist.

Ist während der Anbahnung des Beschäftigungsverhältnisses oder in einem bestehenden Beschäftigungsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten (vgl. Ziff. 13 f) erforderlich, ist im Zweifel eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Beschäftigungsverhältnisses stehen, jedoch nicht originär der Erfüllung des Beschäftigungsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, im Rahmen der datenschutzrechtlichen Vorgaben zu gestaltende Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder unsererseits bestehende, überwiegende berechtigte Interessen (vgl. Ziff. 4.6) sein. Besteht ein gesetzlicher oder vereinbarter Handlungsspielraum, sind stets die schutzwürdigen Interessen des Mitarbeiters zu berücksichtigen.

Kontrollmassnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismässigkeit der Kontrollmassnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmassnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Massnahme betroffenen Mitarbeiters am Ausschluss der Massnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Massnahme festgestellt und dokumentiert werden. Etwaige Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen sind dabei zu berücksichtigen.

Telefonanlagen, E-Mail-Accounts, Intranet und Internet sowie interne soziale Netzwerke werden den Beschäftigten zur Erledigung der betrieblichen Aufgaben durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Vorgaben genutzt werden. Im Falle der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das Telekommunikationsrecht zu beachten, soweit dies Anwendung findet.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmassnahmen an den Übergängen in das Netz der CHROMOS Group implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Accounts, des Intranets und Internets sowie der internen sozialen Netzwerke zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstosses gegen Gesetze oder Vorgaben der CHROMOS Groupund deren Unternehmen erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismässigkeitsprinzips erfolgen. Die jeweils einschlägigen Gesetze sind ebenso zu beachten wie bestehenden Unternehmensvorgaben.

5. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger ausserhalb der CHROMOS Group oder an Empfänger innerhalb der CHROMOS Group unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten gemäss Abschnitt 4. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

Im Falle einer Datenübermittlung an einen Empfänger ausserhalb der CHROMOS Group in einem Drittstaat (vgl. Ziff. 13 g) muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Eine solche gesetzliche Verpflichtung kann sich aus dem nationalen Recht ergeben oder das nationale Recht erkennt das mit der gesetzlichen Verpflichtung eines Drittstaats verfolgte Ziel der Datenübermittlung an.

Im Falle einer Datenübermittlung von Dritten an Unternehmen der CHROMOS Group muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

6. Pflichten bei Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist sowohl mit externen Auftragnehmern als auch zwischen Unternehmen der CHROMOS Group eine Vereinbarung über eine Auftragsverarbeitung abzuschliessen. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Geschäftsbereich muss ihre Umsetzung sicherstellen.

a) Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmassnahmen auszuwählen.
b) Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
c) Die vom jeweils zuständigen Datenschutzbeauftragen bereitgestellten Vertragsstandards müssen beachtet werden.
d) Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung oder sonstiger geeigneter Datensicherheitsbelege nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit zu wiederholen.
e) Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die gesetzlichen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:

(1) Vereinbarung der EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern,
(2) Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus,
(3) Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz-Aufsichtsbehörden.

7. Rechte von Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

a) Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Wenn im Rahmen eines Beschäftigungsverhältnisses weitergehende arbeitsrechtliche Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.
b) Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.
c) Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
d) Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Im Falle des Widerspruchs für diese Zwecke müssen seine Daten gesperrt werden.
e) Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
f) Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet

8. Vertraulichkeit

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Verarbeitung ist sämtlichen Mitarbeitern der CHROMOS Group untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein.

Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

Alle Mitarbeiter werden bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichtet und hierauf verpflichtet. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

9. Datenschutzkontrolle / Rechenschaftsbericht

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmässig, wenigstens einmal jährlich, im Rahmen von Datenschutzkontrollen überprüft. Die Durchführung obliegt den jeweils zuständigen Datenschutzbeauftragten, ggf. unter Hinzuziehung der IT-Sicherheitsbeauftragten sowie ggf. weiteren mit Auditrechten ausgestatteten Unternehmensbereichen oder beauftragten externen Prüfern.

Die Ergebnisse fasst der jeweils zuständige Datenschutzbeauftragte einmal jährlich in einem Rechenschaftsbericht zusammen, der wenigstens folgende Punkte beinhaltet:

- neue Verfahrensbeschreibungen
- Datenschutzvorfälle
- Personenbezogene Anfragen

Des Weiteren ist dem Rechenschaftsbericht eine Auflistung der durch den jeweiligen Datenschutzbeauftragten zu dokumentierenden Lösch- und Änderungsanfragen von personenbezogenen Daten als Anlage beizufügen.

Über die wesentlichen Ergebnisse der Datenschutzkontrollen sind die jeweiligen Geschäftsführungen der Unternehmen der CHROMOS Group zu informieren. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

10. Datenschutzvorfälle

Jeder Mitarbeiter muss seinem jeweiligen Vorgesetzten und den jeweils zuständigen Datenschutzbeauftragten unverzüglich Fälle von Verstössen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle, vgl. Ziff. 13 e) melden.

Bei

- unrechtmässiger Übermittlung personenbezogener Daten an Dritte,
- unrechtmässigem Zugriff durch Dritte auf personenbezogene Daten, oder
- Verlust personenbezogener Daten

veranlasst der jeweils zuständige Datenschutzbeauftragte, soweit der Datenschutzvorfall zu einem Risiko für Betroffene führt, die nach Art. 33 DSGVO vorgeschriebene Meldung an die zuständige Aufsichtsbehörde.

Soweit

- durch den Datenschutzvorfall ein hohes Risiko für Rechte und Freiheiten von Betroffenen besteht,
- keine geeigneten technischen und organisatorischen Massnahmen vorhanden sind, die den unbefugten Zugang zu personenbezogenen Daten verhindern (z. B. Verschlüsselung) und
- keine wirksamen Massnahmen zur Schadensbegrenzung ergriffen wurden, die das zum Zeitpunkt des Datenschutzvorfalls bestandene hohe Risiko eliminiert haben

veranlasst der jeweils zuständige Datenschutzbeauftragte die nach Art. 34 DSGVO vorgeschriebene Benachrichtigung des Betroffenen.

11. Technische und organisatorische Sicherheitsmassnahmen

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmässige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Massnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Massnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (vgl. Schutzstufen gemäss Abschnitt 12) zu orientieren.

Die Massnahmen werden jährlich überprüft und bei Bedarf angepasst. Überprüfung und Anpassungen werden dokumentiert.

Folgende technische und organisatorische Massnahmen sind in den Unternehmen der CHROMOS Group getroffen:

Zutrittskontrolle	Zutrittsbeschränkung von Personen zu Räumen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	• Daten der Schutzstufe A: Gebäude Schliessanlage oder Hauswart; Räume im Gebäude nicht abschliessbar, normale Arbeitsplätze • Arbeitsplätze mit Zugriff auf Daten der Schutzstufe C und D; zusätzlich Raumtüren abschliessbar, • Serverräume; Einbruchmeldeanlage, Zutrittsgesichert mit Protokoll, keine Fenster, für Daten aller Schutzstufen
Zugangskontrolle	Zugangsbeschränkung zu Daten und Datenverarbeitungsgeräten um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können	• Daten der Schutzstufe A-C; normaler Arbeitsplatz (incl. virtuelle Umgebung) mit AD-Kontrolle ohne externen Zugriff. • Daten der Schutzstufe A und B; Normaler Arbeitsplatz mit externem Zugriff über das Web. zusätzlich gesonderte Sicherheitsschicht (Netscaler) • Serverzugriff; Für Daten aller Schutzstufen, gesonderte Authentifizierung (entweder AD plus Admin-AD oder AD für PC plus lokale Anmeldung Server)
Zugriffskontrolle	Zugriffsbeschränkung auf Daten innerhalb einer Applikation um zu 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	• Applikation für Daten der Schutzstufe A: keine Rechte und Rollenvergabe • Applikation für Daten der Schutzstufe B: Einfache Anmeldung an der Applikation • Applikation für Daten der Schutzstufe C: Rechte und Rollenkonzept • Applikation für Daten der Schutzstufe D: Rechte und Rollenkonzept, zwei Faktor Authentifizierung • Für Personendatenverarbeitung aller Schutzstufen mit öffentlich/rechtlichen Charakter (Sozialversicherung, Arbeitsamt, Gericht etc.) müssen die von öffentlich/rechtlichen Organschaft vorgegebenen Zugriffskontrollen verwendet werden.

Weitergabe-kontrolle	Es muss verhindert werden, dass personenbezogene Daten bei der elektronischen Übertragung oder beim Transport oder bei der Speicherung auf Datenträgern unbefugt gelesen, kopiert, verändert oder gelöscht werden können und dass festgestellt werden kann, an welchen Stellen eine Übermittlung solcher Daten im DV-System vorgesehen ist.	• Daten der Schutzklasse A und B: keine zusätzliche Beschränkung, bei Webübertragung Transportverschlüsselung (Https) • Daten der Schutzstufe C: zusätzlich Übermittlungsprotokollierung (protokolliert in Microsoft Navision) • Daten der Schutzstufe D: zusätzlich Inhaltsverschlüsselung • Für Personendatenverarbeitung aller Schutzstufen mit öffentlich/rechtlichen Charakter (Sozialversicherung, Arbeitsamt, Gericht etc.) müssen die von öffentlich/rechtlichen Organschaft vorgegebenen Weitergabekontrollen verwendet werden.
Eingabekontrolle	Es muss sichergestellt werden, dass nachträglich überprüft werden kann ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht worden sind.	• Daten der Schutzstufe A: eine Eingabekontrolle ist nicht notwendig • Daten der Schutzstufe B und höher: Sachbearbeitungsprotokollierung • Für Personendatenverarbeitung aller Schutzstufen mit öffentlich/rechtlichen Charakter (Sozialversicherung, Arbeitsamt, Gericht etc) müssen die von öffentlich/rechtlichen Organschaft vorgegebenen Eingabekontrollen verwendet werden.
Auftragskontrolle	Es muss sichergestellt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, gemäss den Weisungen des Auftraggebers verarbeitet werden.	• Erzeugung eines Datensicherheitskonzeptes (TOM) in Abhängigkeit von den Schutzstufe entsprechend dieser Ausführung

Verfügbarkeits-kontrolle	Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt werden.	• Daten der Schutzstufe A: Virenschutz • Ab Daten der Schutzstufe B: zusätzlich Snapshots, Backupkonzept • Ab Daten der Schutzstufe C: zusätzlich Klimaanlage, USV • Ab Daten der Schutzstufe D: zusätzlich Aufbewahrung an getrennten Orten • Für Personendatenverarbeitung aller Schutzstufen mit öffentlich/rechtlichen Charakter (Sozialversicherung, Arbeitsamt, Gericht etc.) müssen die von öffentlich/rechtlichen Organschaft vorgegebenen Verfügbarkeitskontrollen verwendet werden.
Trennungsgebot	Es ist sicher zu stellen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden können.	• Für Daten aller Schutzstufen; Mandantentrennung, Buchungskreise

12. Schutzstufen

Um die technischen und organisatorischen Sicherheitsmassnahmen (vgl. Ziff. 11) bezüglich ihrer Angemessenheit bewerten zu können, sind personenbezogene Daten je nach Schadenspotential (Grad möglicher Beeinträchtigung schutzwürdiger Belange) in die nachfolgenden Schadens-/Schutzstufen unterteilt:

Stufe A:
Frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z.B. Adressbücher, Mitgliederverzeichnisse, Print- und Online-verzeichnisse.

Stufe B:
Personenbezogene Daten, deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. beschränkt zugängliche öffentliche Dateien, Kundenaufträge, Verträge mit Geschäftspartnern.

Stufe C:
Personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann ("Ansehen"), z.B. Einkommen, Sozialleistungen, Grundsteuer, Ordnungswidrigkeiten, Arbeitsverträge (ohne Gesundheitsdaten).

Stufe D:
Personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen

Verhältnisse des Betroffenen erheblich beeinträchtigen kann ("Existenz"), z.B. Ordnungswidrigkeiten schwerwiegender Art, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Insolvenzen.

Stufe E:
Daten, deren Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann, z.B. Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können.

13. Definitionen

a) **Angemessenes Datenschutzniveau** von Drittstaaten ist ein von der EU Kommission anerkanntes Datenschutzniveau eines Nicht-EU-Staates, nach dem der Kernbestand der Privatsphäre, so wie er in den Mitgliedstaaten der EU übereinstimmend verstanden wird, im Wesentlichen geschützt wird. Die EU Kommission berücksichtigt bei ihrer Entscheidung alle Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Dies schliesst die Beurteilung staatlichen Rechts sowie der jeweiligen geltenden Standesregeln und Sicherheitsmassnahmen ein.

b) **Anonymisierte Daten** sind solche, bei denen ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismässig grossen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

c) **Besonders schutzwürdige Daten** sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

d) **Betroffener** im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden.

e) **Datenschutzvorfälle** sind alle Ereignisse, bei denen der begründete Verdacht besteht, dass personenbezogene Daten rechtswidrig ausgespäht, erhoben, verändert, kopiert, übermittelt oder genutzt wurden. Das kann sich sowohl auf Handlungen durch Dritte als auch Mitarbeiter beziehen.

f) **Dritter** ist jeder ausserhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle. Auftragsdatenverarbeiter sind innerhalb der EU nicht Dritte im Sinne des Datenschutzrechtes, da sie gesetzlich der verantwortlichen Stelle zugeordnet sind.

g) **Drittstaaten** im Sinne der Datenschutzrichtlinie sind alle Staaten ausserhalb der Europäischen Union und des EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU Kommission als angemessen anerkannt worden ist.

h) **Erforderlich** ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismässig hohem Aufwand zu erreichen ist.

i) **Europäischer Wirtschaftsraum (EWR)** ist ein mit der EU assoziierter Wirtschaftsraum, dem Norwegen, Island und Liechtenstein angehören.

j) **Jeweils zuständiger Datenschutzbeauftragter** ist der/die für das jeweilige Unternehmen der CHROMOS Group bestellte Datenschutzbeauftragte.

k) **Personenbezogene Daten** sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann.

l) **Übermittlung** ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.

m) **Verarbeitung personenbezogener Daten** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.

n) **Verantwortliche Stelle** ist diejenige juristisch selbständige Gesellschaft der CHROMOS Group, deren Geschäftsaktivität die jeweilige Verarbeitungsmassnahme veranlasst.

Anhang 1: PCI-DSS-Compliance

Die Verarbeitung von Kreditkarten-Daten erfolgt in der CHROMOS Group unter Einhaltung der nachstehenden PCI-DSS-Compliance-Vorgaben:

- SAQ 12.8.1:
  Es muss eine Liste von Dienstanbietern geführt werden. Die Liste muss eine Beschreibung der jeweils erbrachten Leistungen enthalten. Die Liste ist von IT-Sicherheit zu führen. Alle Bereichsverantwortliche sind verpflichtet, Änderungen bzgl. der Dienstanbieter unverzüglich an IT-Sicherheit zu melden.

- SAQ 12.8.2
  Jeder Dienstanbieter muss mit den jeweiligen Unternehmen der CHROMOS Group eine schriftliche Vereinbarung zum Schutz von Karteninhaberdaten vereinbaren. IT-Sicherheit muss die Vereinbarung und die Richtlinie zur Umsetzung der Vereinbarung überprüfen.

- SAQ 12.8.3:
  IT-Sicherheit muss ein Verfahren etablieren das bei der Auswahl von Dienstanbietern verpflichtend einzuhalten ist.

- SAQ 12.8.4:
  IT-Sicherheit überprüft einmal jährlich die PCI-DSS-Compliance von Dienstanbietern und dokumentiert diese.

- SAQ 12.8.5:
  IT-Sicherheit dokumentiert alle PCI-DSS-Anforderungen und vermerkt dabei die Verantwortlichkeit (eigen oder Dienstanbieter).

- SAQ 12.10.1:
  IT-Sicherheit sorgt dafür, dass Störungen im Incident-Response-Verfahren umgesetzt werden.