Impressum

Herausgeber:
Skizunft Markgröningen e.V.

Adresse:

Skizunft Markgröningen e.V.
z.Hd. Thomas Porth

Eckenerstr. 3/1
71706 Markgröningen

Tel. +49 7145 8325
Email: info@skizunft-markgroeningen.de
www.skizunft-markgroeningen.de

Geschäftsstelle:
Marktplatz 10
71706 Markgröningen

Vereinsregister: Amtsgericht Ludwigsburg Nr.????

Webmaster: Philipp Lutz
eMail: info@skizunft-markgroeningen.de

Bilder: Alle, die irgendwo eine Kamera dabei haben.
Hinweis: Sollte sich jemand an Bildern stören bzw. möchte das Bilder gelöscht werden sollen, soll dies an den Webmaster mit Angabe der Bildquelle melden. Diese werden dann zeitnah gelöscht.

Hinweise gemäß Teledienstgesetz
Für Internetseiten Dritter, auf die wir mit Hyperlinks verweisen, tragen die jeweiligen Anbieter die Verantwortung. Die Skizunft Markgröningen e.V. ist für den Inhalt solcher Seiten Dritter nicht verantwortlich.Die Webseiten der Skizunft Markgröningen e.V. können von anderen Seiten ohne unser Wissen verlinkt sein. Skizunft Markgröningen e.V. übernimmt diesbezüglich keine Verantwortung für den Inhalt auf den Webseiten Dritter.
Für fremde, rechtswidrige oder strafbare Inhalte ist Skizunft Markgröningen e.V. nur dann verantwortlich, wenn er von ihnen Kenntnis hat und es dem Skizunft Markgröningen e.V. technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Skizunft Markgröningen e.V. ist nach dem Teledienstgesetz jedoch nicht verpflichtet, die fremden Inhalte ständig zu überprüfen.

Dateschutz

Haftung für Inhalte

Die Inhalte unserer Seiten wurden mit größter Sorgfalt erstellt. Für die Richtigkeit, Vollständigkeit und Aktualität der Inhalte können wir jedoch keine Gewähr übernehmen. Als Diensteanbieter sind wir gemäß § 7 Abs.1 TMG für eigene Inhalte auf diesen Seiten nach den allgemeinen Gesetzen verantwortlich. Nach §§ 8 bis 10 TMG sind wir als Diensteanbieter jedoch nicht verpflichtet, übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen bleiben hiervon unberührt. Eine diesbezügliche Haftung ist jedoch erst ab dem Zeitpunkt der Kenntnis einer konkreten Rechtsverletzung möglich. Bei Bekanntwerden von entsprechenden Rechtsverletzungen werden wir diese Inhalte umgehend entfernen.

Haftung für Links

Unser Angebot enthält Links zu externen Webseiten Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich. Die verlinkten Seiten wurden zum Zeitpunkt der Verlinkung auf mögliche Rechtsverstöße überprüft. Rechtswidrige Inhalte waren zum Zeitpunkt der Verlinkung nicht erkennbar. Eine permanente inhaltliche Kontrolle der verlinkten Seiten ist jedoch ohne konkrete Anhaltspunkte einer Rechtsverletzung nicht zumutbar. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Urheberrecht

Die durch die Seitenbetreiber erstellten Inhalte und Werke auf diesen Seiten unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechtes bedürfen der schriftlichen Zustimmung des jeweiligen Autors bzw. Erstellers. Downloads und Kopien dieser Seite sind nur für den privaten, nicht kommerziellen Gebrauch gestattet. Soweit die Inhalte auf dieser Seite nicht vom Betreiber erstellt wurden, werden die Urheberrechte Dritter beachtet. Insbesondere werden Inhalte Dritter als solche gekennzeichnet. Sollten Sie trotzdem auf eine Urheberrechtsverletzung aufmerksam werden, bitten wir um einen entsprechenden Hinweis. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Inhalte umgehend entfernen.

Datenschutz

Die Nutzung unserer Webseite ist in der Regel ohne Angabe personenbezogener Daten möglich. Soweit auf unseren Seiten personenbezogene Daten (beispielsweise Name, Anschrift oder eMail-Adressen) erhoben werden, erfolgt dies, soweit möglich, stets auf freiwilliger Basis. Diese Daten werden ohne Ihre ausdrückliche Zustimmung nicht an Dritte weitergegeben.

Wir weisen darauf hin, dass die Datenübertragung im Internet (z.B. bei der Kommunikation per E-Mail) Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich.

Der Nutzung von im Rahmen der Impressumspflicht veröffentlichten Kontaktdaten durch Dritte zur

Übersendung von nicht ausdrücklich angeforderter Werbung und Informationsmaterialien wird hiermit ausdrücklich widersprochen. Die Betreiber der Seiten behalten sich ausdrücklich rechtliche Schritte im Falle der unverlangten Zusendung von Werbeinformationen, etwa durch Spam-Mails, vor.

Datenschutzerklärung für die Nutzung von Facebook-Plugins (Like-Button)

Auf unseren Seiten sind Plugins des sozialen Netzwerks Facebook, 1601 South California Avenue, Palo Alto, CA 94304, USA integriert. Die Facebook-Plugins erkennen Sie an dem Facebook-Logo oder dem "Like-Button" ("Gefällt mir") auf unserer Seite. Eine Übersicht über die Facebook-Plugins finden Sie hier: http://developers.facebook.com/docs/plugins/.
Wenn Sie unsere Seiten besuchen, wird über das Plugin eine direkte Verbindung zwischen Ihrem Browser und dem Facebook-Server hergestellt. Facebook erhält dadurch die Information, dass Sie mit Ihrer IP-Adresse unsere Seite besucht haben. Wenn Sie den Facebook "Like-Button" anklicken während Sie in Ihrem Facebook-Account eingeloggt sind, können Sie die Inhalte unserer Seiten auf Ihrem Facebook-Profil verlinken. Dadurch kann Facebook den Besuch unserer Seiten Ihrem Benutzerkonto zuordnen. Wir weisen darauf hin, dass wir als Anbieter der Seiten keine Kenntnis vom Inhalt der übermittelten Daten sowie deren Nutzung durch Facebook erhalten. Weitere Informationen hierzu finden Sie in der Datenschutzerklärung von facebook unter http://de-de.facebook.com/policy.php

Wenn Sie nicht wünschen, dass Facebook den Besuch unserer Seiten Ihrem Facebook-Nutzerkonto zuordnen kann, loggen Sie sich bitte aus Ihrem Facebook-Benutzerkonto aus.

Datenschutzerklärung für die Nutzung von Google Analytics

Diese Website benutzt Google Analytics, einen Webanalysedienst der Google Inc. ("Google"). Google Analytics verwendet sog. "Cookies", Textdateien, die auf Ihrem Computer gespeichert werden und die eine Analyse der Benutzung der Website durch Sie ermöglicht. Die durch den Cookie erzeugten Informationen über Ihre Benutzung dieser Website (einschließlich Ihrer IP-Adresse) wird an einen Server von Google in den USA übertragen und dort gespeichert.

Google wird diese Informationen benutzen, um Ihre Nutzung der Website auszuwerten, um Reports über die Websiteaktivitäten für die Websitebetreiber zusammenzustellen und um weitere mit der Websitenutzung und der Internetnutzung verbundene Dienstleistungen zu erbringen. Auch wird Google diese Informationen gegebenenfalls an Dritte übertragen, sofern dies gesetzlich vorgeschrieben ist oder soweit Dritte diese Daten im Auftrag von Google verarbeiten. Google wird in keinem Fall Ihre IP-Adresse mit anderen Daten der Google Inc. in Verbindung bringen.

Sie können die Installation der Cookies durch eine entsprechende Einstellung Ihrer Browser Software verhindern; wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen dieser Website voll umfänglich nutzen können. Durch die Nutzung dieser Website erklären Sie sich mit der Bearbeitung der über Sie erhobenen Daten durch Google in der zuvor beschriebenen Art und Weise und zu dem zuvor benannten Zweck einverstanden.

Datenschutzerklärung für die Nutzung von Google Adsense

Diese Website benutzt Google AdSense, einen Dienst zum Einbinden von Werbeanzeigen der Google Inc. ("Google"). Google AdSense verwendet sog. "Cookies", Textdateien, die auf Ihrem Computer gespeichert werden und die eine Analyse der Benutzung der Website ermöglicht. Google AdSense verwendet auch so genannte Web Beacons (unsichtbare Grafiken). Durch diese Web Beacons können Informationen wie der Besucherverkehr auf diesen Seiten ausgewertet werden.

Die durch Cookies und Web Beacons erzeugten Informationen über die Benutzung dieser Website

(einschließlich Ihrer IP-Adresse) und Auslieferung von Werbeformaten werden an einen Server von Google in den USA übertragen und dort gespeichert. Diese Informationen können von Google an Vertragspartner von Google weiter gegeben werden. Google wird Ihre IP-Adresse jedoch nicht mit anderen von Ihnen gespeicherten Daten zusammenführen.

Sie können die Installation der Cookies durch eine entsprechende Einstellung Ihrer Browser Software verhindern; wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen dieser Website voll umfänglich nutzen können. Durch die Nutzung dieser Website erklären Sie sich mit der Bearbeitung der über Sie erhobenen Daten durch Google in der zuvor beschriebenen Art und Weise und zu dem zuvor benannten Zweck einverstanden.

Datenschutzerklärung für die Nutzung von Google +1

Erfassung und Weitergabe von Informationen:
Mithilfe der Google +1-Schaltfläche können Sie Informationen weltweit veröffentlichen. über die Google +1-Schaltfläche erhalten Sie und andere Nutzer personalisierte Inhalte von Google und unseren Partnern. Google speichert sowohl die Information, dass Sie für einen Inhalt +1 gegeben haben, als auch Informationen über die Seite, die Sie beim Klicken auf +1 angesehen haben. Ihre +1 können als Hinweise zusammen mit Ihrem Profilnamen und Ihrem Foto in Google-Diensten, wie etwa in Suchergebnissen oder in Ihrem Google-Profil, oder an anderen Stellen auf Websites und Anzeigen im Internet eingeblendet werden.
Google zeichnet Informationen über Ihre +1-Aktivitäten auf, um die Google-Dienste für Sie und andere zu verbessern. Um die Google +1-Schaltfläche verwenden zu können, benötigen Sie ein weltweit sichtbares, öffentliches Google-Profil, das zumindest den für das Profil gewählten Namen enthalten muss. Dieser Name wird in allen Google-Diensten verwendet. In manchen Fällen kann dieser Name auch einen anderen Namen ersetzen, den Sie beim Teilen von Inhalten über Ihr Google-Konto verwendet haben. Die Identität Ihres Google-Profils kann Nutzern angezeigt werden, die Ihre E-Mail-Adresse kennen oder über andere identifizierende Informationen von Ihnen verfügen.

Verwendung der erfassten Informationen:
Neben den oben erläuterten Verwendungszwecken werden die von Ihnen bereitgestellten Informationen gemäß den geltenden Google-Datenschutzbestimmungen genutzt. Google veröffentlicht möglicherweise zusammengefasste Statistiken über die +1-Aktivitäten der Nutzer bzw. gibt diese an Nutzer und Partner weiter, wie etwa Publisher, Inserenten oder verbundene Websites.

Quellen: Disclaimer *von eRecht24, dem Portal zum Internetrecht von Rechtsanwalt Sören Siebert,* eRecht24 Datenschutzerklärung für Facebook, Datenschutzerklärung für Google Analytics, Google Adsense Haftungsausschluss, Datenschutzerklärung Google +1

Datenschutzgrundverordnung

Erläuterungen zu Technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO

In dem Vertrag müssen die technischen und organisatorischen Maßnahmen festgelegt werden, die bei der Datenverarbeitung umzusetzen sind.

Rechtsgrundlage ist § 32 DSGVO, in dem beschrieben ist, welche Prüfungen ein Auftraggeber vor einer Auftragsvergabe durchzuführen hat. So muss der Auftragnehmer unter besonderer Berücksichtigung der Zuverlässigkeit und der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden. Im Auftrag sind insbesondere die technischen und organisatorischen Maßnahmen schriftlich festzulegen. Auch hat der Auftraggeber zu prüfen, ob beim Auftragnehmer erforderliche Maßnahmen getroffen werden.

Werden personenbezogene Daten verarbeitet, deren Verarbeitung für die Betroffenen keine besonderen Risiken erwarten lässt, so bietet das Grundschutzhandbuch des BSI für bestimmte technische Konstellationen einen Katalog an Sicherheitsmaßnahmen.

Wenn der Auftragnehmer ein Datensicherheitskonzept (sollte ein solches Datensicherheitskonzept vorliegen, bitten wir um Übermittlung) besitzt, muss der Auftraggeber prüfen und schriftlich festlegen, ob es seinen Anforderungen entspricht. Die Sicherheitsziele sind in der Anlage zu § 9 BDSG genannt. Ist das Konzept nicht ausreichend, sind ergänzende Maßnahmen zu vereinbaren. Das daraus resultierende Sicherheitskonzept sollte zum Vertragsbestandteil gemacht werden. In diesem Fall kann darauf verzichtet werden, im Sicherheitskonzept genannte Maßnahmen im Vertrag zu wiederholen.

Wenn der Auftragnehmer kein Datensicherheitskonzept vorlegen kann, müssen die Maßnahmen im Vertrag vereinbart werden. Dabei sind wiederum die in der Anlage zu § 9 BDSG genannten Sicherheitsziele zu erreichen. Aus dem Katalog sollten die einzelnen Maßnahmen in den Vertrag übernommen werden. Es handelt sich um keinen abschließenden Maßnahmenkatalog. Insbesondere bei der Verarbessxitung sensibler Daten sind in der Regel zusätzliche Maßnahmen erforderlich.

Besonders wichtig sind Regelungen zu folgenden Sachverhalten:

- V e r a n t w o r t l i c h k e i t e n: Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken.

- A b s c h o t t u n g v o n N e t z e n: Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine absolute Sicherheit zu erreichen ist, müssen derartige Versuche erkannt werden. Technische Komponenten, die in Betracht kommen, sind Firewalls, Intrusion Detection Systeme und insbesondere dem Stand der Technik entsprechende Verschlüsselungsverfahren.

- A b h ö r e n d e r K o m m u n i k a t i o n: Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten entsprechend dem Stand der Technik zu verschlüsseln.

- Ab m e l d e p r o z e d u r e n: Die Abmeldung am System oder Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Personen überwinden müssen. An dieser Stelle müssen qualitativ hochwertige Maßnahmen ergriffen werden.-

  Beschreibung der technischen und organisatorischen Maßnahmen zu VI Datensicherungsmaßnahmen

1. Zutrittskontrolle

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Die vom Auftragnehmer gemieteten Server (physische Maschinen) stehen in klimatisierten Räumen der tldHost AG (Adresse dort) in einem Dunkelrechenzentrum. Dunkelrechenzentren werden personallos betrieben und werden, außer in Störungsfällen, nicht betreten. Die Störungs-Überwachung des Rechenzentrums obliegt der tldHost, Störungen und deren Behebung sowie geplante Unterbrechungen zu Maintenancezwecken werden informiert.

Zutritt zu den Serverräumen haben nur ausgewählte Mitarbeiter der tldHost über biometrische Authentifizierung.

2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Die Server sind exclusiv zur Nutzung durch den Auftragnehmer und seine Kunden eingerichtet. Dritte Kunden der tldHost haben darauf keinen Zugriff – die Administration der Server obliegt alleine dem Auftragnehmer und wird auch nur von den durch den Auftragnehmer benannten Personen durchgeführt.

Der Anwendungsserver ist mit einem Zertifikat belegt (https-Zugang) - alle in eMemberline eingerichteten User können per Kunden-spezifischer URL auf ihr jeweiliges System (Applikationen und Datenbanken) zugreifen.

Das Zertifikat wird jährlich erneuert/upgedatet.

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

In jedem kundenspezifischen System werden die zugehörigen Nutzer eingerichtet mit der jeweiligen Nutzerberechtigung. Die Basis-Benutzerberechtigungen sind dabei

- Nutzer mit vollerBerechtigung (Zugriff, Verändern,Löschen,Administratorfunktionen,die das Einrichten von Nutzern beinhaltet und Datenbankberechtigung)

- Nutzer mit Teilberechtigung aus den Basisberechtigungen

- reine Auskunftsnutzer ohne jede weitere Berechtigung.

Jedem Benutzer wird ein Initialpasswort zugeteilt, das er anschließend selbst ändern muss. Die Passwörter werden verschlüsselt gespeichert und können nicht reproduziert werden. Bei Verlust wird ein neues Initialpasswort vergeben vom Administrator.

Die Anmeldeversuche werden mitgezählt und beim 4. vergeblichen Versuch wird der Benutzer gesperrt – der Login-Zähler kann mit Administratorfunktion im Benutzerprofil zurückgesetzt und

ggfls. ein neues Passwort zugeteilt werden. Passwörter sind mindestens 8 Stellen lang und müssen

Buchstaben (case-sensitiv), Zahlen und/oder Sonderzeichen enthalten. Zur Änderungshäufigkeit werden Empfehlungen vergeben, alle 4 Wochen zu ändern.

Die Administration der User wird in der Regel durch den Kundenadministrator durchgeführt.

Der Auftragnehmer hat einen eigenen Nutzer eingerichtet, dessen Zugangsdaten nur ihm bekannt sind. Zur schnellen Problemlösung ist ein solcher Zugang wichtig, kann aber auf Wunsch des Kunden gelöscht bzw. gesperrt werden und nur im Problemfall freigeschaltet werden (hier wäre der doppelte Zugang zum System einsetzbar oder durch kundenseitige Eintragung eines neuen Passwortes, das dem Auftragnehmer zu jedem Einsatz mitgeteilt werden müsste).

Weitere, programmbezogene oder daten(bereichs)bezogene Benutzerberechtigungen oder Ausschlüsse von Berechtigungen sind auf Wunsch des Kunden möglich. So sind zu den Basisberechtigungen weitere datenbereichs- oder funktionsbezogene Einschränkungen möglich.

Eine optionale erweiterte Zugangsberechtigung ist mit der doppelten Anmeldung möglich. Hier wird nach der normalen Anmeldung mit Nutzername und Passwort ein 4-stelliger Zahlencode per Zufallsmethode erzeugt und dem Nutzer per eMail oder SMS (Eintrag ins Nutzerprofil) mitgeteilt. Erst nach Eingabe dieses Zahlencodes gelangt der Nutzer in sein eMemberline. Der Zahlencode ist nur für eine Session gültig, nach jeder Anmeldung wird ein neuer Code generiert.

Dieses VerfahrenkannauchsinnvollfürtemporäreZugangsberechtigungengenutztwerden(Aushilfen etc.), ein Löschen der eMailadresse oder der Mobilfunknummer im Nutzerprofil hat zur Folge, dass ein Zugang nicht mehr möglich ist.

Die Einrichtung der Benutzer und deren Berechtigungen werden in der Regel vom Kundenadministrator vorgenommen (Basisberechtigungen), weitergehende Berechtigungen müssen durch den Auftragnehmer vergeben werden, wenn diese nicht schon zur Systemerstnutzung eingerichtet wurden.

Die Gültigkeit von Zugangsberechtigungen werden vom Kunden gepflegt – so sind Mitarbeiter/Nutzer sofort nach Verlassen des/der Vereins/Verbandes/Organisation zu sperren bzw. zur Sperrung mitzuteilen.

(Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsselungsverfahren entsprechend dem Stand der Technik. Bei Online-Zugriffen des Auftraggebers ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.)

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.

Explizite systemimmanente Datenübertragungen finden nicht statt. An zwei Punkten sind im System Schnittstellen notwendig:

- bei Einsatz eines Buchhaltungssystem, werden die erzeugten Buchungen über eine zwischen

Buchhaltungssystem undeMemberlineeingerichteteSchnittstelleexportiertbzw.importiert,

- beim SEPA-Lastschriftverfahren wird eine SEPA-Datei (XML-Format) erzeugt, die entweder in ein Onlinebanking oder in ein Bankprogramm eingespeist werden.-

Für beide Verfahren ist für die technische Kopplung bzw. die organisatorische Trennung der Kunde selbst verantwortlich. Der Kunde muss Daten auf externen Trägern bzw. bei Übermittlung per eMail selbst verschlüsseln.

Die SEPA-Dateien sollten nach der Verarbeitung auf den Kundenrechnern gelöscht werden, da eine Reproduktion über die Historienfunktion jederzeit möglich ist.

(Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

5. Dateneingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Personenbezogene Daten werden ausschließlich durch den Kunden selbst eingeben, verändert oder verarbeitet. eMemberline schreibt alle Veränderungen und Dateneingaben mit; jedes Feld wird mit altem/neuem Inhalt und mit durchführendem Nutzer sowie Datum protokolliert. Die Änderungsprotokolle können durch den Kundenadministrator gelöscht werden. Die Änderungsprotokolle werden mit gesichert.

Der Auftragnehmer gewährleistet keine Aufbewahrung, wenn die Änderungen vom Kunden gelöscht werden – außer in den Sicherungen.

(Sämtliche Systemaktivitäten werden protokolliert; die Protokolle werden mindestens 3 Jahre lang durch den Auftragnehmer aufbewahrt.)

6. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Alle Daten und Datenbanken sowie auf dem Server abgelegte Dokumente werden nächtlich gesichert. An Wochenenden werden freitags und sonntags Sicherungen gezogen. Am Monatsende werden zusätzlich alle Anwendungsprogramme gesichert. Zusätzliche Sicherungen können für den Kunden zum Download in regelmäßigen Abständen (wöchentlich, monatlich etc.) zur Verfügung gestellt werden. Die täglichen Sicherungen werden nach 14 Tagen gelöscht, Monatssicherungen werden nach Jahresende gelöscht und Jahresend-Sicherungen nach 10 Jahren.

Die Sicherungen sind auf dem Auftragnehmer - Datenbankserver abgelegt, zusätzlich werden alle Datenbanken auf einem weiteren Server durch tldHost gesichert, um in Katastrophenfällen eine schnelle Systemwiederherstellung zu gewährleisten.

(Sicherungskopien des Datenbestandes werden in folgenden Verfahren hergestellt: hier Beschreibung von Rhythmus, Medium, Aufbewahrungszeit und Aufbewahrungsort für Back-up-

Kopien.)

7. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. entfällt