IT-Verbund endica der Stadtwerke

kommunale informationsverarbeitung baden-franken

Allgemeine technische und organisatorische Maßnahmen

gemäß Art. 32 Abs. 1 DS-GVO

www.kivbf.de

Dokumentenlenkung

Dokumentenhistorie			
Version	Datum	Autor	Kommentar
1.0	04.11.2015	Josef Bergner, Christoph Franz	Erstellung
1.1	13.05.2016	Christoph Franz	Anpassung Vorbemerkung Zertifizierung
1.1.1	24.05.2018	Matthias Stumpf	endica-Version

Aufbewahrungsort
Das Dokument ist in Dokumea gespeichert unter:
KIVBF-Zentrale Services ➔ Datenschutz/Revision ➔ Datenschutz ➔ Verfahrensverzeichnisse ➔ Anlagen zu den Punkten 9 und 10 des Verfahrensverzeichnisses

Zugriffsregelung	
Editierrechte pdf-Datei:	IT-SB, Datenschutz g
Leserechte pdf-Datei:	Alle-kivbf,Alle-endica
Editierrechte Word-Datei:	IT-SB, Datenschutz g
Leserechte Word-Datei:	
Klassifizierung	Intern

Inhaltsverzeichnis

1 Vorbemerkungen

Umfassende, allgemeingültige Darstellung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO für Auftragsverarbeiter (Art. 30 Abs. 2 Buchst. d DS-GVO)

Die en*dica* GmbH hat nach den in Art. 32 Abs. 1 DS-GVO vorgesehenen Kontrollbereichen die nachstehend aufgeführten technischen und organisatorischen Maßnahmen ergriffen. Sie gelten als generelle Maßnahmen in allen Bereichen, in denen sie anwendbar sind. In einzelnen Verfahren und Lösungen der en*dica* GmbH sind ergänzende Maßnahmen getroffen, die in den jeweiligen speziellen Verfahrensverzeichnissen bzw. Meldungen aufgeführt werden.

Gleichbehandlung der Geschlechter im Sprach- und Schriftgebrauch (Gender Mainstreaming)

Wir weisen darauf hin, dass im Hinblick auf eine bessere Lesbarkeit und einer verkürzten Darstellung überall dort, wo die männliche Form im üblichen Sprachgebrauch verwendet wird oder als kürzere Form der angesprochenen Personenkreise gelten kann (Mitarbeiter und Mitarbeiterinnen), diese hier verwendet wurde, dabei jedoch immer auch die weibliche Form gemeint ist.

Geltungsbereich der allgemeinen technischen und organisatorischen Maßnahmen

Die Unternehmensgruppe Kommunale Informationsverarbeitung Baden-Franken (KIVBF) umfasst den Zweckverband Kommunale Informationsverarbeitung Baden-Franken (ZV KIVBF) und die Kommunales Rechenzentrum Baden-Franken GmbH (KRBF). Ebenfalls Teil der Unternehmensgruppe ist die endica GmbH (en*dica*)

Der ZV KIVBF und die en*dica* GmbH bedienen sich für die gesamte Produktion der KRBF
Diese allgemeinen technischen und organisatorischen Maßnahmen gelten für alle drei Betriebe: KIVBF, KRBF und endica.

Zertifizierung
Die KIVBF ist zertifiziert:

- ISO27001-Zertizierung nach IT-Grundschutz (BSI-Zertifizierung)
- ISO27001:2013-Zertifzierung

Bei beiden Zertifizierungen wurde derselbe Untersuchungsgegenstand betrachtet. Dieser ist dem BSI-Zertifikat zu entnehmen, welches auf der Homepage der KIVBF veröffentlicht ist.

2 Technische und organisatorische Maßnahmen der Kontrollbereiche

2.1 Organisationskontrolle

2.1.1 Datenschutzbeauftragter/IT-Sicherheitsbeauftragter

Die en*dica* GmbH hat einen behördlichen Datenschutzbeauftragten bestellt und seinen Aufgabenbereich ergänzend zu den gesetzlichen Vorgaben inhaltlich in seinem Bestellungsschreiben näher bestimmt.
Zusätzlich sind ein IT-Sicherheitsbeauftragter und dessen Stellvertreter bestellt. Hier wurden die Aufgaben und Pflichten im Bestellungsschreiben definiert.
Neben der Beratung der Beschäftigten und der Unternehmensleitung in Fragen des Datenschutzes und Informationssicherheit, kontrollieren beide Stellen die Einhaltung der vorgegebenen (Datenschutz-)Maßnahmen.

2.1.2 Verpflichtung auf Einhaltung des Datengeheimnisses

Die Beschäftigten der en*dica* GmbH sind bereits durch Gesetz auf das Datengeheimnis verpflichtet, da sie Beschäftigte einer öffentlich-rechtlichen Körperschaft sind. Zur Verdeutlichung werden dennoch alle Beschäftigten förmlich auf das Datengeheimnis und auch auf andere gesetzlich vorgegebene Geheimniswahrungsvorschriften verpflichtet.

Beauftragt die en*dica* GmbH einen Dritten, wird dieser Auftragnehmer schriftlich auf die Einhaltung der gesetzlichen Bestimmungen, der anzuwendenden Datenschutzgesetze bzw. datenschutzrechtlichen Regelungen im speziellen Rechtsgebiet verpflichtet und überwacht.

2.1.3 Trennung der Arbeitsphasen/Rollen-/Funktionstrennung

Bei der en*dica* GmbH wird die organisatorische Trennung (Funktionstrennung) der verschiedenen Bereiche eingehalten:
So gibt es für Teilbereiche der Administration unterschiedliche Rollen (Netzwerk, Serveradministration, Datenbankadministration, Endgeräteadministration). Die Programmierung und das Druckoutputmanagement sind ebenfalls eigene organisatorische Bereiche.
Die Geschäftsverteilung ist in der Allgemeinen Geschäftsordnung (AGO) mit der Anlage Geschäftsverteilungsplan geregelt

2.1.4 schriftliche Anweisungen/-vereinbarungen

Dienstanweisungen und Dienstvereinbarungen sind erstellt und im Prozessmanagement für alle Mitarbeiter veröffentlicht. So gibt es Dienstanweisungen und Dienstvereinbarungen (Betriebsanweisungen/-vereinbarungen) zu folgenden Themenbereichen

- Sicherheit im Gebäude
- Nutzung der PC-Ausstattung
- Nutzung von Internetdiensten

Zusätzlich existieren im Sicherheitsmanagement Prozessrichtlinien und Vorgaben zu folgenden Themenbereichen:

- IT-Sicherheitsleitlinie für MitarbeiterInnen
- IT-Betrieb und Serverbetrieb
- Virenschutz
- Patch-Management
- Netzwerke und Firewalls

Eine Benutzungsordnung regelt das Verhältnis zwischen en*dica* GmbH und Kunden und enthält Regelung zu

- Betrieb zentraler Verfahren und Zugriff
- Datenschutzrechtliche Bestimmungen
- IT-Sicherheits-Grundsätze

2.1.5 Mitarbeiterinformationen

Jährlich finden an allen Standorten Mitarbeiterschulungen statt. In diesen Schulungen unterrichten der Datenschutzbeauftragte und IT-Sicherheitsbeauftragte alle Mitarbeiter über die rechtlichen und organisatorischen Vorgaben.
Neue Mitarbeiter erhalten die grundlegenden Informationen zum Datenschutz und Informationssicherheit im Rahmen der Einführungsveranstaltung.

2.1.6 Datenträgerverwaltung

Datenträger werden vom zuständigen Bereich technisch verwaltet, dokumentiert und in einem speziell gesicherten Raum vorgehalten. Die Verwaltung der Medienbestände erfolgt automatisiert durch das Managementsystem.
Eine Entsorgung von magnetischen Datenträgern erfolgt ausschließlich über den zuständigen Bereich, der die Datenträger vor Verlassen des Hauses mit einen BSI-zertifizierter Degausser löscht und diese Löschung protokolliert.

2.1.7 Verfahrensverzeichnis

Im Rahmen der Ausgestaltung der Auftragsdatenverarbeitung stellt die en*dica* GmbH alle zentralen Verfahren die Inhalte für das Verfahrensverzeichnis zur Verfügung. Allerdings nur in dem Umfang, wie es durch die en*dica* GmbH geführt werden kann.

2.1.8 Richtlinie zur Entwicklung von DV-Verfahren

Es existieren entsprechende Entwicklungsrichtlinien in den jeweiligen Programmierbereichen. Eine IT-Sicherheitsrichtlinie zur Systementwicklung ist veröffentlich und kommuniziert.

2.1.9 Verfahrensdokumentation

Verantwortlich für die Verfahrensdokumentation ist der Produktmanager der jeweiligen Lösung.

2.1.10 Brand- und Katastrophenordnung

Im Rahmen des Risikomanagements wurde ein Krisenhandbuch erstellt, in dem die Aufgaben, Besetzungen und Zuständigkeiten von Krisenstäben und die Verhaltensregeln und Maßnahmenkataloge für bestimmte Schadensereignisse festgelegt wurden. Dieses Handbuch wird fortgeschrieben. In unregelmäßigen Abständen werden einzelne Krisen- und Katastrophenszenarien als Rahmenübung durchgespielt.

2.2 Zutrittskontrolle

2.2.1 Gebäudeschutz außen

Das Gebäude der Betriebsstätte Karlsruhe (RZ-Standort) wurde bereits als Rechenzentrumsgebäude geplant und gebaut, so dass von Beginn an viele sicherheitsrelevante bauliche Vorkehrungen und Maßnahmen verwirklicht werden konnten.

Der Standort wurde sorgfältig ausgewählt und als freistehender Gebäudekomplex gebaut. Die Räume der zentralen Datenverarbeitung sind weder im Erdgeschoss noch von außen einsehbar oder erreichbar. Es wurden nur zwei Zugänge hergestellt Haupt- (Personal-)Eingang und ein Ein-/Ausgang für Materialan- und –Ablieferungen). Das Gebäude wurde in Stahlbetonbauweise ausgeführt, die Räume der zentralen EDV-Anlagen (Rechen- und Speichereinheiten, Archivierung, zentrale Netzkomponenten) wurden durch verstärkte Wände und Stahltüren abgesichert. Die Scheiben im Erdgeschoss sind aus Spezialglas. Die Aufzüge und die sonstigen Schächte sind, wie die aus Gründen des Personenschutzes im Brand- und Katastrophenfall vorgeschriebenen Fluchttüren, in das Sicherungskonzept einbezogen und durch eine geeignete Alarmanlage abgesichert. Die Alarmanlage in sich ist gesondert gesichert. Das zugehörige Grundstück ist durch einen stabilen Metallzaun von einer Höhe von 2 m gegen einen einfachen Zutritt abgegrenzt.

2.2.2 Gebäudeschutz innen

Allgemein:
Die Zugangstüren sind mit Sicherheitsschlössern nach VdS ausgestattet. Bei unverschlossenen Schlössern kann die geschlossene Türe von außen jedoch nur über einen elektrisch auszulösenden Entriegelungsvorgang geöffnet werden. Für dessen Bedienung besteht an jeder Dienststelle ein einheitliches automatisches Zugangskontroll-(Schließ-)System, das mit einem personenbezogenen elektronischen Zugangschip bedient wird. Mit Ausnahme der besonders zu schützenden Bereiche (siehe unten) werden innerhalb des Rechenzentrums keine Zutrittsbewegungen festgehalten, während die Zu- und Abgänge zum Gebäude bei ordnungsgemäßer Bedienung der Anlage protokolliert werden. Schlüssel werden zentral verwaltet und die Ausgabe und Rückgabe von Schlüsseln wird protokolliert.
Fluchttüren können bauartbedingt nur von Innen geöffnet werden und sind an die zentrale Alarmanlage angeschlossen.

Besucher:
Alle Besucher (Kunden, Schulungsteilnehmer, Fremdfirmenmitarbeiter) werden mit Namen, Arbeitgeber, Grund des Besuchs bzw. besuchte Person und der Zeit des Eintreffens und Verlassens registriert. Schulungsteilnehmer dürfen sich nur im Schulungsbereich aufhalten. Der Zugang und Aufenthalt in nichtöffentlichen Bereichen ist nur in Begleitung eines Rechenzentrumsmitarbeiters zulässig. Besonders schutzbedürftige Bereiche sind durch an die Schließanlage angeschlossene Türen abgesichert. Fremdfirmenmitarbeiter werden nach Art der Tätigkeit im Haus angemessen überwacht.

Büroräume:
Alle Büroflure der Standorte der en*dica* GmbH sind ebenfalls über das zentrale Zutrittssystem geschützt.

Druckstraße:
Der Zutritt zu den Druckerstraßen ist nur einem eingeschränkten Mitarbeiterkreis über das Zutrittssystem möglich.

Serverräumlichkeiten:
Hier ist der Zutritt nur einem eingeschränkten Mitarbeiterkreis über das Zutrittssystem möglich. Der Zugang zu den zentralen Serverräumlichkeiten erfolgt über eine durch ein Fernsehmonitorsystem überwachte Schleuse. Zutritt und Verlassen dieses zentralen Sicherheitsbereiches werden protokolliert. Fremdfirmenmitarbeiter dürfen in diesem Bereich nicht ohne Aufsicht tätig sein.

2.3 Datenträgerkontrolle

2.3.1 Organisation der Datenträgerverwaltung

Die Verwaltung der Festplatten des laufenden Rechenzentrumsbetriebs erfolgt grundsätzlich im SAN-Verbund mit RAID-Technologie, welches sich im Serverraum befindet.
Werden Datensicherungen auf Festplatten durchgeführt (Backup-to-Disk) so befinden sich diese ebenfalls in einem SAN-Verbund, allerdings in einem anderen Brandabschnitt in den Serverräumlichkeiten.
Die SAN-Verbünde verwalten die Datenträger

Werden die Datensicherung auf Band durchgeführt (Backup-to-Tape) erfolgt die Verwaltung der Magnetbänder durch das zugehörige Managementsystem in den Serverräumlichkeiten.

Alle Datenträger in den Serverräumlichkeiten befinden sich in verschließbaren Schränken oder Behältern.

2.3.2 Ordnungsgemäße Vernichtung von Datenträgern

Eine Entsorgung von magnetischen Datenträgern erfolgt ausschließlich über den zuständigen Bereich, der die Datenträger vor Verlassen des Hauses mit einen BSI-zertifizierter Degausser löscht und diese Löschung protokolliert.

Papier als Datenträger wird durch zertifizierte Entsorger einer Vernichtung zugeführt. Innerhalb der Standorte erfolgt eine Sammlung von sicherheitskritischem Papier in verschlossenen Behältnissen.

2.4 Speicher-, Benutzer-, Zugriffs-, Eingabekontrolle

Für die Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle und Eingabekontrolle können die Maßnahmen im Wesentlichen unter dem Stichwort Benutzer- und Berechtigungsverwaltung zusammengefasst werden, so dass die nachstehenden Maßnahmen für alle Kontrollbereiche stehen. Dabei ist immer Voraussetzung, dass eine angemessene Protokollierung erfolgt.

Maßnahmen in den vorgenannten Kontrollbereichen setzen eine ausgeprägte Benutzer- und Berechtigungsverwaltung im organisatorischen und technischen Sinne voraus sowie eine umfassende Protokollierung der Vorgänge im DV-System.

Der Zugriff auf Datenspeicher, auf denen personenbezogene Daten gespeichert sind, erfolgt für Benutzer ausschließlich durch Programme. Direkte Zugriffe auf Datenbanksysteme werden durch das Datenbankmanagement protokolliert.

Allgemein:
Das Rechenzentrum setzt nur Programme ein, die entweder bereits eine ihrer Bedeutung nach geeignete Benutzer- und Berechtigungsverwaltung enthalten oder für die eine geeignete Benutzer- und Berechtigungsverwaltung durch zusätzliche Software ermöglicht wird. Die Wirksamkeit der Berechtigungsvergabe wird in Testeinrichtungen überprüft oder vom Hersteller der Programme gewährleistet. Benutzerkennungen werden immer personenbezogen vergeben, so dass über die Protokollierung nachvollzogen werden kann, wer wann in welcher Art auf die Daten zugegriffen hat. In den Programmen vorgesehene Protokollierungen werden genutzt.
Eine Kontrolle der Protokolldaten findet nur anlassbezogen statt.

en*dica* GmbH sichert den Zugang zum Rechenzentrumsnetz und somit den Zugang der Kunden zu den zentralen Anwendungen durch geeignete Hard- und Software ab. Außerdem sind innerhalb des zentralen Netzes der en*dica* GmbH Programme zur Abwehr unberechtigter Eindringversuche (Intrusion Detection Systeme) und unterschiedliche Virenscan-Programme im Einsatz.

Die Benutzer- und Berechtigungsverwaltung obliegt dem Kunden.
Die Benutzer- und Berechtigungsverwaltung für zentrale Verfahren wird durch die en*dica* GmbH nach der Vorgabe des Kunden (Auftraggeber) erbracht.
Innerhalb einzelner Verfahren ist es möglich, dass die Benutzer- und Berechtigungsverwaltung durch die Kunden selbst durchgeführt wird.
Dabei setzt die en*dica* GmbH voraus, dass die Kunden die Ihnen durch die en*dica* GmbH zur Verfügung gestellten Möglichkeiten der Zugangs- und Zugriffs-(Berechtigungs-)Verwaltung im Sinne ihrer Verantwortung nutzen.

Die Kunden haben auch dafür zu sorgen, dass die bei ihnen angeschlossenen IT-Endgeräte nicht durch Unberechtigte genutzt werden können (z. B. automatisches Sperren des Endgerätes, Protokollierung der fehlerhaften Zugriffsversuche).

Im Zuge der Eingabekontrolle kontrolliert die KIVBF zusätzlich, soweit das innerhalb der Verarbeitung eingerichtet ist, ob die Daten in die richtigen Dateien und Formate für die Weiterverarbeitung dem Verfahren übergeben werden.

Über Terminpläne und festgelegte Job-Abläufe gewährleistet die KIVBF, dass die eingegangenen Daten zur richtigen Zeit in die Produktion weitergegeben werden.

2.5 Übermittlungskontrolle

Der Datenverkehr innerhalb des Datennetzes der en*dica* GmbH findet ausschließlich über vertrauenswürdige Verbindungen statt. Personenbezogene Daten, die aus IT-Anwendung heraus übertragen werden müssen, werden bereits durch die Übertragungssoftware gesteuert und geprüft ob die die physische Übermittlung richtig war. Bei der Datenübermittlung werden Übermittlungsprotokolle erstellt, die von den Sachbearbeitern der en*dica* GmbH kontrolliert werden.

2.6 Auftragskontrolle

Soweit die en*dica* GmbH Teile der ihr übertragenen Auftragsdatenverarbeitung durch Dritte im Rahmen eines Unterauftrags verarbeiten lässt, sucht en*dica* GmbH diese Auftragnehmer sorgfältig unter Beachtung der für das grundsätzliche Auftragsverhältnis geltenden Auftragsbedingungen, insbesondere zum Datenschutz aus.

Die Leistungsfähigkeit des Unterauftragnehmers richtet sich in erster Linie nach den von ihm getroffenen Maßnahmen zum Datenschutz. Dabei lässt sich die en*dica* GmbH die unbedingte Weisungsbefugnis und das Kontrollrecht vertraglich zusichern. Soweit die Unteraufträge nicht bereits im Vertrag inhaltlich eindeutig bestimmt sind, erfolgen Verarbeitungen nur auf Einzelanweisungen durch Mitarbeiter der en*dica* GmbH, die darüber Protokoll führen. Die Leistungen der Unterauftragnehmer werden regelmäßig überprüft.

Die en*dica* GmbH erledigt die ihr übertragene Auftragsverarbeitung nur und ausschließlich in dem im Auftrag vorgegebenem Umfang. Einzelweisungen an die en*dica* GmbH müssen schriftlich erfolgen. Im Zuge des Einsatzes elektronischer Medien kann die Weisung auch mittels einer elektronischen Nachricht erfolgen. Im Zweifel wird die en*dica* GmbH bei solchen Einzelweisungen oder Verarbeitungs-aufträgen auch urschriftliche Anweisungen anfordern. Sie müssen klar, eindeutig und vollständig sein; die Kompetenzen zwischen Auftraggeber und Auftragnehmer müssen auch für den Einzelfall eindeutig beschrieben und klar abgegrenzt sein. Im Rahmen der jährlichen Unterrichtung der Beschäftigten der en*dica* GmbH durch den Datenschutzbeauftragten wird jedes Mal darauf hingewiesen, dass Verarbeitungen nur im Rahmen der vorliegenden Anweisungen durchgeführt werden dürfen.

2.7 Transportkontrolle

Der Datenverkehr innerhalb des Datennetzes der en*dica* GmbH findet ausschließlich über vertrauenswürdige Verbindungen statt.

Datenträger für den Betrieb des Backup-Rechenzentrums (siehe Nr. 2.8.3) bzw. für extern zu lagernde Sicherungsdatenträger werden in sicheren Behältern und Fahrzeugen transportiert.

Der Transport gedruckten Daten zwischen den Standorten der en*dica* GmbH erfolgt durch einen Kurierdienst. Je nach Vertraulichkeitsstufe werden die Unterlagen in verschlossenen Umschlägen weitergegeben. Der Transport von Daten oder Ergebnisunterlagen innerhalb der Standorte der KIVBF erfolgt grundsätzlich geschützt gegen einfache Kenntnisnahme.

Soweit Datenträger, insbesondere Ausdrucke, an die Auftraggeber ausgeliefert werden, geschieht dies über Postdienstleister, die dem Briefgeheimnis unterliegen
Datenträger für einen Empfänger werden zusammengefasst und in geeignete Behältnisse zum Schutz vor unbefugter Kenntnisnahme gegeben.
Die beteiligten Unternehmen wurden vertraglich auf unsere datenschutzrechtlichen Vorgaben verpflichtet.

Unmittelbar auf Datenträger ausgegebene Verarbeitungsergebnisse werden innerhalb des Druckbereichs in vorgegebenen Strukturen und Wegen bis zum Empfänger geleitet. An- und Auslieferungswege sowie das Personal ist genau festgelegt. Nur die Sachbearbeiter des jeweiligen Fachbereichs haben bei Bedarf Zutritt.

2.8 Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle überschneidet sich mit einigen anderen Maßnahmen; hier werden die Sicherheitsanforderungen aus einer anderen Sicht dargestellt. Die en*dica* GmbH betreibt ein Risikomanagement. In diesem werden zur Minderung der verschiedenen Risiken vorbeugende Maßnahmen festgeschrieben und soweit verhältnismäßig, umgesetzt. Für die Beseitigung von Störungen sind ITIL-konforme Incident- und Problem-Management-Prozesse implementiert. Zusätzlich sind im Rahmen des Krisenmanagements verschiedene Szenearien für die Aufrechterhaltung des Geschäftsbetriebes und des Wiederanlaufs beschrieben.

2.8.1 Sicherung der Funktionsfähigkeit

In Karlsruhe sind Anlagen für eine für eine unterbrechungsfreie Stromversorgung installiert und werden regelmäßig getestet. Die Klimakühlgeräte sind redundant ausgelegt. Die Klimabedingungen werden automatisiert überwacht und im Fehlerfall an die zuständigen Mitarbeiter gemeldet.

2.8.2 Sicherungen für den Notfall

Im Gesamten Gebäude sind Feuermelder installiert, die regelmäßig gewartet werden. Feuerlöschen sind an den vorgeschriebenen Standorten teilweise in doppelter Ausführung installiert und werden ebenfalls regelmäßig gewartet. Es sind Brandschutzhelfer eingeteilt und ausgebildet. Wassereinbruch wird über Leckage-Melde-Einrichtungen gemeldet und selbsttätige Pumpanlagen entwässern die betroffenen Bereiche.

2.8.3 Sicherung und Wiederherstellung von Datenbeständen

Die Datenbestände werden regelmäßig gemäß dem Sicherungskonzept gesichert, um einen kontinuierlichen Produktionsbetrieb zu gewährleisten. Diese Betriebssicherungen werden ständig erneuert und in einem separaten Brandabschnitt verfügbar gehalten (= interne Datensicherung). Das Zurückspielen der Sicherungen wird regelmäßig getestet.

Die Datenbestände werden außerdem zusätzlich regelmäßig an einen externen Lagerort gebracht (= externe Datensicherung). Zweck dieser externen Sicherung ist die Verfügbarkeit im Katastrophenfall.

Die en*dica* GmbH unterhält ein Backup-Rechenzentrum, in dem sich alle aktuellen Programme und die notwendigen Daten befinden, um im Katastrophenfall (z. B. Zerstörung der Betriebsstätte Karlsruhe) die Verarbeitung für die Kunden im Mindestumfang weiterlaufen lassen zu können. Der Wiederanlauf in diesem Backup-Rechenzentrum wird regelmäßig geübt.

2.9 Trennungsgebot (nach BDSG)

2.9.1 Physikalische Trennung

Eine physikalische Trennung wird aufgrund eines stark virtualisierten RZ-Betriebs nur bei unterschiedlichen Schutzbedarfsbereichen umgesetzt. Zonen und Systeme gleichen Schutzbedarfs werden physisch nicht getrennt.

2.9.2 Logische Trennung

Innerhalb der angebotenen zentralen mandantenfähigen Verfahren findet i.d.R. eine Speicherung der Daten in einer gemeinsamen Datenbank statt. Infolge der in den Programmen vorgesehenen Mandantentrennung und der dazu eingerichteten Datenverwaltung (auch Berechtigungsverwaltung innerhalb eines Mandanten) kann bei ordnungsgemäßem Umgang mit den Berechtigungswerkzeugen sichergestellt werden, dass die Daten nur zu dem vorgesehenen Zweck verarbeitet werden. Die KIVBF hat dafür alle vorbereitenden Maßnahmen getroffen.

Bei nicht mandantenfähigen Verfahren werden die Daten logisch, meist auf Datenbankinstanzen getrennt. Bei anders strukturierten Daten werden individuelle Zugriffs- und Berechtigungskonzepte erarbeitet und umgesetzt.

Copyright

Stabstelle Datenschutz

Josef Bergner
Fon
Fax
josef.bergner@kivbf.de
www.endica.de