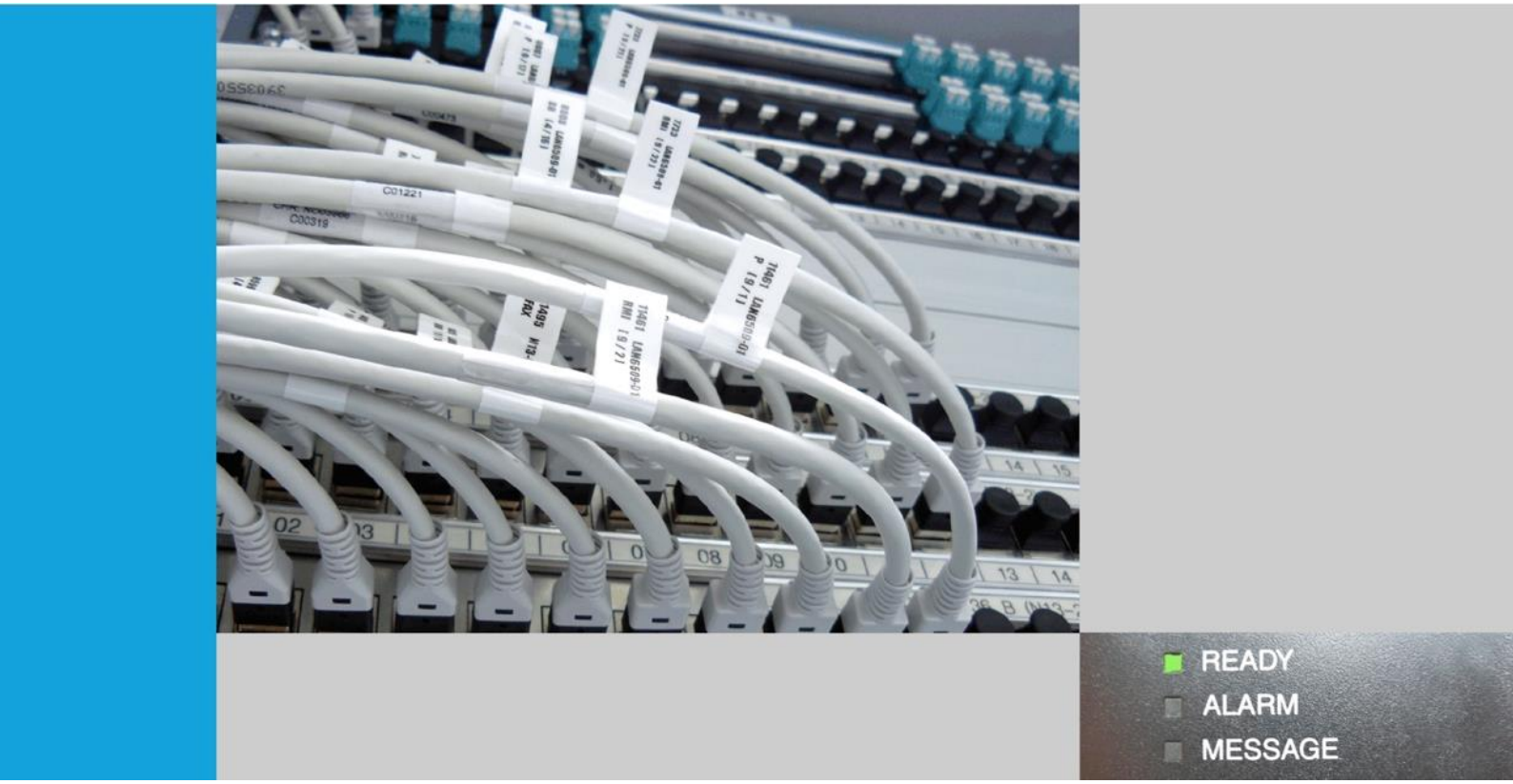
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



Datenschutzkonzept

Version: 1.1

Autor: Beauftragte für den Datenschutz IT-Dienstleistungszentrum Bayern

München, Mai 2018

Inhalt

1 Zielsetzung

Das IT-Dienstleistungszentrum des Freistaats Bayern (IT-DLZ) im Bayerischen Landesamt für Digitalisierung, Breitband und Vermessung (LDBV) ist das staatliche Rechenzentrum für Verwaltung und Gerichte des Freistaats Bayern. Als solches nimmt es Verarbeitungen von Daten im Auftrag öffentlicher Stellen des Freistaates Bayern wahr. Zur Erfüllung dieser Aufgaben erbringt das IT-DLZ IT-Services unterschiedlicher Ausprägungen zentral an Standorten des IT-DLZ und an Standorten öffentlicher Stellen.

Dieses Datenschutzkonzept beschreibt das Datenschutzniveau, das das IT-DLZ bei der Verarbeitung von personenbezogenen Daten unbeschadet abweichender Vereinbarungen allgemein gewährleistet.

2 Geltungsbereich

Das Datenschutzkonzept gilt für die Verarbeitung von Daten sowohl in eigenen Angelegenheiten des IT-DLZ als auch durch das IT-DLZ im Kundenauftrag.

3 Rechtlicher Rahmen

3.1 Allgemein

Die Zuständigkeit des IT-DLZ für informations- und kommunikationstechnische Aufgaben im Freistaat Bayern regelt insbesondere Art. 12 Abs. 3 Satz 2 des Bayerischen Vermessungs- und Katastergesetzes (VermKatG).

3.2 Verarbeitung in eigenen Angelegenheiten

Als staatliche Stelle des Freistaats Bayern sind auf das IT-DLZ bei der Verarbeitung von personenbezogenen Daten primär die Vorschriften der Datenschutzgrundverordnung (DSGVO) und des Bayerischen Datenschutzgesetzes (BayDSG) anzuwenden.

3.3 Verarbeitung im Auftrag

Nehmen öffentliche Stellen des Freistaats Bayern Dienstleistungen des IT-DLZ in Anspruch stellt dies regelmäßig eine Verarbeitung von Daten im Auftrag im Sinne der Datenschutzgesetze dar.

Für das IT-DLZ gelten dann neben der DSGVO und dem BayDSG, indirekt auch die für die jeweiligen öffentlichen Stellen anzuwendenden bereichsspezifischen Vorschriften über den Datenschutz (wie z.B. Sozialgesetzbuch (SGB), Bundesdatenschutzgesetz (BDSG), Asylgesetz (AsylG), Bayerisches Statistikgesetz (BayStatG), Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG), Bayerisches Archivgesetz (BayArchivG), Abgabenordnung (AO) etc.).

Zudem sind die Vorschriften des Kapitels 8 des BayDSG, das die Verarbeitungen im Auftrag nach der Richtlinie (EU) 2016/680 regelt, anzuwenden.

Hieraus entstehende besondere Anforderungen werden dem IT-DLZ gegebenenfalls durch entsprechende Vereinbarungen mit den verantwortlichen Stellen auferlegt, die durch Weisungen im Einzelfall konkretisiert werden können.

Im Rahmen seines Aufgabenzuschnittes fungiert das IT-DLZ als Internetserviceprovider für öffentliche Stellen des Freistaats Bayern; insoweit anzuwenden sind die Vorschriften des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) sowie, später die dann vorrangig anzuwendende Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation - ePrivacy Verordnung).

3.4 Sonstige Rechtsnormen

Weitere Rechtsgrundlagen für Verarbeitungen können u.a. sein: das Bayerische E-Government-Gesetz (BayEGovG), die Bayerische Verordnung zur Schaffung barrierefreier Informationstechnik (Bayerische Barrierefreie Informationstechnik-Verordnung - BayBITV), die Regelungen der Allgemeinen Geschäftsordnung (A-GO)/Informations- und Kommunikationstechnik, sowie die Aussonderungsvorschriften nach dem Bayerischen Archivgesetz (BayArchivG) mit der Bekanntmachung über Aussonderung, Anbietung, Übernahme und Vernichtung von Unterlagen (Aussonderungsbekanntmachung - Aussond-Bek) des Freistaats Bayern.

4 Standorte

Das IT-DLZ erbringt seine Leistungen an folgenden Standorten:

4.1 IT-DLZ Standorte

4.1.1. Hauptstandort:

St.-Martin-Straße 47, 81541 München

4.1.2. Weitere Standorte:

- München, Marsplatz 10 (in den Räumen des Bayerischen Landeskriminalamts)
- Außenstelle Augsburg (in den Räumen der Regierung von Schwaben)
- Außenstelle Landshut (in den Räumen des LDBV, Regionalabteilung Ost)
- Außenstelle Marktredwitz (in angemieteten Räumen im Ost-West-Kompetenzzentrum)
- Außenstelle Nürnberg (in den Räumen des Landesamtes für Steuern, RZ Nord)
- Außenstelle Regensburg (in den Räumen des Landesamtes für Finanzen)

4.2 Kundenstandorte

- Hauptstandorte und Außenstellen staatlicher öffentlicher Stellen flächendeckend in ganz Bayern, in Deutschland (Berlin) und in der Europäischen Union (Belgien – Brüssel, Tschechien – Prag).

5 Datenschutz- und Informationssicherheitsmanagement

Das IT-DLZ hat eine Vielzahl von Anforderungen im Bereich der Informationssicherheit und des Datenschutzes zu erfüllen. Neben den unmittelbar gültigen vorwiegend gesetzlichen Vorgaben bestehen die vertraglich auferlegten Anforderungen der Stellen, die Dienstleistungen des IT-DLZ in Anspruch nehmen.

Mit Blick auf die DSGVO gewinnt die korrekte und vor allem belegbare Umsetzung dieser Anforderungen noch an Bedeutung. Um dieser Herausforderung angemessen gerecht zu werden, werden ein Informationssicherheits- bzw. ein Datenschutzmanagementsystem betrieben.

Ziel hierbei ist, die relevanten Prozesse zu definieren, sie den bestehenden Anforderungen entsprechend gesteuert, kontrolliert und nachweislich umzusetzen sowie gegebenenfalls erforderliche Korrekturen vorzunehmen. Im Idealfall soll auch eine laufende Optimierung erfolgen.

Zur Unterstützung der Zielerreichung wurden eine entsprechende Organisation aufgebaut und die notwendigen Ressourcen bereitgestellt. Insbesondere wurden eine Beauftragte für den Datenschutz und eine Beauftragte für Informationssicherheit bestellt und der Amtsleitung unmittelbar unterstellt.

Diese Beauftragten haben folgende Aufgaben:

Die in Vollzeit bestellte Beauftragte für den Datenschutz dient internen und externen Personen als zentrale Ansprechpartnerin in Fragen des Datenschutzes. Sie wirkt auf die Beachtung des Datenschutzes umfassend hin; mit Anwendbarkeit der DSGVO überwacht sie die Einhaltung der datenschutzrechtlichen Vorschriften.

Die ebenfalls in Vollzeit bestellte Beauftragte für Informationssicherheit steuert und koordiniert den Informationssicherheitsprozess. Das IT-DLZ strebt eine Zertifizierung nach ISO 27001 auf Basis BSI IT-Grundschutz an. Aktuell ist vom Bundesamt für Sicherheit in der Informationstechnik ein entsprechendes Zertifikat für den Informationsverbund „Zentraler Internetübergang und DOI Übergang, Betrieb der zentralen Exchange Infrastruktur für die staatliche Verwaltung, Technischer Datenbank- und Anwendungsbetrieb für die EU-Zahlstelle“ erteilt.

Beide Beauftragte werden frühzeitig und laufend in relevante Projekte einbezogen und stehen der Amtsleitung und anderen Verantwortlichen jederzeit beratend zur Seite.

Als Beauftragte für den Datenschutz ist bestellt:

- Frau Christine Schmid, it-dlz.datenschutz@ldbv.bayern.de

Als Beauftragte für Informationssicherheit ist bestellt:

- Frau Sonja Fahrbach, it-dlz.it-sicherheit@ldbv.bayern.de

Alle Mitarbeiter werden aktiv in den Datenschutz- und Informationssicherheitsprozess eingebunden. Externe Personen werden zur Beachtung der relevanten Regelungen vertraglich verpflichtet.

Zur Erreichung der oben genannten Ziele werden folgende allgemeine Maßnahmen angestrengt:

a. Für alle Prozesse werden klare Verantwortlichkeiten zugewiesen. Die Verantwortung erstreckt sich auf die verarbeiteten Informationen sowie eingesetzte IT-Systeme und IT-Infrastruktur. Für alle Verantwortlichen ist ein geeigneter Vertreter bestellt.
b. Alle eingesetzten Personen werden hinsichtlich ihrer persönlichen und fachlichen Eignung sorgfältig ausgewählt und angemessen überwacht. Soweit notwendig, werden benötigte Kenntnisse und Fähigkeiten vermittelt.
c. Alle Prozesse sind so auszugestalten, dass im jeweils erforderlichen Maß die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit erfüllt sind.
d. Alle zur Verarbeitung eingesetzten Personen müssen in angemessenem Umfang zur Geheimhaltung verpflichtet sein. Informationen werden nur zugänglich gemacht, soweit es zur Erfüllung einer konkreten, rechtmäßigen Aufgabe notwendig ist. Im Übrigen werden Informationen stets angemessen gegen unbefugte Kenntnisnahme oder Offenbarung geschützt.
e. Informationen werden jederzeit angemessen gegen unbefugte oder ungewollte Veränderung geschützt. Sie sind nach Möglichkeit aktuell zu halten.
f. Es werden angemessene Vorkehrungen gegen Störungen und Ausfälle getroffen. Um eingetretene Datenverluste berichtigen zu können, werden in angemessenem Umfang und ausreichender Häufigkeit Datensicherungen angefertigt.
g. Die Verarbeitung personenbezogener Daten erfolgt stets nur im zulässigen Rahmen, zu eindeutig im Voraus festgelegten Zwecken. Sie beschränkt sich auf den jeweils erforderlichen Umfang und erfolgt nur solange die Verarbeitung gestattet oder gesetzlich gefordert ist.
h. Insbesondere zur Wahrung der Rechte betroffener Personen sind Prozesse ausreichend transparent auszugestalten.
i. Externe Personen und Dienstleister werden zur Beachtung der Vorgaben verpflichtet. Sie werden angemessen kontrolliert.
j. Die Amtsleitung erhält regelmäßig Managementberichte und ist dadurch in der Lage, ihre Steuerungsaufgaben angemessen wahrzunehmen.

Weitere Details enthalten insbesondere die Leitlinie zur Informationssicherheit des LDBV und die dieser Leitlinie nachgeordneten taktischen ISMS-Dokumente.

6 Technische und organisatorische Maßnahmen

Nachstehend wird beschrieben, welche technischen und organisatorischen Maßnahmen zur Erfüllung der genannten Anforderungen, insbesondere zur Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit von personenbezogenen Daten ergriffen wurden. Die Vorgaben dafür werden im Rahmen des Informationssicherheitsmanagements in entsprechenden Sicherheitsrichtlinien (SiR) festgeschrieben. Sie sind für die Bediensteten des LDBV verbindlich.

Für die Einzelbeschreibung wurde die Gliederung an den für die Verarbeitung im Auftrag geltenden Artikel 32 des BayDSG zur Umsetzung der Justizrichtlinie angelehnt.

Die Ausführungen zu baulichen und organisatorischen Maßnahmen in Bezug auf die Gebäude- und Rechenzentrumssicherheit beziehen sich auf den IT-DLZ Rechenzentrumsstandort München, St.-Martin-Straße. Alle sonst genannten Maßnahmen erfolgen standortunabhängig.

6.1 Zugangskontrolle

Folgende Maßnahmen wurden ergriffen, um Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

6.1.1 Das Betriebsgelände ist umzäunt.

6.1.2 Es existieren keine freien Zugänge zum Gebäude.

6.1.3 Das IT-DLZ verfügt über ein eigenes Gebäude, und eigene abgesicherte Bereiche; die Betriebsräume befinden sich im Tiefgeschoss.

6.1.4 Der Rechenzentrumsbereich ist fensterlos.

6.1.5 Es besteht eine 7 x 24 Sicherheitsüberwachung des Außenareals sowie aller zentralen Durchgänge durch Videoüberwachungskameras. Eine datenschutzrechtliche Freigabe ist erteilt. Die Aufzeichnungen werden 30 Tage aufbewahrt.

6.1.6 Es besteht ein Einbruchmeldesystem/Alarmanlage.

6.1.7 Zum Schutz der Außenhaut sind Videoüberwachung, Bewegungsmelder und Monitore im Wachraum installiert.

6.1.8 Im Erdgeschoss befinden sich einbruchhemmende Außentüren und -fenster und beschusssicheres Glas; die Fenster können nicht geöffnet werden; Schächte (Klimaanlage, Umluftanlage, Aufzug usw.) sind gesichert.

6.1.9 Der Betrieb ist in mehrere Sicherheitsbereiche unterteilt. Die verschiedenen Zonen sind jeweils durch ein Zutrittskontrollsystem mit Kartenautorisierung abgesichert; die Zutritte werden protokolliert.

6.1.10 Gebäude und Sicherheitsbereiche können nur von Personen betreten werden, deren Zugangsberechtigung entsprechend freigegeben wurde.

6.1.11 Der Zutritt in das Gebäude findet über eine Vereinzelungsanlage (Drehkreuz) mit Kartenautorisierung statt.

6.1.12 Der Zutritt in den Closed Shop Bereich findet zusätzlich über eine Schleuse mit gesonderter Videoüberwachung statt.

6.1.13 Es bestehen Regelungen für Zugangsberechtigungen mit Festlegung der befugten Personen (bezogen auf Zonen und Zeiten).

6.1.14 Es bestehen Regelungen für Besucher und Fremdfirmen.

6.1.15 Besucher und Fremdfirmen können das Gebäude nur über den Haupteingang betreten. Sie müssen sich an der Pforte an- bzw. abmelden. Sie werden namentlich erfasst und innerhalb des Gebäudes von Mitarbeitern begleitet.

6.1.16 Wartungs-, Reparatur- und Reinigungspersonal wird eingewiesen und in sensiblen Bereichen beaufsichtigt.

6.1.17 Mitarbeiter / Besucher müssen den Empfang von Ausweisen, Schlüsseln usw. quittieren.

6.1.18 Es sind Maßnahmen zur Sicherung der Türen getroffen (wie z.B. Türöffner /-schließer, Sicherheitsschlösser, separate Schließgruppe mit Schlüssel und Schlüsselschein, Vereinzelungsanlage, Gegensprechanlage, Ausweisleser, Protokollierung der Zugänge, Fernsehmonitor, personelle Kontrolle)

6.1.19 Die Notausgänge sind gegen missbräuchliche Benutzung gesichert.

6.1.20 Es werden Anwesenheitsaufzeichnungen, Dienstpläne usw. des Bedienpersonals geführt.

6.1.21 Es sind Regelungen bei Verlust von Ausweisen, Schlüsseln etc. getroffen.

6.1.22 Ein elektronisches Zutrittskontrollsystem basierend auf berührungslosen, individualisierten Zutrittskarten mit Foto und PIN Tastencodes (in sensiblen Bereichen) ist installiert.

6.1.23 Bei Verlust einer Zutrittskarte erfolgt unverzüglich deren Sperrung.

6.1.24 Das gesamte Rechenzentrum wird über ein zentrales Gebäudemanagementsystem überwacht.

Einzelheiten enthalten auch die Sicherheitsrichtlinie Zutritt LDBV und das Zutrittskonzept IT-DLZ.

6.2 Organisationskontrolle

Folgende Maßnahmen wurden ergriffen, um die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

6.2.1 Alle Mitarbeiter werden bei der Einstellung zur Verschwiegenheit nach beamten- und tarifrechtlichen Vorschriften verpflichtet.

6.2.2 Es wird nur Fachpersonal eingesetzt, dass auf die jeweilige Aufgabe ausführlich geschult wurde bzw. die entsprechenden Fähigkeiten bereits erworben hat. Dem eingesetzten Personal wird die Möglichkeit gegeben, sich

laufend nach dem Stand der Technik fortzubilden und ggf. durch Hersteller zertifizieren zu lassen.

6.2.3 Alle Mitarbeiter des IT-DLZ besitzen eine Smartcard mit Zertifikaten der Bayerischen Verwaltungs-PKI; sie sind angehalten vertrauliche Informationen beim E-Mailversand signiert und verschlüsselt zu versenden.

6.2.4 Personal, das an einer sicherheitsempfindlichen Stelle des IT-DLZ eingesetzt ist, wird einer einfachen Sicherheitsüberprüfung (Ü 1) im Wege des vorbeugenden personellen Sabotageschutzes, Art. 1 Abs. 2 Nr. 2 BaySÜG, Art. 3 Abs. 1 Nr. 4 BaySÜG, Art. 10 Abs. 1 Nr. 2 BaySÜG unterzogen. Sicherheitsempfindliche Stellen / Tätigkeiten sind über alle Abteilungen des IT-DLZ hinweg festgelegt. Der überprüfte Personenkreis erstreckt sich sowohl auf IT-DLZ eigenes Personal (Vorgesetzte / Beschäftigte) als auch auf Mitarbeiter externer Dienstleister (z.B. Reinigungspersonal / Wartungspersonal / Bewachungsdienste / Betriebsunterstützung). Die Sicherheitsüberprüfung wird vor Aufnahme der Tätigkeit durch den Geheimschutzbeauftragten des LDBV veranlasst.

6.2.5 Alle Mitarbeiter des IT-DLZ werden im Datenschutz und in der Informationssicherheit sensibilisiert und ausreichend geschult. Die Amtsleitung unterstützt und fördert diese Maßnahmen aktiv. Einzelheiten sind insbesondere im Konzept Sensibilisierung und Schulung zur Informationssicherheit im IT-DLZ geregelt.

6.2.6 Zuständigkeiten und Verantwortlichkeiten (Aufgaben, Aufgabenzuweisung, Stellvertretung) sind klar geregelt im Organisations- bzw. Geschäftsverteilungsplan sowie in Dienstanweisungen des LDBV. Diese werden laufend fortgeschrieben und zusammen mit den entsprechenden Änderungsmitteilungen den Beschäftigten via LDBV Intranet bekannt gegeben.

6.2.7 Scheiden Mitarbeiter aus dem Dienst aus, erfolgt der Hinweis auf weiterhin bestehende Pflichten zur Vertraulichkeit.

6.3 Datenträgerkontrolle

Folgende Maßnahmen wurden ergriffen, um zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

6.3.1 Es bestehen Regelungen zur Verwendung und Aufbewahrung von Datenträgern, insbesondere zu ihrer eindeutigen Kennzeichnung und welche Datenträger sich in welchen Zonen befinden dürfen.

6.3.2 Die zur Datenträgerentnahme befugten Personen sind festgelegt.

6.3.3 Die Vernichtung von Datenträgern erfolgt in Abhängigkeit vom Medium. Nicht mehr benötigte Daten in Papierform werden in jeweils auf den Stockwerken befindlichen verschlossenen Datenschutztonnen gesammelt. Anschließend wird das Schriftgut durch Beauftragung Dritter gemäß DIN 66399 entsorgt. Daten auf Datenträger werden physikalisch zerstört (mittels Degausser oder Shredder). Anschließend werden sie durch Beauftragung Dritter gemäß DIN 66399 entsorgt. Die Vorgänge werden dokumentiert.

6.3.4 Soweit zur Vernichtung von Daten auf Papier und Daten auf Datenträger eine Beauftragung von Dritten erfolgt, geschieht dies im Rahmen der ge-

setzlichen Vorgaben. Es werden die datenschutzrechtlich erforderlichen Verträge geschlossen, die mindestens den Anforderungen der entsprechenden Verträge zwischen dem IT-DLZ und den Verantwortlichen (Auftraggebern) entsprechen.

Einzelheiten siehe Sicherheitsrichtlinie Beschaffung und Aussonderung.

6.4 Speicherkontrolle

Folgende Maßnahmen wurden ergriffen, um die unbefugte Eingabe sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern.

6.4.1 Die Benutzer- und Rechteverwaltung erfolgt gesteuert und restriktiv.

6.4.2 Vergabe und Verwaltung von Zugangs- und Zugriffsberechtigungen erfolgen geregelt.

6.4.3 Es bestehen Regelungen beim Ausscheiden und Wechseln von Berechtigten.

6.4.4 Es werden nur individuelle Zugriffsrechte vergeben. Auf Interessenskollisionen oder andere Unverträglichkeiten wird geachtet; es erfolgt insb. die Trennung von System- und Datenbankadministratoren.

6.4.5 Benutzer müssen sich durch Benutzerkennung und Passwort ausweisen; sie sind zur Geheimhaltung Ihrer Zugangsinformationen verpflichtet.

6.4.6 An- und Abmeldungen werden in der Regel protokolliert.

6.4.7 Die Änderung von Passwörtern erfolgt in der Regel kontrolliert über Passwortrichtlinien (wie Zeitabstände, Passwortlänge, Verwendung gleicher Passworte u.a.)

6.4.8 Zugriffe und im Aufgabenbereich genutzte Funktionen (z.B. Änderung, und/oder Löschung von Benutzern und Berechtigungen, Zeitpunkt der Verbindung und Benutzer) werden protokolliert.

6.4.9 Details regeln insbesondere die Sicherheitsrichtlinie Benutzer und Administratoren im LDBV, die Sicherheitsrichtlinie Benutzer- und Berechtigungsverwaltung sowie die Passwortrichtlinie LDBV und die Sicherheitsrichtlinie Protokollierung.

6.5 Benutzerkontrolle

Folgende Maßnahmen wurden ergriffen, um zu verhindern, dass automatisierte Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.

6.5.1 Teilweise sind Zugriffe auf dedizierte Netzbereiche / IP-Adressen beschränkt.

6.5.2 Es bestehen funktionale, zeitliche und/oder räumliche Beschränkungen der Terminalnutzung.

6.5.3 Zugriffssicherungen auf das Netz erfolgen mittels Hard- und Softwaremaßnahmen.

6.5.4 Fernadministration und Fernwartung sind spezifisch geregelt.

6.5.5 Das für die Übertragung genutzte Bayerische Behördennetz wird durch den Netzbetreiber Vodafone gesichert. Ab BayKom2017 werden die zur Sicherung des Behördennetzes notwendigen Schlüssel durch das IT-DLZ verwaltet.

6.5.6 Die Systeme sind durch den Einsatz von Firewalls und Netzwerksegmentierung geschützt.

6.5.7 Durch Einsatz eines Schwachstellenscanners wird die IT Infrastruktur des IT-DLZ permanent auf Schwachstellen in der Systemsicherheit überwacht.

6.5.8 Die Überwachung des Bayerischen Behördennetzes erfolgt durch das Landesamt für Sicherheit in der Informationstechnik; es prüft regelmäßig die vom Internet aus erreichbaren Systeme im Hinblick auf ihre Sicherheit.

6.6 Transportkontrolle

Folgende Maßnahmen wurden ergriffen, um zu verhindern, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

6.6.1 Das für die Übertragung genutzte Bayerische Behördennetz wird durch den Netzbetreiber Vodafone gesichert. Ab BayKom2017 werden die zur Sicherung des Behördennetzes notwendigen Schlüssel durch das IT-DLZ verwaltet. Die Daten sind bei der Übertragung zwischen öffentlichen Stellen innerhalb des Bayerischen Behördennetzes durch für VS-NfD zugelassene Komponenten verschlüsselt.

6.6.2 Zentrale IT-Infrastrukturen zur Datenübertragung per Webbrowser werden in der Regel als SSL gesicherte Verbindungen (https) mit dem Verschlüsselungsprotokoll TLS 1.2 bereitgestellt. Zur Serverauthentifizierung dienen Zertifikate der Bayerischen SSL PKI auf Basis von RSA mit einer Schlüssellänge von 2048 BIT. Mit der Einstellung „Perfect Forward Secrecy“ wird zudem für jede verschlüsselte Verbindung (Session) ein eigener (exklusiver) Verschlüsselungsschlüssel generiert.

6.6.3 Der Versand von E-Mails ist durch die Einstellung „STARTTLS“ an der Zentralen Exchange Server Infrastruktur generell transportverschlüsselt. Durch die Einstellung „Perfect Forward Secrecy“ wird zudem bei jedem E-Mailversand ein zusätzlicher exklusiver Verschlüsselungsschlüssel pro E-Mail/Transport generiert.

6.6.4 Zur gesicherten Datenübertragung zwischen zentralen IT-Infrastrukturen und oder Clients erhalten die Systeme zumeist zur Authentifizierung Gerätezertifikate der Bayerischen Infrastruktur PKI auf Basis von RSA mit einer Schlüssellänge von 2048 Bit.

Zu Maßnahmen beim Transport von Datenträgern siehe Einzelheiten in den Maßnahmen 6.3 zur Datenträgerkontrolle.

6.7 Zugriffskontrolle

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

6.7.1 Informationen, Anwendungen und Systeme werden den bestehenden Risiken entsprechend eindeutig klassifiziert und und entsprechenden Schutzzonen zugewiesen.

6.7.2 Die Benutzer- und Rechteverwaltung erfolgt gesteuert und restriktiv. Es bestehen Regelung beim Ausscheiden und Wechseln von Berechtigten.

6.7.3 Bei Änderungen der Beschäftigungsverhältnisse werden Berechtigungen in einem regelmäßigen Reviewzyklus entsprechend angepasst.

6.8 Übertragungskontrolle

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.

6.8.1 Abruf- und Übermittlungsprogramme werden dokumentiert (z.B. sFTP = Secure File Transfer Protocol, http/s, Firewall, Remote Access Verfahren)

6.8.2 Administrative Tätigkeiten werden in der Regel nicht direkt über den Client der Administratoren durchgeführt, sondern über ein gesondertes Managementnetz.

6.8.3 Es erfolgt in der Regel eine Protokollierung der schreibenden Dateizugriffe und eine Auswertung der Protokolle.

6.9 Eingabekontrolle

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind.

6.9.1 Die Tätigkeiten der Administratoren werden in der Regel protokolliert und überwacht.

6.9.2 Die Eingabekontrolle bei Datenbanksystemen erfolgt über Changelogs und Transaktionslogs.

6.9.3 Änderungen innerhalb des Dateisystems werden in der Regel über die aktivierte Auditierung des Basisbetriebssystems aufgezeichnet.

Einzelheiten siehe auch in der Sicherheitsrichtlinie Protokollierung.

6.10 Verfügbarkeitskontrolle

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

6.10.1 Die Infrastruktur befindet sich im gleichen Gebäude und ist gesichert (Klima, Stromeinspeisung, Unterbrechungsfreie Stromversorgung).

6.10.2 Es werden angemessen dimensionierte, redundant ausgelegte IT-Systeme, Netzwerkkomponenten und Stromversorgung sowie Klimatisierung eingesetzt.

6.10.3 Es besteht ein Schutz gegen Umweltgefahren; insb. erfolgt eine automatische Branddetektion und Brandlöschung.

6.10.4 Die Netzwerkanbindungen sind redundant ausgelegt.

6.10.5 Die internen Löschabschnitte sind redundant versorgt und räumlich getrennt (Power Distribution Units an gegenüberliegenden Gebäudeseiten). Die Verfügbarkeit der Stromversorgung liegt bei 99.99%.

6.10.6 Das Rechenzentrum ist redundant an das städtische Versorgungsnetz angeschlossen. Bei Störungen in der Versorgung mit Elektrizität stehen unabhängige Stromversorgungssysteme bereit. Bei Stromausfall übernehmen Dieselgeneratoren kurzfristig die Stromversorgung. Der Treibstoffvorrat erlaubt einen Volllastbetrieb für mindestens 28 Stunden. Bei Absinken des Vorrats unter 75% wird eine Treibstofflieferung ausgelöst. Hierfür bestehen Verträge mit ortsansässigen Lieferanten, die jederzeitige Versorgung sicherstellen.

6.10.7 Die ausreichend dimensionierte Klimatisierung des Rechenzentrums ist redundant ausgelegt.

6.10.8 Es existieren automatische Meldeeinrichtungen für Wassereinbruch, Temperaturanstieg, Brandfrüherkennung und sonstige betriebsrelevanten Störungen. Auch Bereiche mit Unterbodenleitungen werden automatisch überwacht. Die Meldeeinrichtungen werden regelmäßig gewartet und auf Funktion getestet. Die Feuerlösch- und Rauchabzugsanlage wird automatisch beim Eintreten von kritischen Situationen durch mehrfach vorhandene Brandmeldeanlagen ausgelöst. Die Brandmeldeanlage ist bei der Feuerwehr aufgeschaltet. Die Feuerlöschanlage wird automatisch ausgelöst.

6.10.9 Das Gebäude ist in mehrere selbständige Brandabschnitte unterteilt. Innerhalb des eigentlichen Rechenzentrumsbereichs erfolgt keine Lagerung, insbesondere von entflammbaren Materialien.

6.10.10 Brandschutzwartungen erfolgen nach geltender Brandschutzverordnung. Betriebsrelevante Systeme wie z.B. Gebäudetechnik, USV / UPS inkl. Batterie und Generatortechnik, Klimatechnik werden nach Richtlinien der Hersteller gewartet.

6.10.11 Es werden regelmäßig Notfallübungen durchgeführt; Einzelheiten auch in der Leitlinie zum Notfallmanagement LDBV, im Konzept Notfallübungen im IT-DLZ und der Richtlinie Sicherheitsvorfälle im IT-DLZ.

6.10.12 Zusätzlich erfolgt ein jährlicher „Black Building“-Test zur Simulation eines totalen Stromausfalls.

6.10.13 Die Rechenzentrums-Infrastruktur wird nach den entsprechenden Wartungsrichtlinien regelmäßig überprüft.

6.10.14 IT-Infrastrukturen und IT-Systeme werden dokumentiert.

6.10.15 Die Wartung der IT-Systeme und -Infrastruktur erfolgt grundsätzlich nur durch eigene Mitarbeiter. Im Bedarfsfall werden externe Spezialisten hinzugezogen. Mit diesen werden die zur Aufrechterhaltung der Sicherheit und die gesetzlich geforderten Vereinbarungen geschlossen. Grundsätzlich werden die Tätigkeiten externer Personen überwacht.

6.10.16 Hinsichtlich der RZ-Infrastruktur werden nach den Wartungsrichtlinien regelmäßige Funktionstest einzelner Systeme durchgeführt. Bei den Diesel-Generatoren erfolgt z.B. ein monatlicher Testlauf gegen eine Lastbank, der die Funktion der Notstromaggregate bei Volllast prüft.

6.10.17 Ein definierter Changeprozess sorgt dafür, dass Netzwerkkomponenten, IT Infrastrukturen, Server und Software regelmäßig mit aktuellen Sicherheits- und sonstigen notwendigen Updates bestückt werden. Der Einsatz von Updates erfolgt i.d.R. nach Tests auf separaten Testsystemen.

6.10.18 Die Installation und Konfiguration von Systemen sowie die Verarbeitung von und der Umgang mit Informationen ist geregelt.

6.10.19 Geplante Wartungen und andere notwendige Maßnahmen – z.B. Veränderungen an der RZ Infrastruktur – werden hinsichtlich der Beeinträchtigung verschiedenen Klassifizierungsstufen zugeordnet.

6.10.20 Bevor mit Änderungen an Systemen begonnen wird, ist die alte Konfiguration zu sichern, um sie im Bedarfsfall wiederherstellen zu können.

6.10.21 Konfigurationsänderungen haben soweit möglich außerhalb der regulären Geschäftszeiten zu erfolgen. Wenn die Möglichkeit von Beeinträchtigungen für Nutzer besteht, sind diese vorab zu informieren.

6.10.22 Alle vorgenommenen Änderungen sind zu dokumentieren.

6.10.23 Einzelheiten finden sich im Dokument zum Prozess Change Management und dem Konzept Change Management.

6.10.24 Zum Auffinden von Schwachstellen in IT-Komponenten wird zusätzlich ein Schwachstellenscanner eingesetzt, der permanent alle IT-Systeme nach Auffälligkeiten untersucht.

6.10.25 Der Virenschutz im IT-DLZ erfolgt abhängig vom Einsatzbereich auf mehrfache Weise:

- Internetgateway: McAfee
- Mail Security: Sophos
- Server- / Storagesysteme: McAfee, Sophos

6.10.26 Die Virenprogramme werden permanent und automatisiert mit den aktuellen Virenpattern der Hersteller versorgt.

6.11 Zuverlässigkeit

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.

6.11.1 Überwachungssysteme melden permanent den Zustand der IT-Infrastruktur. Bei ungewöhnlichem Verhalten wird die Problemanalyse und ggf. -lösung eingeleitet.

6.11.2 Die eingesetzten IT-Systeme und Netzwerkdienste werden laufend überwacht. Insbesondere werden in der Regel

- Prozessorauslastung
- Arbeitsspeicherauslastung
- Leistungsauslastung
- Festplattenauslastung
- Storageauslastung

protokolliert und auf Auffälligkeiten hin überwacht.

6.11.3 Es finden automatisierte, permanente elektronische Tests der Core IT-Systeme statt, die die Funktion und Leistungsfähigkeit (z.B. den Durchsatz) prüfen.

6.11.4 Eine Beauftragte für das Notfallmanagement wurde von der Amtsleitung LDBV bestellt. Sie ist direkt dem Direktor des IT-DLZ Bayern unterstellt.

6.11.5 Werden Störungen festgestellt, erfolgt die Benachrichtigung darüber IT-DLZ intern durch den ServiceDesk per E-Mailbenachrichtigung, SMS und Veröffentlichung im Intranet. Verantwortliche werden durch Veröffentlichung der Störung auf der IT-DLZ Extranet Seite im Bayerischen Behördennetz über den Status der Entstörung auf dem Laufenden gehalten. Zudem werden entsprechende Informationen an fachliche und technische Ansprechpartner der Verantwortlichen telefonisch, per E-Mailbenachrichtigung oder SMS kommuniziert.

6.11.6 Treten Störungen nach Ende der bedienten Betriebszeit auf können Verantwortliche sich an die im Service Level Agreement kommunizierte Service Hotline Nr. bzw. E-Mailadresse wenden. Der jeweils zur Rufbereitschaft eingeteilte Notfallmanager koordiniert die zur Fehlerverifizierung und Behebung erforderlichen Schritte. Je nach Störungsbild werden die Beauftragte für das Notfallmanagement und weitere Gremien eingebunden.

6.11.7 Das bestehende Notfallkonzept beinhaltet regelmäßige Tests der Infrastruktur (Notfallübungen) die dokumentiert durchgeführt werden.

6.11.8 Einzelheiten werden auch in der Leitlinie zum Notfallmanagement LDBV, im Konzept Notfallübungen im IT-DLZ, in der Arbeitsanweisung Notfallübungen im IT-DLZ und der Richtlinie Sicherheitsvorfälle im IT-DLZ sowie in der Sicherheitsrichtlinie Protokollierung und in den Detailkonzepten zur Überwachung von IT-Systemen und Netzwerkdiensten geregelt.

6.11.9 Im Regelfall wird der Betrieb der IT Infrastruktur für 7x24 gewährleistet. Die Zentrale Anbindung des Bayerischen Behördennetzes an das Internet er-

folgt über eine redundante Leitung des Netzproviders Vodafone. Die garantierte Verfügbarkeit der Anbindung liegt bei 99,95%.

6.11.10 Backbonestörungen im Bayerischen Behördennetz sind innerhalb von maximal 4 Stunden zu beheben.

6.11.11 Soweit im Rahmen des Risikomanagements festgestellt wird, dass eine Redundanz von Systemen oder Diensten erforderlich ist, werden geeignete Maßnahmen zur Schaffung von Redundanz ergriffen.

6.12 Datenintegrität

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

6.12.1 Alle Systeme, die für den Produktiveinsatz eingesetzt werden sollen und durch Fehlfunktion sicherheitstechnische Auswirkungen auf den Rechenzentrumsbetrieb haben können, werden vorab getestet.

6.12.2 Im Rahmen eines geregelten Changemanagements erhalten alle IT-Systeme die erforderlichen Soft- und Hardwareupdates. Bugfixreports der Lieferanten garantieren darüber hinaus eine Prävention von Hard- und Softwarefehlern.

6.12.3 Die Stabilität einer Hard-/Software hat Vorrang vor Featurevielfalt, wenn die Entscheidung für ein Update getroffen werden soll.

6.12.4 Am Markt absolut neue Hardware wird i.d.R. aufgrund der fast immer vorhandenen und noch nicht bekannten Fehler nicht sofort eingesetzt.

6.12.5 Abgekündigte Hardware wird andererseits i.d.R. immer schon vor deren „End of“ Zyklus (z.B. Life, Support) ausgemustert. Es wird grundsätzlich versucht, die neuesten Features unter Beibehaltung der höchst möglichen Stabilität einzusetzen. Hard- und Softwareupdateverträge sind dazu vorhanden.

Einzelheiten siehe auch Maßnahmen 6.10 zur Verfügbarkeitskontrolle und in der Dokumentation zum Prozess Change Management und dem Konzept Change Management.

6.13 Wiederherstellung

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

6.13.1 Es existiert ein globales Datensicherungskonzept und weitere spezielle Datensicherungskonzepte.

6.13.2 Die Sicherung erfolgt, soweit nicht anders vereinbart, täglich inkrementell.

6.13.3 Es werden, soweit nicht anders vereinbart, über die jeweils letzten 14 Tage alle Veränderungen, also Versionen 1 bis 14 vorgehalten. Daten, die länger als 180 Tage gelöscht sind, sind nicht mehr wiederherstellbar.

6.13.4 In den speziellen Datensicherungskonzepten werden besondere Anforderungen und Merkmale festgelegt und beschrieben, die durch das globale Datensicherungskonzept nicht abgedeckt werden.

6.13.5 Die Backups werden in einem mindestens 5 km entfernten Rechenzentrum (im Bayerischen Landeskriminalamt, Marsplatz, München) vorgehalten.

Einzelheiten finden sich in oben genannten Konzepten zur Datensicherung; siehe auch Maßnahmen 6.10 zur Verfügbarkeit, Maßnahmen 6.11 zur Zuverlässigkeit und Dokumentationen zum Notfallmanagement.

6.14 Auftragskontrolle

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen (Auftraggeber) verarbeitet werden können.

6.14.1 Die gesetzlichen und vertraglichen Anforderungen an die Verarbeitung von Informationen werden festgestellt.

6.14.2 Die Verarbeitungen von Daten im Auftrag erfolgen im Rahmen der zugrundeliegenden Vereinbarungen ausschließlich nach Weisung der Verantwortlichen (z.B. Festlegungen im ADV Vertrag, Servicelevel Agreement, zusätzliche Anforderungen mindestens in Textform, über Ticketsystem). Sie entsprechen den formellen Anforderungen des Art. 28 BayDSG, § 80 SGB X.

6.14.3 In einem regelmäßigen Sicherheitsbericht gibt das IT-DLZ den Verantwortlichen und dem Landesbeauftragten für den Datenschutz Auskunft über den Stand der technischen und organisatorischen Maßnahmen, aufgetretene Sicherheitsprobleme und erforderliche Maßnahmen zur Verbesserung der Datensicherheit; desweitern eine aktuelle Liste der Unterauftragnehmer.

6.14.4 Verantwortlichen steht ein Ticketsystem zur Störungsmeldung zur Verfügung. Hierbei kann der Stand der Entstörung grundsätzlich mitverfolgt werden.

6.14.5 Über das Ticketsystem können zudem Bearbeitungsstände von Servicebeauftragungen, sonstigen Anfragen oder ggf. auch Weisungen durch den Verantwortlichen mitverfolgt werden.

6.14.6 Zur Dokumentation der Beauftragungen steht den Verantwortlichen ein Online Kundenportal zur Verfügung. Dort können alle aktuell beauftragten Services und vertraglichen Regelungen detailliert eingesehen werden.

6.14.7 Es erfolgt eine regelmäßige Anpassung von allgemeinen Arbeits-, Datenschutz- und Datensicherheitsregelungen und -Maßnahmen an geänderte Verhältnisse.

6.14.8 Soweit vereinbarungsgemäß eine Beauftragung von Subunternehmern erfolgen darf, erfolgt dies transparent gegenüber den Verantwortlichen. Neben den bundes- bzw. landesweit einheitlichen EVB-IT Verträgen werden darüber hinaus die datenschutzrechtlich erforderlichen Verträge geschlossen, die mindestens den Anforderungen des Vertrages zwischen dem IT-DLZ und den Verantwortlichen entsprechen.

6.14.9 Generell werden Mitarbeiter externer Dienstleister (Berater, Wartung/Support, Betriebsunterstützung) schriftlich unter Aushändigung der entsprechenden Gesetzesauszüge auf die Erfüllung ihrer Obliegenheit nach dem Verpflichtungsgesetz formell verpflichtet; ebenso auf die Wahrung des Datengeheimnisses nach dem Bayerischen Datenschutzgesetz sowie des Sozialgeheimnisses; sofern sie zum betroffenen Personenkreis gehören, werden sie auch einer Sicherheitsüberprüfung (Ü1) unterzogen.

6.14.10 Falls Mitarbeiter externer Dienstleister an sicherheitsempfindlichen Stellen/Tätigkeiten eingesetzt werden, wird in den Ausschreibungsunterlagen bekanntgegeben, dass die Mitarbeiter des Bieters als Zuschlagskriterium ihre grundsätzliche Bereitschaft zu einer einfachen Sicherheitsüberprüfung (Ü1) nach dem Bayerischen Sicherheitsüberprüfungsgesetz erklären müssen.

6.14.11 Sind Mitarbeiter von externen Dienstleistern eingesetzt, erhalten sie, soweit für Ihre Tätigkeit erforderlich, IT-DLZ eigene Clientgeräte und personalisierte Zugangskennungen mit Berechtigungen nur für ihren Tätigkeitsbereich. Ihre administrativen Tätigkeiten werden, wie beim eigenen Personal, im Rahmen der technischen und organisatorischen Maßnahmen mitprotokolliert.

6.15 Trennbarkeit

Folgende Maßnahmen wurden ergriffen, um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

6.15.1 Die den Verantwortlichen zur Verfügung stehenden IT-Infrastrukturen werden zumindest logisch voneinander getrennt. Soweit vereinbart, erfolgt eine physikalische Trennung durch Einsatz von dedizierten Systemen.

6.15.2 Die Erhebung bzw. Verarbeitung von Daten für verschiedene Zwecke erfolgt auftragsbezogen auf physikalisch oder logisch voneinander getrennten IT-Systemen.

gez. Martin Stegmeier

Direktor IT-Dienstleistungszentrum des Freistaats Bayern