STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Kooperationsvorhaben GKDZ der SiKoop und BE

Gemeinsames Kompetenz- und Dienstleistungszentrums auf dem Gebiet der polizeilichen TKÜ (AöR)

Informationsveranstaltung für die Datenschutzbeauftragten der beteiligten Länder

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Agenda

- Ausgangslage und Zielarchitektur
- Untersuchungsfelder und externe Beratung
- Ergebnisse
- GKDZ - rechtsfähige Anstalt öffentlichen Rechts
- GKDZ - Aufgaben
- Aktueller Stand und Ausblick
- Datenschutz und IT-Sicherheit

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Ausgangslage und Zielarchitektur

- Grundsatzerklärung der Innen-StS (BB, SN, ST und TH) am 4. Mai 2010 in Leipzig
- Einrichten und Beauftragen der (ministeriellen) AG TKÜ mit der Beteiligung Berlins am 26. Sept. 2010 in Dresden, FF SN
- Bestimmen der Zielarchitektur:
  - zwei gegenseitig georedundant ausgelegte Standorte eines gemeinsamen Kompetenzzentrums gewährleisten ein hohes Maß an Ausfallsicherheit
  - Zwingende Bündelung aller technisch sicherstellenden Prozesse (Betrieb, Wartung, Beschaffung und Weiterentwicklung)
  - größtmögliches Zentralisieren von standardisierten bzw. standardisierbaren Prozessen im administrativen Bereich
  - Verbleib von nicht zentralisierbaren Kernkompetenzen, Steuerung und Kontrolle der Aufgabenerledigung sowie operative TKÜ bei reduzierten TKÜ-Stellen

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Untersuchungsfelder und externe Beratung I

Teil 1 - Grundsatz

- Rechtliche Zulässigkeit, Rechtsrahmen, Rechtsform, haushaltsrechtliche Betrachtungen
- Wirtschaftlichkeitsbetrachtung gem. BMI-Standard „WiBe Version 4.1 – 2007"
- Standorte

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Untersuchungsfelder und externe Beratung II

Teil 2 - Konzeptionierungsgrundlagen

- Stellen- und Personalbetrachtungen
- Finanzierungsmodell/Haushaltsvorsorge
- Technische und organisatorische Grobplanung
- Prozessmodellierung/Aufgabenabgrenzung
- Kooperationsform und Geschäftsmodell
- Vertragliche Voraussetzungen (Staatsvertragsentwurf, StV-E) und Entscheidungsvorlage des Gutachters

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Untersuchungsfelder und externe Beratung III

- ESG Elektroniksystem- und Logistik-GmbH
  - im Vorfeld gesonderte Untersuchungen zur TKÜ-Landschaft und aktuellen Anforderungen im Auftrag des BMI (SFZ TK)
  - weitere Beratung des BMI
- Univ.-Prof. Dr. Dirk Heckmann
  - Mitglied des Bayerischen Verfassungsgerichtshofs
  - Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht der Universität Passau, Mitglied des Direktoriums des Instituts für IT-Sicherheit und Sicherheitsrecht sowie Leiter der Forschungsstelle für IT-Recht und Netzpolitik an der Universität Passau

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Ergebnisse - juristische Prüfungen

Die Einrichtung eines länderübergreifenden GKDZ auf dem Gebiet der polizeilichen TKÜ ist möglich:

- in öffentlich-rechtlicher Rechtsform
- auf Grundlage eines Staatsvertrags
- mit begrenztem Aufgaben- und Tätigkeitsbereich
- unter Berücksichtigung der Grundsätze der Auftragsdatenverarbeitung
- unter Gewährleistung eines adäquaten IT-Sicherheitsniveaus

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Ergebnisse - technische Anforderungen ...

... aus dem Rechtsgutachten abgeleitet:

- **Hochverfügbarkeit** (Tier3 +);
- komplette Dopplung des Systems an zwei geo-redundanten Standorten im synchronen Clusterbetrieb;
- Notwendigkeit einer Unterbringung in einem geeigneten Umfeld betreffend Strom, Klima, Anbindung und sicherheitstechnischer Abriegelung etc.;
- **Redundanz** über direkte Kommunikationsverbindungen;
- Hohe redundante Speicherfähigkeit im Petabyte-Bereich (= mehrere Billiarden Bytes);
- Schnelle Zugänge für IP-Ausleitungen;
- **Systeme** für Evaluierung und Schulung erforderlich;
- Zugriff der polizeilichen Sachbearbeiter über Terminal-Systeme vom eigenen Arbeitsplatz aus

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Ergebnisse - wirtschaftlich

Sehr deutlicher wirtschaftlicher Vorteil des GKDZ gegenüber separaten Länderlösungen mit vergleichbaren Leistungen!

- erhebliche Einsparungen bei Baukosten
- erhebliche Einsparungen bei Investitionskosten
- Betriebskosten fallen deutlich
- höchste Anforderungen der Informationssicherheit müssten bei den Altsystemen unter vergleichsweise hohem Aufwand nachgerüstet werden

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

GKDZ - Rechtsfähige Anstalt des öffentlichen Rechts

- Träger und Nutzer der Anstalt sind die Teilnehmerländer
- wirtschaftliche Eigenverantwortung des GKDZ - kaufmännisch, kostendeckend, keine Gewinne
- Dienstherrnfähigkeit
- Finanzierung des GKDZ nach bestätigtem Wirtschaftsplan:
  - anteilig nach dem modifizierten Königsteiner Schlüssel
  - näheren Einzelheiten werden in einem Verwaltungsabkommen geregelt
  - nach der Evaluierung ist die Einführung eines Abrechnungsmodells gemäß tatsächlicher Länderinanspruchnahme möglich
- Rechtsaufsicht: Teilnehmerländer, Aufsichtsbehörde: SMI im Benehmen mit Innenressorts der Teilnehmerländer

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

GKDZ - Rechtsfähige Anstalt des öffentlichen Rechts II

- Anwendung von sächsischem Landesrecht für Errichtung und Betrieb soweit keine staatsvertraglichen Regelungen einschlägig sind
- Verwaltungsrat des GKDZ:
  - je ein Ländervertreter
  - Einstimmigkeit bei Grundsatzfragen
- Vorstand des GKDZ:
  - Leitung und gesetzliche Vertretung
  - Sitzungsteilnehmer des Verwaltungsrates mit beratender Stimme
- Betrieb eines Rechenzentrums an zwei geographisch getrennten Standorten:
  - aufbauend auf der physischen Sicherheitsarchitektur BOS-Digitalfunk Sachsen
  - Hauptsitz Leipzig, Nebensitz Dresden

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

GKDZ - Aufgaben I

- Zentraler Dienstleister auf dem Gebiet der polizeilichen TKÜ i. R. v. Auftragsdatenverarbeitung gem. § 11 BDSG, Compliance
- Errichtung und Betrieb von IT-Systemen zur Verarbeitung von entgegengenommenen Telekommunikationsdaten (berechtigte Stelle)
  - ohne selbst hoheitlich polizeiliche Aufgaben wahrzunehmen,
  - polizeifachliche Entscheidungen zur TKÜ verbleiben in den Polizeibereichen der Teilnehmerländer
- Hard- und Softwarekontrollen (Prozessmonitoring) und Wartungsarbeiten sowie die Beseitigung von Störungen an den betriebenen IT-Systemen,
- technisch-organisatorische Umsetzung der Maßnahmen auf dem Gebiet der polizeilichen TKÜ,
- Bereitstellung und Betrieb der technischen Schnittstellen zu den Datenverarbeitungssystemen der polizeilichen Nutzer

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

GKDZ - Aufgaben II

- logische Trennung der von den Verpflichteten an das GKDZ ausgeleiteten Überwachungskopien, mandantenfähige Speicherung, Verarbeitung und Bereitstellung
- technische Analyse und Decodierung von Rohdaten, GKDZ stellt die TKÜ-Daten interpretier- und auswertbar zur Verfügung,
- Identifizierung/ Analyse verschlüsselter Kommunikation und ggf. deren Entschlüsselung,
- Mandantentrennung, d.h. Datenzugriff erfolgt durch die jeweils ermittelnden und hierfür gesondert berechtigten Stellen/ Polizeivollzugsbeamten (VPN-Tunnel)
- Auftragsverwaltung (einschließlich Dokumentation der Aufwände, die der Polizei bei der Strafverfolgung oder Gefahrenabwehr im Rahmen der jeweils beauftragten Telekommunikationsüberwachung entstanden sind),
- Statistiken und Berichte zur Auftragsabwicklung sowie Kostenerhebung und unterstützende Maßnahmen für die Verwaltungshilfe durch die Teilnehmerländer,

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

GKDZ - Aufgaben III

- Wahrnehmung von Unterstützungsaufgaben im Bereich der Aus- und Fortbildung von Polizeibeamten auf dem Gebiet der polizeilichen TKÜ,
- Unterstützung und Beratung als fachkundige Stelle nach Maßgabe des Verwaltungsrates auf dem Gebiet der technisch-organisatorischen Weiterentwicklung und Umsetzung polizeilicher TKÜ
- Wahrnehmung weiterer Unterstützungsfunktionen, soweit die Kernaufgabe nicht beeinträchtigt wird

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Aktueller Stand

- Umsetzungsreife Grob-Konzepte (Geschäftsmodell, Personal, Finanzierung, techn.-org. Grobplanung, Prozessmodell etc.) sowie Staatsvertragsentwurf (StV-E) liegen vor und sind durch die zuständigen Abteilungsleiter der Innenresorts bestätigt
- WiBe-Ergebnis, Mittelbedarf → HH-Vorsorge in SN (Regierungsentwurf zum Haushaltsplan 15/16)
- Thematisierung in verschiedenen Pressemedien und im parlamentarischen Raum
- derzeit: UBV der Innen-StS, „Auftakt" für inhaltlich und zeitlich abgestimmte Kabinetts- und Parlamentsbefassungen
- Datenschutzbeauftragte:
  - Einbindung SächsDSB seit November 2013,
  - Vorlage des externen Rechtsgutachtens Februar 2015
  - Zentrale Infoveranstaltung für alle DSB am 14. April 2015
- Einbindung Justiz und Finanzen

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Ausblick

- Kabinetts- und Parlamentsbefassung
- gemeinsamer Aufbaustab
  - Satzung,
  - Geschäftsordnung des Verwaltungsrates,
  - Benutzerordnung,
  - Verträge über die Auftragsdatenverarbeitung,
  - technische und organisatorische Feinplanungen
- konstituierende Sitzung des Verwaltungsrates
- Probebetrieb (August 2017)
- Wirkbetrieb (April 2018)

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Datenschutz und IT-Sicherheit I

- vgl. Rechtsgutachten, insbesondere Seiten 141 - 178
- techn.-organisatorische Grobplanung/**systemische Anforderungen**: eindeutige Vorgaben des Rechtsgutachtens, welche das Design von Prozessen und Technik entscheidend beeinflusst haben:
  - Liegenschaft, Unterbringung, Brandmelde- und Löschanlage, physikalische Trennung von anderen Komponenten, Zugangskontrollsysteme
  - Elektronisches Überwachungs- und Alarmsystem für technische Fehlfunktionen
  - Datensicherheit (Angriffe von außen, technisch bedingte Verluste o. Verfälschungen)
  - Entgegennahme der Ausleitung, Speicherfähigkeiten
  - Mandantentrennung, Benutzerverwaltung, Rechte- und Rollenmodelle
  - ...

STAATSMINISTERIUM DES INNERN | Freistaat SACHSEN

Datenschutz und IT-Sicherheit II

- **Staatsvertragsentwurf**
  - Rechtsform
  - Aufgaben
  - Rechtsaufsicht
  - Anwendbares Datenschutzrecht, Auftragsdatenverarbeitung
  - Schutz personenbezogener Daten aus der TKÜ
  - Informationssicherheit
  - Informationspflichten
  - Sicherheitsüberprüfungen
- Handout: § § 1, 4, 10, 12 - 16 StV-E

Auszüge aus dem

Entwurf

Zur Vorlage bei den AL

mit Stand vom 21. Januar 2015
zum

„Staatsvertrag über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums (GKDZ) auf dem Gebiet der polizeilichen Telekommunikationsüberwachung der Teilnehmerländer als rechtsfähige Anstalt öffentlichen Rechts

(GKDZ-Staatsvertrag)

Vom“

Das Land Brandenburg, vertreten durch den Ministerpräsidenten, vertreten durch den Minister des Innern und für Kommunales,

das Land Sachsen-Anhalt, vertreten durch den Ministerpräsidenten, vertreten durch den Minister für Inneres und Sport,

der Freistaat Sachsen, vertreten durch den Ministerpräsidenten, vertreten durch den Staatsminister des Innern,

der Freistaat Thüringen, vertreten durch die Ministerpräsidenten, vertreten durch den Minister für Inneres und Kommunales,

das Land Berlin, vertreten durch den Regierenden Bürgermeister, vertreten durch den Senator für Inneres und Sport,

– im Folgenden „**Teilnehmerländer**“ –

schließen vorbehaltlich der Zustimmung ihrer verfassungsmäßig berufenen Organe folgenden

Staatsvertrag

über die Errichtung eines Gemeinsamen Kompetenz- und Dienstleistungszentrums auf dem Gebiet der polizeilichen Telekommunikationsüberwachung als rechtsfähige Anstalt des öffentlichen Rechts

– im Folgenden „**Anstalt**“ –

[...]

§ 1

Errichtung und Rechtsform, Name und Sitz, anzuwendendes Recht, Dienstsiegel

(1) Die Teilnehmerländer errichten auf dem Gebiet der polizeilichen Telekommunikationsüberwachung eine rechtsfähige Anstalt des öffentlichen Rechts.

(2) Die Anstalt trägt den Namen Gemeinsames Kompetenz- und Dienstleistungszentrum (GKDZ). Sie besitzt die Dienstherrnfähigkeit.

(3) Die Anstalt betreibt ein Rechenzentrum an zwei geographisch getrennten Standorten. Der Hauptsitz der Anstalt ist Leipzig. Ihr Nebensitz befindet sich in Dresden.

(4) Für die Errichtung und den Betrieb findet das sächsische Landesrecht Anwendung, soweit sich nicht aus den nachfolgenden Bestimmungen etwas anderes ergibt.

(5) Die Anstalt führt ein Dienstsiegel.

[...]

§ 4

Aufgaben, Benutzungsverhältnis

(1) Die Anstalt ist die zentrale Dienstleisterin der Teilnehmerländer auf dem Gebiet der polizeilichen Telekommunikationsüberwachung. Die Teilnehmerländer nutzen die Anstalt im Wege der Auftragsdatenverarbeitung für Daten aus polizeilichen Telekommunikationsüberwachungen (Kernaufgabe). Sie errichtet und betreibt IT-Systeme zur Verarbeitung von aufgezeichneten Telekommunikationsdaten, ohne selbst polizeiliche Aufgaben wahrzunehmen. Sie gewährleistet hierzu:

1. Hard- und Softwarekontrollen (Prozesscontrolling) und
2. Wartungsarbeiten sowie die Beseitigung von Störungen an den betriebenen IT-Systemen,
3. die technisch-organisatorische Umsetzung der Maßnahmen auf dem Gebiet der polizeilichen Telekommunikationsüberwachung,
4. die Gewährleistung der Schnittstellen zu den Datenverarbeitungssystemen der Polizei,
5. die technische Analyse und Decodierung von Rohdaten,
6. die Erkennung verschlüsselter Kommunikation und ggf. deren Entschlüsselung,
7. die Auftragsverwaltung (einschließlich Dokumentation der Auslagen, die der Polizei bei der Strafverfolgung oder Gefahrenabwehr im Rahmen der jeweils beauftragten Telekommunikationsüberwachung entstanden sind),
8. Statistiken und Berichte zur Auftragsabwicklung und unterstützende Maßnahmen der Verwaltungshilfe für das Fertigen von Statistiken und Berichten durch die Teilnehmerländer,
9. die Wahrnehmung von Unterstützungsaufgaben im Bereich der Aus- und Fortbildung von Polizeibeamten auf dem Gebiet der polizeilichen Telekommunikationsüberwachung.

Die Anstalt unterstützt und berät als fachkundige Stelle nach Maßgabe des Verwaltungsrates auf dem Gebiet der technisch-organisatorischen Realisierung polizeilicher Telekommunikationsüberwachung und kann hierzu weitere Unterstützungsfunktionen wahrnehmen, soweit die Kernaufgabe nicht beeinträchtigt wird.

(2) Wurde die Anstalt mit der Datenverarbeitung auf dem Gebiet der polizeilichen Telekommunikationsüberwachung beauftragt, ist sie berechtigt, die am Übergabepunkt gemäß § 5 Abs. 2 Satz 1 der Telekommunikationsüberwachungsverordnung (TKÜVO) bereitgestellten Daten entgegenzunehmen. Sie ist insoweit dann zugleich für die Vertragsparteien zentrale Kontaktstelle im Sinne der Nr. 2 der Allgemeinen Vorbemerkung der Anlage 3 zu § 23 Abs. 1 JVEG zur Anforderung und Abrechnung für Leistungen zur Telekommunikationsüberwachung.

(3) Zur Erledigung ihrer Aufträge zur Datenverarbeitung hat sich die Anstalt ihrer eigenen IT-Systeme zu bedienen. Die Anstalt kann sich im Übrigen Dritter bedienen, insbesondere der Teilnehmerländer, die der Anstalt die Inanspruchnahme von Unterstützungsleistungen gewähren. Näheres wird durch die Satzung der Anstalt und/oder in separat abzuschließenden Verwaltungsabkommen geregelt. Die zulässige Inanspruchnahme Dritter durch die Polizeien der Länder wird durch die Regelung nicht beschränkt.

(4) Das Nähere zur Ausgestaltung des Nutzungsverhältnisses regelt die Nutzungsordnung.

[...]

§ 11

Rechtsaufsicht über die Anstalt

Die Rechtsaufsicht über die Anstalt obliegt den Teilnehmerländern zusammen. Aufsichtsbehörde ist das Sächsische Staatsministerium des Innern. Es führt die Aufsicht im Benehmen mit den für Sicherheit und Ordnung zuständigen obersten Landesbehörden der übrigen Teilnehmerländer, soweit die Eilbedürftigkeit nicht ein unverzügliches Einschreiten gebietet.

[...]

§ 12

Anwendbares Datenschutzrecht, Auftragsdatenverarbeitung

(1) Für die Verarbeitung personenbezogener Daten durch die Anstalt, die nicht als Auftragsdatenverarbeitung erfolgt, gelten die Vorschriften des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (SächsDSG). Zuständiger Landesdatenschutzbeauftragter für die Anstalt ist der Sächsische Datenschutzbeauftragte.

(2) Verarbeitet die Anstalt personenbezogene Daten im Auftrag, gelten die Vorschriften über den Datenschutz des auftraggebenden Landes. Der Landesdatenschutzbeauftragte dieses Landes überwacht die Einhaltung dieser Vorschriften, berät die Anstalt insoweit in Fragen des Datenschutzes und nimmt das Kontrollrecht gegenüber der Anstalt wahr. Die Unterrichtung über eine gegenüber dem Vorstand der Anstalt erklärte Beanstandung erfolgt gegenüber der für öffentliche Sicherheit und Ordnung zuständigen obersten Landesbehörde des Auftrag gebenden Landes sowie gegenüber dem Sächsischen Staatsministerium des Innern als Rechtsaufsichtsbehörde.

(3) Der Sächsische Datenschutzbeauftragte, der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, der Landesbeauftragte für den Datenschutz Sachsen-Anhalt, der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit sowie der Berliner Beauftragte für Datenschutz und Informationsfreiheit können sich einvernehmlich mit der Durchführung der Kontrolle der Anstalt beauftragen. Die Anstalt lässt in diesem Fall eine Kontrolle durch den jeweils beauftragten Landesdatenschutzbeauftragten zu.

(4) Die Anstalt bestellt eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten im Sinne des § 11 SächsDSG. Diese oder dieser hat die Aufgabe für die im Wege der Auftragsdatenverarbeitung erfolgende Datenverarbeitung durch die Anstalt die Einhaltung der jeweiligen landesrechtlichen Datenschutzvorschriften, insbesondere der Vorschriften der jeweiligen Landesdatenschutzgesetze und der Landespolizeigesetze und der sich aus diesem Staatsvertrag und den hierauf beruhenden Abkommen und Verträgen ergebenden Anforderungen zu überwachen. Ihm obliegt ferner die Aufgabe der Überwachung der Verarbeitung eigener personenbezogener Daten durch die Anstalt nach § 19 Abs. 1 dieses Vertrages nach Maßgabe der Vorschriften des Gesetzes zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (SächsDSG).

§ 13

Schutz personenbezogener Daten aus der Telekommunikationsüberwachung

Durch den Betrieb der Anstalt darf der gesetzlich determinierte Zugriff der jeweiligen Polizeibehörden der Teilnehmerländer auf die Datensätze der polizeilichen Telekommunikationsüberwachung nicht erweitert werden. Die Polizeibehörden der Teilnehmerländer dürfen auch bei der zentralen Datenvorhaltung in der Anstalt ausschließlich auf die in ihrem Zuständigkeitsbereich und auf ihre Veranlassung hin erhobenen Daten zugreifen. Insoweit sind logisch getrennte Speicherbereiche für jedes Teilnehmerland anzulegen. Soweit das jeweilige Landesrecht neben repressiver auch präventive Telekommunikationsüberwachung zulässt, sind die Speicherbereiche entsprechend zu untergliedern; die Datensätze sind zwingend zu trennen. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Kenntnisnahme durch Nichtberechtigte ausgeschlossen ist.

§ 14

Informationssicherheit

(1) Die Anstalt hat alle angemessenen personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Bestimmungen dieses Staatsvertrages und der nach § 12 Absatz 2 des Vertrages geltenden Bestimmungen des Landesdatenschutzrechts entsprechende Datenverarbeitung zu gewährleisten. Hierbei ist einheitlich derjenige Sicherheitsstandard für die Aufbewahrung und Übermittlung von Daten zugrunde zu legen, der im Vergleich der Datenschutzgesetze der Länder als der strengste anzusehen ist. Die Maßnahmen richten sich nach den im Einzelfall zu betrachtenden Risiken und dem jeweiligen Stand der Technik. Die Mindestsicherheitsstandards richten sich nach den aktuellen IT-Grundschutzkatalogen

des Bundesamtes für Sicherheit in der Informationstechnik. Die Grundsätze der Datenvermeidung und der Datensparsamkeit sind zu beachten.

(2) Die nach dem jeweiligen Stand der Technik zu treffenden personellen, technischen und organisatorischen Maßnahmen sind auf der Grundlage eines Sicherheitskonzepts (Abs. 3) zu ermitteln und haben zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Erhebung, Verarbeitung und Nutzung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und der Entwicklung der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen.

(3) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der Datenverarbeitung sind von der Anstalt die zu treffenden personellen, technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Dazu gehört eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung. Entsprechend der technischen Entwicklung ist die Ermittlung in angemessenen Abständen zu wiederholen. Soweit trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken verbleiben, die nicht durch Maßnahmen nach den Absätzen 1 und 2 oder eine Modifizierung der Datenverarbeitung vermindert werden können, darf ein Verfahren nicht eingesetzt werden. Die Teilnehmerländer bestimmen die Rahmenbedingungen der Risikoanalyse und des Sicherheitskonzepts in der Satzung der Anstalt näher.

(4) Die Datenverarbeitung muss so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

(5) Die Anstalt bestellt eine behördliche IT-Sicherheitsbeauftragte oder einen behördlichen IT-Sicherheitsbeauftragten.

(6) Zuständiger Landesdatenschutzbeauftragter für die Anstalt hinsichtlich der Informationssicherheit ist der Sächsische Datenschutzbeauftragte. Dieser überwacht die Einhaltung der sich aus diesem Staatsvertrag und aus der Satzung der Anstalt ergebenden Anforderungen zur Informationssicherheit.

§ 15

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten und in sonstigen Fällen nicht unerheblicher Beeinträchtigungen der Informationssicherheit

(1) Stellt die Anstalt tatsächliche Anhaltspunkte dafür fest, dass bei ihr gespeicherte personenbezogene oder personenbeziehbare Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen, ist dies unverzüglich dem Innenministerium des jeweils Auftrag gebenden Landes zur Gewährleistung der Erfüllung etwaiger weitergehender gesetzlicher Pflichten mitzuteilen. Bei Fällen tatsächlicher Anhaltspunkte sonstiger nicht unerheblicher Beeinträchtigungen der Informationssicherheit erfolgt eine Mitteilung an das Sächsische Staatsministerium des Innern.

(2) Die Mitteilung muss Angaben zu der Art der unrechtmäßigen Kenntniserlangung, zu möglichen nachteiligen Folgen der unrechtmäßigen Kenntniserlangung und zu den daraufhin ergriffenen Maßnahmen enthalten.

(3) Die Mitteilung muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden sind.

§ 16

Sicherheitsüberprüfungen

Für die Voraussetzungen und das Verfahren zur Überprüfung von Personen, die von der Anstalt mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen oder bereits betraut worden sind, gilt das Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Freistaat Sachsen (Sächsisches Sicherheitsüberprüfungsgesetz – SächsSÜG) in der jeweils geltenden Fassung.

[...]