

Empfehlungen und Hinweise zu Aufgaben, Befugnissen und Zuständigkeiten des Beauftragten für den Datenschutz (BfdD) bei öffentlichen Stellen des Landes Sachsen-Anhalt

Gliederungsübersicht

1. Einsetzung des BfdD

2. Stellung und Befugnisse

3. Aufgaben des BfdD in der öffentlichen Stelle

- Beratung der Leitung der öffentlichen Stelle, der Mitarbeiter und des Personalrates
- Kontrollen der Datenverarbeitungsprozesse
- Datenschutzrechtliche Vorabkontrolle und Freigabe
- Führung des Verfahrensverzeichnisses
- Unterrichtung des Landesbeauftragten für den Datenschutz Sachsen-Anhalt (LfD LSA) über die Einrichtung automatisierter Abrufverfahren
- Unterrichtung des LfD LSA bei der Auftragsdatenverarbeitung durch nicht-öffentliche Stellen
- Kontrolle der Einhaltung des Datenschutzes bei der Verarbeitung oder Nutzung personenbezogener Daten bei Auftragnehmern
- Rechtzeitige Unterrichtung des LfD LSA über Planungen des Landes zum Aufbau automatisierter Informationssysteme nach § 22 Abs. 4 Satz 2 DSGVO
- Mitwirkung am Erlass von Richtlinien und anderen verwaltungsinternen Regelungen
- Mitwirkung bei der Erstellung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter)
- Mitarbeit bei der Gewährleistung der Rechte Betroffener, Mitbearbeitung von Bürgerangaben
- Beteiligung bei der Konzeption und Auswertung von Protokolldateien
- Schulung der Mitarbeiter
- Zusammenarbeit mit dem IT-Sicherheitsbeauftragten
- Verbindung zum LfD LSA und zu Datenschutzbeauftragten anderer Stellen

1. Einsetzung des BfdD gem. § 14a Abs. 1 DSG-LSA

In Deutschland ist das Wirken behördlicher und betrieblicher Datenschutzbeauftragter ein wichtiger Garant für die Gewährleistung des Datenschutzes. Die Selbstkontrolle geht der Fremdkontrolle durch den LfD LSA und die Aufsichtsbehörden vor.

Aus diesem Grunde hat auch der Landesgesetzgeber bei der Novellierung des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) im Jahre 2001 den **öffentlichen** Stellen die Pflicht zur Einsetzung eines BfdD auferlegt.

In welchen öffentlichen Stellen sind BfdD einzusetzen?

Die Verpflichtung zur Einsetzung eines BfdD gilt gem. § 14a Abs. 1 DSG-LSA für jede öffentliche Stelle im Sinne des § 3 Abs. 1 DSG-LSA, wenn diese zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten automatisierte (d.h. programmgesteuerte) Verfahren einsetzt. § 14a Abs. 1 Satz 3 DSG-LSA sieht aber Einschränkungen und Ausnahmen für Notare und die in § 3 Abs. 1 Satz 2 DSG-LSA genannten Stellen (u.a. Beliehene) vor. Ein BfdD muß auch dann nicht eingesetzt werden, wenn ausschließlich Verfahren, die der Unterstützung der allgemeinen Bürotätigkeit (§ 14 Abs. 4 Nr. 2 DSG-LSA) dienen, zum Einsatz kommen.

Durch die Einsetzung eines BfdD wird die Verantwortung der öffentlichen Stelle, insbesondere die deren Leitung, für die Sicherstellung des Datenschutzes in ihrem Verantwortungsbereich nach § 14 Abs. 1 DSG-LSA nicht ersetzt.

Welche Kriterien sind bei der Auswahl des BfdD zu beachten (§ 14a Abs. 2 DSG-LSA)?

Als BfdD darf nur eingesetzt werden, wer über die erforderliche Fachkunde in Fragen des Datenschutzes und der Datensicherheit und die erforderliche Zuverlässigkeit verfügt.

Bei fehlender fachlicher Qualifikation in Teilbereichen sollte ihm Gelegenheit gegeben werden, sich diese durch entsprechende Schulungsmaßnahmen anzueignen.

Um eine effektive Arbeit leisten zu können, sollte der BfdD eine Vertrauensperson sein, die mit den Aufgaben und der Arbeitsweise der öffentlichen Stelle möglichst aus eigener Erfahrung vertraut ist. Soll ein externer BfdD eingesetzt werden, ist die effektive Aufgabenerfüllung durch geeignete interne Ansprechpartner zu gewährleisten.

Darf der BfdD noch andere Aufgaben erfüllen?

Gem. § 14a Abs. 2 Satz 4 DSG-LSA ist der BfdD im erforderlichen Umfang von anderen Aufgaben freizustellen. Er muß jedoch nicht ausschließlich mit Aufgaben des Datenschutzes betraut sein. Je nach Größe der öffentlichen Stelle, Art und Umfang der Verarbeitung personenbezogener Daten und der damit möglicherweise verbundenen Datenschutzprobleme können ihm weitere Aufgaben übertragen werden. Dabei sind jedoch Interessenkonflikte oder Abhängigkeiten möglichst auszuschließen, die eine Aufgabenerfüllung gefährden würden.

Interessenkonflikte können insbesondere auftreten, wenn der BfdD gleichzeitig Aufgaben in Organisationseinheiten mit einer sehr umfangreichen oder sensiblen Verarbeitung personenbezogener Daten wahrnimmt oder z.B. Leiter des IT-Bereiches ist.

Geeignet sein können Mitarbeiter aus den Bereichen Justitiariat / Recht, Organisation, Rechnungsprüfung oder auch der IT-Sicherheitsbeauftragte, falls dieser nicht organisatorisch unmittelbar dem IT-Bereich zugeordnet ist.

Über welche Kenntnisse sollte der BfdD verfügen?

Er sollte die einschlägigen Rechtsvorschriften kennen und sicher anwenden können. Dazu gehören insbesondere

- die Grundrechte mit einem Bezug zum Datenschutz (vorrangig Art. 1 Abs. 1 und Art. 2 Abs. 1 GG sowie Art. 6 Abs. 1 LVerf),
- das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA),
- die zur Anwendung gelangenden spezialgesetzlichen Datenschutzbestimmungen,
- in bestimmten Fällen das BDSG.

Daneben sollte er

- über organisatorische Kenntnisse und Fähigkeiten,
- Verwaltungserfahrung sowie
- über ausreichende Kenntnisse auf dem Gebiet der Informations- und Kommunikationstechnik (IuK) verfügen.

Da der BfdD die Mitarbeiter der öffentlichen Stelle in allen Fragen des Datenschutzes beraten und unterstützen soll, würde eine einseitige Orientierung des BfdD auf Kenntnisse der IuK den gestellten Anforderungen ebensowenig gerecht werden wie eine einseitige Orientierung auf Rechtskenntnisse.

Wie erfolgt die Einsetzung des BfdD?

Im Allgemeinen wird der BfdD durch die Leitung der öffentlichen Stelle eingesetzt. Unterliegt die öffentliche Stelle einer Dienstaufsicht, kann gem. § 14a Abs. 1 Satz 2 DSG-LSA die Einsetzung auch durch die Dienstaufsichtsbehörde erfolgen. Die Einsetzung des BfdD hat schriftlich zu erfolgen und sollte im Wege einer Organisationsverfügung bzw. durch die Darstellung im Geschäftsverteilungsplan allen Mitarbeitern bekannt gemacht werden.

2. Stellung

Die gesetzlich garantierte Unabhängigkeit und organisatorisch herausgehobene Stellung ist für eine wirkungsvolle Tätigkeit des BfdD von ausschlaggebender Bedeutung. Er darf bei der Wahrnehmung seiner Aufgaben nicht den Weisungen der Organisationseinheiten unterliegen, die er zu kontrollieren hat (§ 14a Abs. 2 Satz 1 DSGVO). In seiner Funktion als BfdD sollte er im Sinne einer Stabsfunktion dem Leiter der öffentlichen Stelle zugeordnet sein. Der BfdD hat das direkte Vortragsrecht beim Leiter der öffentlichen Stelle (§ 14a Abs. 2 Satz 2 DSGVO). Soweit ein Bezug zu seiner Tätigkeit besteht, ist er umfassend und frühzeitig zu unterrichten. Dies kann geschehen durch:

- Beteiligung an Leitungsbesprechungen,
- Bekanntgabe von Planungen, die den Umgang mit personenbezogenen Daten betreffen,
- Verpflichtung aller Organisationseinheiten, den BfdD an datenschutzrelevanten Vorgängen zu beteiligen.

Wichtig ist auch, daß der BfdD von der Leitung der öffentlichen Stelle und von allen Mitarbeitern unterstützt wird. Soweit erforderlich, sind ihm Hilfspersonal sowie Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Für den Fall, daß er vertiefte rechtliche oder technische Beratung benötigt, sollten ihm geeignete Ansprechpartner zur Verfügung stehen, auf die er bei Bedarf zurückgreifen kann.

Werden nach Auffassung des BfdD bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten die Bestimmungen des DSGVO oder anderer Vorschriften zum Datenschutz verletzt, hat er die Verantwortlichen oder die Leitung der öffentlichen Stelle darauf hinzuweisen. Ein Weisungsrecht gegenüber den datenverarbeitenden Organisationseinheiten steht ihm nicht zu.

3. Aufgaben des BfdD in der öffentlichen Stelle (§ 14a Abs. 4 DSGVO)

Der BfdD soll dazu beitragen, daß die ihn einsetzende öffentliche Stelle den Erfordernissen des Datenschutzes umfassend Rechnung trägt. Er hat die Einhaltung der Vorschriften des Datenschutzes in allen Bereichen zu überwachen. Er nimmt seine Aufgaben vorrangig durch Beratung, aber auch durch Kontrollen wahr.

Für die Mitarbeiter der öffentlichen Stelle sollte der BfdD Ansprechpartner in allen Fragen des Datenschutzes sein, an den sie sich jederzeit vertrauensvoll wenden können. Bei erkannten Schwachstellen und Versäumnissen sollte er zunächst gemeinsam mit den Beteiligten nach konstruktiven Lösungen suchen.

Wichtig ist, den Mitarbeitern bewußt zu machen, daß Datenschutz positiv und nützlich ist und im Hintergrund stets der Betroffene mit seinen gesetzlich und verfassungsrechtlich verbrieften Rechten steht. Bei angemessener Verwirklichung wird der Datenschutz Arbeitsabläufe im Ergebnis eher fördern als erschweren.

Wenn eine öffentliche Stelle zu viele personenbezogene Daten sammelt, personenbezogene Daten zu schnell oder zu spät löscht oder personenbezogene Daten unberechtigt übermittelt, verstößt sie nicht nur gegen Datenschutzrecht, sondern verursacht auch unnütze Bürokratie und Mehrkosten. Datenschutz ist Element einer bürgerfreundlichen Verwaltung und trägt damit zum Gesamterfolg öffentlichen Handelns bei.

Der BfdD hilft der Leitung der öffentlichen Stelle, ihre Verantwortung für die Wahrung des Persönlichkeitsschutzes wahrzunehmen und Zwischenfälle zu vermeiden, die dem Ansehen der öffentlichen Stelle abträglich wären.

Zur sachgemäßen Durchführung seiner Aufgaben ist eine regelmäßige Weiterbildung des BfdD notwendig. Dazu können

- Fortbildungsseminare zum Datenschutz, die von den verschiedensten Stellen angeboten werden,
- Fachliteratur zum Datenschutz sowie
- Möglichkeiten des Erfahrungsaustausches mit anderen BfdD des gleichen Geschäftsbereiches oder aus öffentlichen Stellen mit verwandten Aufgaben

genutzt werden.

Der spezielle Zuschnitt der Aufgaben des BfdD richtet sich im Einzelfall nach den Aufgaben, der Größe, dem Aufbau und der Gliederung der jeweiligen öffentlichen Stelle. Der folgende Katalog gibt einen Überblick über die Aufgaben, die dem BfdD in jeder öffentlichen Stelle gesetzlich obliegen oder zusätzlich übertragen werden können:

Grundlegende Aufgaben

- Beratung der Leitung der öffentlichen Stelle, des Personalrats und der Mitarbeiter in datenschutzrelevanten Fragen.
- Durchführung von Kontrollen.

Zu diesem Zweck hat er Zutritt zu allen Diensträumen und kann alle dienstlichen Unterlagen einsehen, die personenbezogene Daten enthalten oder den Umgang mit diesen betreffen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist (§ 14a Abs. 3 Satz 1 und 3 DSGVO). Gem. § 14a Abs. 3 Satz 2 DSGVO gilt dies nicht, wenn Berufs- oder besondere Amtsgeheimnisse (z.B. das Arzt- oder Steuergeheimnis) entgegenstehen.

Übersichten und Register

- Führung des Verfahrensverzeichnisses gem. § 14a Abs. 4 Satz 1 DSGVO.
- Sammlung der Nachweise zur datenschutzrechtlichen Vorabkontrolle (§ 14a Abs. 4 Satz 2 Ziffer 2 DSGVO) von automatisierten Verfahren.

Automatisierte Abrufverfahren und Auftragsdatenverarbeitung

- Unterrichtung des LfD LSA über die Einrichtung automatisierter Abrufverfahren (§ 7 Abs. 3 DSG-LSA).
- Unterrichtung des LfD LSA über die Auftragsdatenverarbeitung nicht-öffentlicher Stellen (§ 8 Abs. 6 DSG-LSA).
- Kontrolle der Einhaltung des Datenschutzes bei Auftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 8 DSG-LSA)

Mitwirkung

- Erarbeitung oder Mitwirkung bei der Erstellung von Richtlinien, Rundschreiben, Dienstvereinbarungen und weiteren allgemeinen Verlautbarungen, die den Umgang mit personenbezogenen Daten betreffen.
- Mitwirkung bei der Erarbeitung und Anwendung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter).
- Mitwirkung bei Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsverlangen nach §§ 15 und 16 DSG-LSA, bei der Erstellung von Bürgerinformationen sowie bei allgemeinen Bürgereingaben und Anfragen zum Datenschutz.
- Beteiligung bei der Konzeption und Auswertung von Protokolldateien mit Personenbezug.

Schulung und Zusammenarbeit

- Schulung der Mitarbeiter zu Fragen des Datenschutzes und der Datensicherheit.
- Regelmäßige oder gelegentliche Berichte an die Leitung der öffentlichen Stelle über den Stand der Sicherstellung des Datenschutzes und der Datensicherheit innerhalb der öffentlichen Stelle.
- Zusammenarbeit mit dem IT-Sicherheitsbeauftragten.
- ggf. Zusammenarbeit mit den Datenschutzbeauftragten der Aufsichtsbehörde, anderer öffentlichen Stellen des Geschäftsbereichs und öffentlicher Stellen mit verwandten Aufgaben.
- Zusammenarbeit mit dem Personalrat

Besondere gesetzliche Regelungen zum Verhältnis zwischen Personalvertretung und BfdD bestehen nicht. Es ist aber vom Gebot der Zusammenarbeit auszugehen, denn der BfdD ist Teil der Dienststelle, und es gibt bei beiden gleichgerichtete Interessen. Deshalb unterstützt der BfdD die Personalvertretung. Er hat seinerseits die Unabhängigkeit der Personalvertretung zu beachten. Insoweit besteht kein Kontrollrecht des BfdD.

Erläuterungen zu den Einzelaufgaben:

- **Beratung der Leitung der öffentlichen Stelle, der Mitarbeiter und des Personalrates**

Der BfdD berät die Leitung der öffentlichen Stelle, die Organisationseinheiten, die personenbezogene Daten verarbeiten, und den Personalrat in allen Fragen des Datenschutzes sowie der datenschutzgerechten Organisation.

Dabei ist zu berücksichtigen, daß der Datenschutz sehr weit reicht und maßgeblich auch die innere Organisation der öffentlichen Stelle beeinflussen kann.

Dies betrifft auch Fragen der Zutrittsberechtigung (z.B. bei der Organisation von Reinigungs- oder Reparaturarbeiten), der Postbearbeitung oder Archivierung bis hin zur Gestaltung und Ausstattung von Diensträumen (u.a. hinsichtlich der Verschlusssicherheit von Räumen und Mobiliar und zur Gewährleistung der Vertraulichkeit bei Bürgergesprächen).

Der BfdD sollte bei Bedarf rechtzeitig über die Planung und Beschaffung von Hard- und Software, mit der personenbezogene Daten verarbeitet werden soll, sowie über die Einführung oder Änderung von IT-Verfahren informiert werden, um eventuelle datenschutzrechtliche Probleme vorab klären zu können.

Gleichzeitig sollte der BfdD darauf hinwirken, daß bei der Einführung oder Änderung von IT-Vorhaben ein spezifisches Sicherheitskonzept erarbeitet wird und die jeweils festgelegten Sicherheitsmaßnahmen auch umgesetzt werden. Maßstab für die Sicherheitsmaßnahmen bei der automatisierten Verarbeitung personenbezogener Daten bilden die Sicherheitsziele in § 6 Abs. 2 DSG-LSA.

- **Kontrolle der Datenverarbeitungsprozesse**

Kontrolle ist darauf gerichtet, Mängel zu erkennen und abzustellen. In der Regel ist es deshalb sinnvoll, schon während der Kontrolle mit den Beteiligten über mögliche Abhilfen zu sprechen. Beim Erarbeiten von Lösungen ist zu beachten, daß es nicht in erster Linie darauf ankommt, die vorgefundenen Symptome zu beseitigen. Es müssen vielmehr die Ursachen für Mängel festgestellt und über technische und organisatorische Maßnahmen hinaus ggf. auch die Organisationsstrukturen verändert werden. Hierbei kommt es darauf an, die Sensibilität und die Motivation der Verantwortlichen so zu fördern, daß der Datenschutz besser gewährleistet wird.

Werden erkannte Mängel von den verantwortlichen Organisationseinheiten auch nach Anmahnung nicht abgestellt, wird der BfdD die Leitung der öffentlichen Stelle spätestens dann unterrichten und deren Entscheidung herbeiführen müssen.

- **Datenschutzrechtliche Vorabkontrolle und Freigabe**

Gemäß § 14 Abs. 2 DSG-LSA ist vor dem erstmaligen Einsatz der dort genannten automatisierten Verfahren zu überprüfen, ob sie datenschutzrechtlich zulässig und die gem. § 6 Abs. 2 DSG-LSA zu treffenden technischen und organisatorischen Maßnahmen ausreichend sind. Diese Prüfung ist so rechtzeitig durchzuführen, daß erforderliche Änderungen ohne Schwierigkeiten vor Einführung oder besser bereits bei der Programmierung bzw. vor Erwerb des Verfahrens realisiert werden können.

Die Unterlagen zur Vorabkontrolle sollten vorzugsweise beim BfdD gesammelt werden.

- **Führung des Verfahrensverzeichnisses gem. § 14a Abs. 4 DSG-LSA**

Der BfdD führt das Verfahrensverzeichnis i.S. des § 14 Abs. 3 DSG-LSA.

Für dieses Verzeichnis besteht eine interne Meldepflicht für die die Verfahren betreibenden Organisationseinheiten innerhalb der öffentlichen Stelle. Für die schriftlichen Festlegungen gem. § 14 Abs.3 Nrn. 1 bis 9 DSG-LSA sind die Nutzer der Verfahren (Fachbereiche) verantwortlich, die den Nachweis der Erforderlichkeit und Zulässigkeit der im Verfahren verarbeiteten personenbezogenen Daten führen müssen.

Bei den Festlegungen über die genutzten Verfahren sollte der BfdD darauf achten, daß die Zwecke hinreichend präzisiert sind und jede Zweckänderung nur im Rahmen der Anforderungen des § 10 Abs. 2 DSG-LSA oder spezialgesetzlicher Regelungen erfolgt.

- **Unterrichtung des LfD LSA über die Einrichtung automatisierter Abrufverfahren**

Gem. § 7 Abs. 3 DSG-LSA ist der LfD LSA **vor** der Einrichtung eines automatisierten Abrufverfahrens zu unterrichten. Diese Unterrichtung unter Mitteilung der Festlegungen nach § 7 Abs. 2 DSG-LSA sollte durch den BfdD oder im Benehmen mit ihm erfolgen.

- **Unterrichtung des LfD LSA bei der Auftragsdatenverarbeitung durch nicht-öffentliche Stellen**

Ein Auftrag zur Verarbeitung oder Nutzung personenbezogener Daten durch andere Stellen ist nach § 8 Abs. 2 DSG-LSA schriftlich zu erteilen. Der BfdD sollte beim Erteilen derartiger Aufträge stets beteiligt werden. Dabei sollte er in den Fällen des § 8 Abs. 6 DSG-LSA darauf achten, daß vertraglich sichergestellt wird, daß der private Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den LfD LSA unterwirft.

Die Auftragsdatenverarbeitung durch nicht-öffentliche Stellen ist bei öffentlichen Aufgaben besonders sensibel. Deshalb hat der Gesetzgeber in § 8 Abs. 6 DSG-LSA zusätzliche Sicherheitsregeln vorgesehen. Die bei der Beauftragung nicht-öffentlicher Stellen geforderte Unterrichtung des LfD LSA (§ 8 Abs. 6 Satz 2 DSG-LSA) sollte durch den BfdD oder im Benehmen mit ihm vorgenommen werden.

- **Kontrolle der Einhaltung des Datenschutzes bei Auftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten im Auftrag**

Gemäß § 8 Abs. 3 DSGVO darf der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Der BfD sollte in geeigneter Weise kontrollieren, ob die Weisungen des Auftraggebers im jeweiligen Einzelfall eingehalten werden. Außerdem hat er sich gem. § 8 Abs. 2 DSGVO von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

- **Rechtzeitige Unterrichtung des LfD LSA über Planungen des Landes zum Aufbau automatisierter Informationssysteme nach § 22 Abs. 4 Satz 2 DSGVO**

Soweit die öffentliche Stelle dafür zuständig ist, hat sie nach § 22 Abs. 4 DSGVO die Verpflichtung, den LfD LSA rechtzeitig über Planungen des Landes zum Aufbau automatisierter Informationssysteme zu unterrichten, sofern in ihnen personenbezogene Daten verarbeitet oder genutzt werden sollen. Hierbei kann und muß der BfD eine umfassende und zeitgerechte Vorarbeit leisten.

- **Mitwirkung am Erlaß von Richtlinien und anderen verwaltungsinternen Regelungen**

Richtlinien, Rundschreiben o.ä., die die Leitung der öffentlichen Stelle als Querschnittsregelungen zum Umgang mit personenbezogenen Daten erläßt, sollten unter Beteiligung des BfD erarbeitet werden.

Für Regelungen im IT-Bereich können die in den Tätigkeitsberichten des LfD LSA gegebenen Empfehlungen Anhaltspunkte geben.

Bei der Erarbeitung von Dienstvereinbarungen zwischen der Dienststelle und dem Personalrat über den Umgang mit personenbezogenen Daten sollte der BfD hinzugezogen werden.

- **Mitwirkung bei der Erstellung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter)**

In der Verwaltung werden zur Rationalisierung der Verwaltungsabläufe Vordrucke eingesetzt. Dabei zeigt sich immer wieder, daß vielfach Daten über das erforderliche Maß hinaus erhoben werden. Ursache kann sein, daß nach Änderung von Rechtsvorschriften keine Anpassung der Vordrucke an die geänderte Rechtslage erfolgt ist, gemeinsame Vordrucke für verschiedene Verwaltungsaufgaben verwendet werden oder Vordrucke anderer Bundesländer übernommen werden, ohne vorher geprüft zu haben, ob in Sachsen-Anhalt die gleichen rechtlichen Voraussetzungen zum Umgang mit personenbezogenen Daten vorliegen.

Zur Gewährleistung des Datenschutzes sollte deshalb der BfD die von der öffentlichen Stelle genutzten Vordrucke in seine Prüfung permanent einbeziehen und zumindest bei Eigenentwicklungen in die Prüfung der Zulässigkeit der Datenerhebung einbezogen werden.

- **Mitarbeit bei der Gewährleistung der Rechte der Betroffenen, Mitbearbeitung von Bürgereingaben**

Die Arbeitsteilung zwischen dem BfdD und den zuständigen Fachabteilungen hängt wesentlich vom speziellen Aufgabenbereich und von der Größe der öffentlichen Stelle ab. Bei der Beantwortung allgemeiner Bürgereingaben und -anfragen zum Datenschutz sollte der BfdD grundsätzlich hinzugezogen werden. Ansonsten wird besonders bei aus datenschutzrechtlicher Sicht problematischen oder bedeutsamen Angelegenheiten eine Einbindung des BfdD erforderlich sein. Dementsprechend sollte er auch bei der Einführung neuer Auskunftsverfahren, bei der Erstellung von Merkblättern für Bürger und bei der datenschutzgerechten Gestaltung von Formularen gehört werden (s.o.).

- **Beteiligung bei der Konzeption und Auswertung von Protokolldateien**

Bei der Einführung automatisierter Verfahren sollte grundsätzlich die Erforderlichkeit und der Umfang zur Führung von Protokolldateien geprüft und festgelegt werden. Auch eine Protokolldatei kann datenschutzrechtliche Risiken in sich bergen.

Auch die Auswertung personenbezogener Protokolldaten (i.d.R. nur in Form von Stichproben) sollte unter Beteiligung des BfdD erfolgen (vgl. z.B. § 28 Abs. 4 DSGVO).

- **Schulung der Mitarbeiter**

Für die Schulung und sonstige Unterrichtung der Mitarbeiter, die personenbezogene Daten erheben, verarbeiten oder nutzen, bieten sich an:

- Einweisung neuer Mitarbeiter, Hinweis auf das Datengeheimnis (§ 5 DSGVO)
- Schulung im Rahmen der allgemeinen Aus- und Fortbildung der Bediensteten
- Vorträge oder Referate für einzelne Abteilungen oder Mitarbeitergruppen
- Ausgabe von Merkblättern, die nach Bedarf aktualisiert werden
- Mitteilungen am Schwarzen Brett
- Mitteilungen in Dienstbesprechungen
- Berichte bei Personalversammlungen
- Beiträge zu Hauszeitschriften und sonstigen internen Mitteilungsblättern
- Verteilung geeigneter Literatur (z.B. Informationsmaterial des LfD LSA)
- Hinweise auf das Informationsangebot des LfD LSA oder anderer Einrichtungen im Intranet bzw. Internet

- **Zusammenarbeit mit dem IT-Sicherheitsbeauftragten**

Sofern die öffentliche Stelle einen IT-Sicherheitsbeauftragten bestellt hat und keine Personalunion mit dem BfdD besteht, empfiehlt sich naturgemäß eine enge Zusammenarbeit. Der BfdD sollte vor allem bei der Erstellung eines IT-Sicherheitskonzeptes hinzugezogen werden, damit auch aus datenschutzrechtlicher Sicht die Belange der Datensicherheit (§ 6 Abs. 2 DSG-LSA) im erforderlichen Maß berücksichtigt werden.

Auch bei der Überprüfung, ob die im IT-Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen in der Praxis umgesetzt werden, ist ein gemeinsames koordiniertes Vorgehen wünschenswert.

- **Verbindung zum LfD LSA und zu Datenschutzbeauftragten anderer Stellen**

Für auch durch Beratung mit der zuständigen Fachaufsichtsbehörde nicht lösbare Probleme auf den Gebieten Datenschutz und Datensicherheit und bei der Erledigung seiner Aufgaben nach § 14a Abs. 4 Satz 2 Nr. 2 DSG-LSA in Zweifelsfällen findet der BfdD Ansprechpartner beim LfD LSA. Bei der letztgenannten Aufgabe muß der Dienstweg nicht einzuhalten werden.

Gleichartige datenschutzrechtliche Fragestellungen treten häufig in mehreren öffentlichen Stellen parallel auf. Deshalb sollte dem Erfahrungsaustausch große Beachtung geschenkt werden. Dazu sollte der BfdD den Informationsaustausch zum BfdD seiner Fachaufsichtsbehörde und insbesondere zu den BfdD von öffentlichen Stellen mit verwandten Aufgaben suchen.

Auch sollten die im Abstand von 2 Jahren erscheinenden Tätigkeitsberichte des LfD LSA (§ 22 Abs. 4a DSG-LSA) sowie dessen Homepage (www.datenschutz.sachsen-anhalt.de) als wichtige Informationsquellen genutzt werden.