



Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Andrea Voßhoff

Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit

POSTANSCHRIFT Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,
Postfach 1468, 53004 Bonn

Staatssekretär im
Bundesministerium der Finanzen

Wilhelmstr. 97
10117 Berlin

nachrichtlich:

Bundesministerium der Finanzen
- Projekt PVS -
Wilhelmstr. 97
10117 Berlin

Bundesministerium der Finanzen
- behördlicher Datenschutzbeauftragter -
Wilhelmstr. 97
10117 Berlin

Generalzolldirektion
Am Probsthof 78 a
53121 Bonn

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL @bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 13.04..2017
GESCHÄFTSZ. 12-452/051#0058

Bitte geben Sie das vorstehende Geschäftszeichen bei
allen Antwortschreiben unbedingt an.

BETREFF **Datenschutzrechtlicher Beratungs- und Kontrollbesuch im Bereich Personal-
wesen bei der Bundesfinanzdirektion Südwest (BFD Südwest) in der Zeit vom
13. bis 16. Oktober 2015**

BEZUG Mein Ankündigungsschreiben vom 11. August 2015 - III-452/051#0058 -

Sehr geehrter Herr [REDACTED],

in der Zeit vom 13. bis 16. Oktober 2015 haben meine Mitarbeiter, [REDACTED]
[REDACTED] einen datenschutzrechtlichen Beratungs- und Kontroll-
besuch nach § 24 Absatz 1 und § 26 Absatz 3 Bundesdatenschutzgesetz (BDSG)
bei der BFD Südwest zum Umgang mit Personal- und Personalaktendaten der dort
Beschäftigten - insbesondere im Zusammenhang mit dem hierfür eingesetzten „ein-



heitlichen Personalverwaltungssystem in der BFV (PVS)" - durchgeführt. Der Besuch wurde durch den stellvertretenden Beauftragten für den Datenschutz des Bundesministeriums der Finanzen (BMF), [REDACTED] sowie [REDACTED] aus dem Projekt PVS des BMF begleitet. Für die gewährte Unterstützung bedanke ich mich.

I. Allgemeines

Mein Besuch bei der BFD Südwest stand u. a. in Zusammenhang mit meinem Kontroll- und Beratungsbesuch bei der BFD Nord in der Zeit vom 7. bis 10. Juli 2014, über den ich auch in meinem 25. Tätigkeitsbericht (Nr. 5.7.4) berichtet hatte. Zu meinem Kontrollbericht vom 12. Januar 2015 - III-452/05#0058 - hatten Sie mit Schreiben vom 3. März 2015 - DSB-O1991/14/10002 - Stellung genommen. Der Besuch bei der BFD Südwest sollte hierbei auch die Umsetzung der mir vom BMF gegebenen Zusagen zur automatisierten Personaldatenverarbeitung im dortigen Praxisbetrieb überprüfen.

II. Konkrete Feststellungen

Feststellungen mit Beanstandung

Die Kontrolle in der BFD Südwest führte zusammenfassend insbesondere zu folgenden Feststellungen:

- Unzulässige Speicherung von – teilweise sehr sensiblen - Personalaktendaten (vgl. Nr. 2.1).
- Mangelnder Zugriffsschutz auf Personalaktendaten in Laufwerken des Personalbereichs (vgl. Nr. 2.2).
- Unzulässiger Umgang mit Personal- und Personalaktendaten in manueller Form (vgl. Nr. 3.1).

Die Feststellungen sind in der Summe so gravierend, dass ich sie nach § 25 Abs. 1 BDSG als Verstoß gegen die Regelungen der §§ 106 ff BBG, insbesondere in § 107 Abs. 1 und § 113 Abs. 2 BBG sowie gegen § 12 Abs. 4 i.V.m. § 32 Abs. 1 BDSG beanstanden muss.



SEITE 3 VON 13 **Feststellungen mit Empfehlungen**

- Beendigung des parallelen elektronischen und manuellen Umgangs mit Beschäftigendaten bei der Urlaubsverwaltung (vgl. Nr.1.4).
- Erstellung elektronischer Mustervorlagen (vgl. Nr. 2.3).
- Anpassung der Dienstvereinbarung zur Gleitenden Arbeitszeit an die Rechtslage (vgl. Nr. 2.4).
- Anschaffung von Metallschränken zur Aufbewahrung von Personalakten (vgl. Nr. 3.2).
- Verbesserung des Krankmelde-Verfahrens (vgl. Nr. 3.3).
- Entfernung brennbarer Stoffe aus dem Serverraum und sichere Lagerung von Datenträgern (vgl. Nr. 4.1).
- Erstellung eines Konzeptes zur Datenträgervernichtung (vgl. Nr. 4.2).
- Erhöhung der Datensicherheit bei der Nutzung von Notebooks (vgl. Nr. 4.3).
- Einsatz geeigneter Verschlüsselungssoftware (vgl. Nr. 4.4).

Die Feststellungen beruhen auf folgenden Erkenntnissen:

1. Personalverwaltungssystem PVS

1.1 Zugriffsberechtigungen

Die stichprobenartige Prüfung der in der BFD Südwest erteilten Zugriffsberechtigungen in PVS (schwerpunktmäßig in den Arbeitsbereichen RF 11 und RF 12) entsprach im Ergebnis den gesetzlichen Bestimmungen. Die Vorgaben des § 107 Absatz 1 Bundesbeamten-gesetz (BBG) - Zugang zur Personalakte - waren im Praxisbetrieb umgesetzt.

1.2 Vergabe von Rollen in PVS

Nach der Kontrolle der BFD Nord hatte ich empfohlen, den jeweiligen Auftrag zur Vergabe einer bestimmten Berechtigung in PVS und damit die Gewährleistung des Zugangs zu Personalaktendaten schriftlich zu dokumentieren und beim zuständigen „Rollenverwalter“ aufzubewahren. Daraufhin hat das BMF ein neues Rollenverfahren, einschließlich der Möglichkeit, die in einer Dienststelle vergebenen Zugriffsberechtigungen im Einzelfall überprüfen zu können, erstellt und mich hierüber unterrichtet.

Dieses neue PVS-Rollenkonzept habe ich in der BFD Südwest geprüft und als datenschutzgerecht bewertet.



1.3 Sonstige Feststellungen zum Wirkbetrieb von PVS

Die stichprobenartige Prüfung der aktuellen, in PVS gespeicherten Personal-/Personalaktendaten der Beschäftigten ergab auch in der BFD Südwest, dass diese für Zwecke der Aufgabenerfüllung fachlich begründet, also (noch) erforderlich und damit zulässig gespeichert waren. Die auf Grund der gesetzlichen Aufbewahrungs-/Löschungsvorschriften - z.B. des BBG - notwendigen Löschungen (z.B. zu Urlaub oder Erkrankungen der Beschäftigten) waren in PVS erfolgt.

Auch die Einsichtsrechte der Betroffenen (vgl. § 110 Absatz 1 und 4 BBG, § 114 Absatz 5 BBG) waren in der BFD Südwest durch die Möglichkeit, sich jederzeit an seinem Arbeitsplatz unter Eingabe eines Passwortes die eigenen, in PVS gespeicherten Personal-/Personalaktendaten ansehen zu können, im Praxisbetrieb gewährleistet.

Die Prüfung der in PVS gespeicherten „Bemerkungsfelder/Freitextfelder“ ergab keine unzulässigen Inhalte. Die gesetzlich vorgeschriebene Erforderlichkeit der eingetragenen Inhalte zur aktuellen, konkreten Aufgabenerfüllung der Personalstelle lag vor.

1.4 Unzulässiger paralleler Umgang mit Beschäftigtendaten

Allerdings mussten meine Mitarbeiter wiederum feststellen, dass - u.a. auf Grund von (laut PVS-Anwendern) „mangelndem Vertrauen in PVS“ - bestimmte Aufgaben/Verarbeitungen mit Beschäftigtendaten neben PVS zusätzlich auch noch in Papierform, also manuell wahrgenommen werden.

So erfolgt in der BFD Südwest die gesamte Urlaubsbearbeitung (Erholungsurlaub und Sonderurlaub) - obwohl vom BMF so vorgegeben - nicht ausschließlich automatisiert in PVS, sondern parallel zusätzlich noch manuell in Papierform mittels Urlaubs-Pendelkarten oder Akten (zu den Einzelfeststellungen vgl. Nr. 3.1).

Eine entsprechende Rechtsgrundlage oder Erforderlichkeit für einen solchen zusätzlichen Umgang mit Personalaktendaten ist nicht ersichtlich. Die parallele Erhebung, Verarbeitung und Nutzung von Personalaktendaten (Urlaubsdaten) stellt eine unzulässige Vorratsdatenspeicherung dar und verstößt zudem gegen den Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG).



Dieser Umgang mit Beschäftigtendaten betraf erneut auch besondere Arten personenbezogener Daten im Sinne des § 3 Absatz 9 BDSG (Angaben über Gesundheit). Da ich einen solchen unzulässigen Umgang mit Personal-/Personalaktendaten bereits bei der Kontrolle in der BFD Nord festgestellt habe, scheint es sich um ein grundsätzliches Problem beim Einsatz von PVS zu handeln.

Ich empfehle, das jetzt Notwendige zu veranlassen, um zukünftig einen solchen unzulässigen Parallelbetrieb beim Umgang mit Beschäftigtendaten in den PVS-Anwenderbehörden zu vermeiden.

Für eine Stellungnahme hierzu wäre ich dankbar.

2. Automatisierte Personaldatenverarbeitung außerhalb von PVS

2.1 Unzulässige Speicherung von Beschäftigtendaten

Wie bereits bei der Kontrolle der BFD Nord bemängelt, haben meine Mitarbeiter auch an verschiedenen Arbeitsplätzen des Referates RF 1 in sehr großer Anzahl alte, unzulässige Dokumente sowie Excel-Listen mit teilweise sehr sensiblen Beschäftigtendaten außerhalb von PVS vorgefunden. Diese hätten nach den gesetzlichen Aufbewahrungs-/Löschungsregelungen (z. B. des § 113 Absatz 2 BBG) längst gelöscht sein müssen, da sie für die Aufgabenerfüllung der BFD Südwest nicht mehr erforderlich waren. Hierbei handelte es sich insbesondere um Beschäftigtendaten zu abgeschlossenen Personalvorgängen, z. B. um Bewerber-Ranglisten (u.a. mit Fotos der Betroffenen) aus lange abgeschlossenen Bewerbungsverfahren ab dem Jahr 2009, um Beschäftigtendaten zu einem im Jahre 2013 beendeten Regelbeurteilungsdurchgang oder zu Personal-/Stellenbesetzungsverfahren aus dem Jahr 1999. Unzulässigerweise waren zudem auch besondere Arten personenbezogener Daten im Sinne des § 3 Absatz 9 BDSG (Gesundheitsdaten) gespeichert, z.B. eine Auswertung über Langzeiterkrankte einer Organisationseinheit oder Schreiben zur Versetzung in den Ruhestand wegen Dienstunfähigkeit mit einem kompletten ärztlichen Gutachten.

Diese Beschäftigtendaten waren außerhalb vom PVS ebenfalls für die Zwecke der Personalverwaltung/Personalwirtschaft - für die in der Bundesfinanzverwaltung gerade PVS eingeführt und entwickelt worden ist - gespeichert. Bei solchen zusätzlichen automatisierten Verarbeitungen von Personal- und Per-



sonalaktendaten greifen – hierauf hatte ich bereits bei der Kontrolle der BFD Nord hingewiesen – nicht die umfassenden, aus datenschutzrechtlicher Sicht positiven und einschränkenden Regelungen zu PVS.

2.2 Mangelnder Zugriffsschutz in Laufwerken des Personalbereichs

Erneut haben meine Mitarbeiter in diesem Zusammenhang auch in der BFD Südwest erhebliche datenschutzrechtliche Mängel festgestellt.

Außerhalb von PVS stehen den Beschäftigten - auch im Referat RF 1 - zur Speicherung von Beschäftigtendaten verschiedene Laufwerke zur Verfügung. Bei den Zugriffsberechtigungen wird jedoch nicht nach der konkreten Aufgabenzuteilung einer Bearbeiterin/eines Bearbeiters nach dem Geschäftsverteilungsplan unterschieden. Wie sich daraus ergibt, kann in der Regel jeder Beschäftigte eines Arbeitsbereiches in den Gruppenlaufwerken alle Dokumente oder Excel-Listen mit Beschäftigtendaten lesen und bearbeiten und hat somit auch Zugang zu Personalaktendaten, auch soweit er für die Aufgabenerledigung nicht zuständig ist. Dies ist unzulässig und stellt - aufgrund der festgestellten sehr großen Anzahl von Dokumenten mit sehr sensiblen Inhalten - einen erheblichen Verstoß gegen § 107 Absatz 1 BBG (Zugang zur Personalakte) dar. Die Einhaltung dieser Vorschrift wird im Übrigen in PVS über das datenschutzgerechte Berechtigungskonzept gewährleistet.

Allerdings sind die Zugriffsberechtigungen nicht datenschutzkonform ausgestaltet, was ich beanstandete. Gleichzeitig empfehle ich erneut dringend, die Zugriffsberechtigungen auf Gruppenlaufwerke im Personalbereich so einzuschränken, dass Zugriffsrechte nur dann an einen Beschäftigten vergeben werden, wenn das Laufwerk für dessen Aufgabenerledigung (Personalverwaltung/Personalwirtschaft) benötigt und der Zugang zu Personalaktendaten hierfür erforderlich ist. Wie dies gleichzeitig voraussetzt, müssen die einzelnen Personalaufgaben in den Sachbereichen so strukturiert sein, dass eine entsprechende Aufteilung der jetzt gemeinsam genutzten Laufwerke möglich ist. Für eine datenschutzrechtliche Beratung bei der Umsetzung stehe ich der BFD Südwest - wie bereits angeboten - gerne zur Verfügung.

2.3 Mustervorlagen statt Musterschreiben

Auch bei dieser Kontrolle haben meine Mitarbeiter an verschiedenen Arbeitsplätzen im Personalbereich wieder elektronische Musterschreiben vorgefunden. Sie haben erneut darauf hingewiesen, dass aus datenschutzrechtlicher Sicht anstelle von Musterschreiben (Format .doc) Mustervorlagen (Format



.dot) ohne Personenbezug verwenden werden sollten, damit keine personenbezogenen Daten in den vermeintlichen Musterschreiben zurückbleiben. Ich rege deshalb erneut an zu prüfen, Musterschreiben bereits in PVS zu integrieren und den Nutzern zur Verfügung zu stellen. Sofern dies für einzelne Schreiben nicht möglich ist, sollten die Musterschreiben in Mustervorlagen geändert werden.

Ich wäre Ihnen dankbar, wenn Sie diese (sich wiederholenden) Kontrollfeststellungen zum Anlass nehmen könnten, das Notwendige - auch aus grundsätzlicher Sicht - zu veranlassen und mir die Löschung aller unzulässigen Personal-/Personalaktendaten außerhalb von PVS in der BFD Südwest zu bestätigen.

2.4 Automatisiertes Verfahren zur Gleitenden Arbeitszeit

Auch bei der Durchführung der Gleitenden Arbeitszeit, die in der BFD Südwest auf Grundlage der „Dienstvereinbarung über die Arbeitszeit“ in der Fassung vom 15. November 2010 eingeführt ist, haben meine Mitarbeiter datenschutzrechtlichen Handlungsbedarf aufgezeigt und konkrete datenschutzrechtliche Empfehlungen gegeben.

Dies gilt insbesondere für die Regelung in § 14 Absatz 2 Satz 2 der Dienstvereinbarung, die den jeweils zuständigen Vorgesetzten das Recht einräumt, Arbeitszeitübersichten – dies sind lt. Vertretern der BFD Südwest die Arbeitszeitjournale mit allen Einzelbuchungen – stichprobenweise einzusehen. Dies verstößt gegen § 7 Absatz 8 der Verordnung über die Arbeitszeit der Beamtinnen und Beamten des Bundes (Arbeitszeitverordnung – AZV). Unmittelbare Vorgesetzte dürfen danach keinen Zugang zu den Gleitzeitkonten oder den Einzelbuchungen der Beschäftigten ihrer Organisationseinheit haben. Auch die Regelung, nach der die „Leitung der Behörde“ (in Neustadt und in Trier) und deren Vertretungen ebenfalls Zugang zu den Zeiterfassungsdaten der Beschäftigten haben (§ 15 der Dienstvereinbarung), bewerte ich mangels Rechtsgrundlage als unzulässig. Ich rege an, diese Regelungen der Dienstvereinbarung bei Gelegenheit der Rechtslage anzupassen.

Bezogen auf einen festgestellten, allerdings nicht hinreichend in den Akten dokumentierten konkreten Fall einer solchen Einsichtnahme in das Gleitzeitkonto eines Beschäftigten und entsprechende Auswertung seiner personenbezogene Daten wegen - so die Auskunft der BFD Südwest - Verdachts auf eine vom Betroffenen begangene Straftat im Beschäftigungsverhältnis (Gleitzeitbetrug) haben meine Mitarbeiter auf die sehr einschränkenden Vorausset-



zungen des § 32 Absatz 1 Satz 2 BDSG zur Aufdeckung einer solchen Straftat aufmerksam gemacht und um strikte Beachtung gebeten. Eine Prüfung, ob diese im konkreten Fall vorlagen, war meinen Mitarbeitern vor Ort nachträglich nicht (mehr) möglich. Ebenso konnte nicht (mehr) festgestellt werden, ob die ebenfalls dokumentierten, separat durchgeführten Einsichtnahmen durch den ÖPR-Vorsitzenden und durch den stellvertretenden ÖPR-Vorsitzenden in dieses Zeiterfassungskonto auf Grundlage von schriftlichen Bevollmächtigungen durch den Betroffenen erfolgten. Nur in diesem Fall wären sie rechtmäßig gewesen, da Personalvertretungen oder ihren Mitgliedern kein Einsichtsrecht in Gleitzeitbuchungen/Zeitkonten von Beschäftigten (auch nicht auf Basis des § 32 Absatz 1 Satz 2 BDSG) zusteht. Meine Mitarbeiter haben empfohlen, die Bedingungen und den Ablauf eines solchen Verfahrens nach § 32 Absatz 1 Satz 2 BDSG in der BFD Südwest allgemein zu regeln und in einem solchen konkreten Fall diesen hinreichend aktenkundig zu machen.

Ich wäre Ihnen dankbar, wenn Sie mir die Umsetzung meiner Empfehlungen zur Gleitenden Arbeitszeit bestätigen könnten.

3. Manueller Umgang mit Beschäftigtendaten

3.1 Bearbeitung von Urlaubsangelegenheiten

Erhebliche Datenschutzverstöße haben meine Mitarbeiter bei der manuellen (neben PVS zusätzlichen) Urlaubsbearbeitung in der BFD Südwest festgestellt, die umfassend auch besondere Arten personenbezogener Daten i.S.d. § 3 Absatz 9 BDSG (Angaben über die Gesundheit) zum Gegenstand hatte. Allgemein bewerte ich diesen zusätzlichen parallelen Umgang mit Personalaktendaten neben PVS als unzulässig (vgl. Nr. 1.4).

In Ordnern fanden meine Mitarbeiter in sehr großer Anzahl Beschäftigtendaten der BFD Südwest, die ihr von früheren Beschäftigungsbehörden (Wehrbereichsverwaltungen) ausschließlich zum Abgleich bzw. Übernahme von Urlaubsansprüchen übersandt worden waren. Dort waren unzulässigerweise und teilweise bereits seit langem zu vernichtende Personal-/Personalaktendaten gespeichert, z.B. zu Erkrankungen und sonstigen Abwesenheiten der Beschäftigten ab dem Jahre 1998 oder zu Urlauben ab dem Jahre 2002. Eine Urlaubsunterlage zu einer Mitarbeiterin enthielt zudem ohne Rechtsgrundlage Angaben zu einer bestehenden Schwangerschaft mit dem voraussichtlichen Geburtstermin.



In einer Personal-Teilakte „Urlaub“ eines Bediensteten hatte die BFD Südwest unzulässigerweise eine Sammlung mit ärztlichen Attesten aus den Jahren 2004 - 2006 und 2008, die das minderjährige Kind des Beschäftigten betrafen, sowie alte Urlaubsanträge/-genehmigungen ab dem Jahre 2003 gespeichert. Zu einem anderen Mitarbeiter fand sich diverser Schriftverkehr ab dem Jahre 2008 zu einem beantragten und abgelehnten Sonderurlaub. Unzulässig gespeichert waren auch alte Urlaubskarten von Vorgesetzten aus den Jahren 2010 und 2011.

Dies verstößt gegen § 113 Absatz 2 BBG. Danach sind Unterlagen über Erkrankungen fünf Jahre und solche zu Erholungsurlaub drei Jahre nach Ablauf des Jahres in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, zu löschen. In PVS ist das gesetzmäßige Löschen dieser Personalaktendaten über Löschroutinen sichergestellt.

3.2 Mangelhafte Aufbewahrung von Personalakten

Die Aufbewahrung der (inhaltlich nicht geprüften Personalakten) erfolgt in der BFD Südwest - außer bei denen des höheren Dienstes - in Büro-Rollladenschränken. Mehrere Schränke waren zum Kontrollzeitpunkt zudem defekt, die Rollläden gerissen und notdürftig mit Klebebändern repariert. Somit war ohne technischen Aufwand ein unberechtigter Zugang zu diesen (auch verschlossenen) Büroschränken und damit auch zu den Personalakten möglich, eine hinreichende Sicherheit nicht gewährleistet. Dies stellt einen Verstoß gegen § 106 Absatz 1 Satz 1 BBG dar, wonach die Personalakten vertraulich zu behandeln und durch technische und organisatorische Maßnahmen vor einer unbefugten Einsichtnahme zu schützen sind.

Meine Mitarbeiter haben bereits empfohlen, die vorhandenen Rollladenschränke gegen Metallschränke auszutauschen, wie sie in der BFD Südwest z.B. zur Lagerung der Personalakten des höheren Dienstes verwendet werden.

3.3 Krankmelde-Verfahren

Wie festgestellt, gelangen die Dienst-/Arbeitsunfähigkeitsbescheinigungen der Beschäftigten nicht direkt verschlossen in das Personalreferat der BFD Südwest, da die entsprechenden Briefe bereits in der Poststelle geöffnet werden. Die Beschäftigten der Poststelle sind jedoch nicht berechtigt, diese sensiblen, besonderen Arten personenbezogener Daten nach § 3 Absatz 9 BDSG (Krankmeldungen/Angaben über Gesundheit) zur Kenntnis zu nehmen. Meine



Mitarbeiter haben deshalb bereits vor Ort empfohlen, die innerbehördliche Organisation so zu gestalten, dass weder die Mitarbeiter der Poststelle, noch Boten oder die jeweiligen Fachvorgesetzten, sondern nur die mit der Bearbeitung von Erkrankungen der Beschäftigten Beauftragten solche ärztlichen Bescheinigung einsehen/erhalten dürfen. Dies sollte in einer Dienstanweisung/Organisationsverfügung geregelt werden.

4. Allgemeine technische und organisatorische Feststellungen

4.1 Mängel im Rechnerraum

Bei der Prüfung des Serverraums haben meine Mitarbeiter dort neben üblichen Hardware-Teilen, Kabeln und Monitoren, auch Gegenstände festgestellt, die in einem Serverraum auf Grund des hohen Brandrisikos nicht aufbewahrt werden sollten, z. B. Kartons und Papier. Da Server und andere Komponenten sehr große Wärmemengen abstrahlen können, ist in Serverräumen dem Brandschutz besonders Rechnung zu tragen, auch durch eine Möblierung aus feuerhemmendem Material. Des Weiteren muss ein striktes Rauchverbot verfügt und die Lagerung von brennbaren Stoffen unterbunden werden. Beides war während der Kontrolle in der BFD Südwest nicht gewährleistet.

Des Weiteren fanden sich im Serverraum verschiedene Datenträger, z.B. DVD mit aufgezeichneten TV-Sendungen über die BFD Südwest. Der Zugang zum Serverraum sollte nur so wenigen berechtigten Personen wie erforderlich gestattet werden. Die Lagerung von Archivmaterial unterläuft diese Forderung.

Meine Mitarbeiter haben angeregt, die brennbaren Stoffe aus dem Serverraum zu entfernen und alle beschriebenen oder unbeschriebenen Datenträger sicher an einem anderen Ort zu lagern.

4.2 Alte Datenträger und Festplatten

In drei verschiedenen Räumen haben meine Mitarbeiter defekte Festplatten vorgefunden, die planlos gelagert waren. So fanden sich z.B. im Vorraum zum Serverraum in einem alten Karton unsortiert defekte Festplatten, alte CD, DVD sowie Datenbänder. Eine geordnete Verwaltung und eine frist- und fachgerechte Entsorgung von zu vernichtenden Datenträgern kann so in der BFD Südwest nicht sichergestellt werden.



Sie haben u.a. darauf aufmerksam gemacht, defekte Festplatten durch Kopieren der Seriennummer zu dokumentieren und bis zur Vernichtung, die nach DIN 66399 Schutzklasse 3 Sicherheitsstufe 4 durchgeführt werden sollte, zentral zu sammeln und sicher aufzubewahren. Datenträger, für die in der BFD Südwest kein Laufwerk mehr zur Verfügung steht (Bänder), sollten unverzüglich vernichtet werden.

Vor dem Hintergrund dieser Feststellungen rege ich an, die Erstellung eines Konzeptes zur Datenträgervernichtung in der BFD Südwest zu prüfen.

4.3 Löschprogramm für Notebooks

Im Personalbereich sind auch Notebooks im Einsatz, die allerdings über kein physikalisches Löschprogramm verfügen. Wie festgestellt, erfolgt das Löschen von lokal gespeicherten Dateien über die normale Windows-Funktion. Vor dem Hintergrund, dass die Notebooks in der Dienststelle zirkulieren und ein Verlust durch Diebstahl nicht auszuschließen ist, haben meine Mitarbeiter angeregt, ein geeignetes Löschprogramm zu installieren. Zusätzlich sollte geprüft werden, wie bei den Laptops eine Grundverschlüsselung der Festplatte erreicht werden kann, um die Datensicherheit weiter zu erhöhen.

4.4 Verschlüsselungssoftware

Während des Besuches hat die BFD Südwest meinen Mitarbeitern eine Unterlage zur Prüfung übergeben, in dem der Einsatz der Verschlüsselungssoftware Chiasmus als zu umständlich beschrieben und deshalb der Einsatz anderer Verfahren, beispielsweise Zip-Archiv, angeregt wird.

Nach meiner datenschutzrechtlichen Bewertung bieten die dort beschriebenen Programme keine ausreichende Sicherheit nach § 9 BDSG bzw. der Anlage zu § 9 Satz 1 BDSG.

Der Einsatz von Verschlüsselungssoftware ist an besonders schützenswerte Daten gekoppelt (§ 3 Absatz 9 BDSG) und sollte deshalb nicht durch den Einsatz minderwertiger Verschlüsselungssoftware oder gar Software, die keine Verschlüsselung darstellt (Zip-Archiv), ausgehöhlt werden. Ich rege zunächst an, die Schulungsmaßnahmen gerade für das Produkt Chiasmus zu erweitern und andere geprüfte Produkte vorzuschlagen, sowie das BSI zu beteiligen. Für die Beratung bzw. Schulung von Mitarbeitern beim Einsatz von Verschlüsselungssoftware steht Ihnen gerne auch das Referat 23 meines Hauses zur Verfügung.



Die Leitung der BFD Südwest hat hinsichtlich der festgestellten technisch-organisatorischen Mängel bereits vor Ort meinen Mitarbeitern zugesagt, diese unverzüglich abzustellen und umgehend erste geeignete Maßnahmen zur Gewährleistung des Datenschutzes getroffen. Ich gehe somit davon aus, dass die Beseitigung dieser technischen Mängel zwischenzeitlich erfolgt ist und ich nach § 25 Absatz 2 BDSG auf eine förmliche Beanstandung verzichten kann.

Ich wäre Ihnen dankbar, wenn Sie mich über das Ergebnis der empfohlenen Prüfungen und die Umsetzung der Zusagen informieren könnten.

III. Zusammenfassende datenschutzrechtliche Bewertung der Prüfung

Beanstanden muss ich die bei dem Beratungs- und Kontrollbesuch in der BFD Südwest (wie bereits in der BFD Nord) erneut festgestellten zahlreichen, teils erheblichen datenschutzrechtliche Mängel beim Umgang mit sensiblen personenbezogenen Daten (Personal- und Personalaktendaten). Dies betrifft sowohl die automatisierte Personaldatenverarbeitung, insbesondere den sonstigen automatisierten Umgang mit Personal-/Personalaktendaten außerhalb von PVS, als auch den unzulässigen manuellen Umgang mit Beschäftigtendaten.

Ich begrüße, dass die BFD Südwest meine Mitarbeiter bereits während des Kontrollbesuches schriftlich über umgehend veranlasste Maßnahmen (u.a. erstes Löschen von unzulässig gespeicherten Beschäftigtendaten) informiert und Zusagen gegeben hat, künftig einen datenschutzkonformen Umgang mit den Beschäftigtendaten gewährleisten zu wollen. Hinsichtlich vieler Feststellungen, insbesondere bei den erneut festgestellten Mängeln, sehe ich allerdings auch grundsätzlichen Handlungsbedarf des BMF für den Geschäftsbereich. Ich wäre Ihnen dankbar, wenn Sie meine Empfehlungen aufgreifen könnten, um generell eine datenschutzgerechte Verfahrensweise im Umgang mit Personal-/Personalaktendaten der Beschäftigten in der BFV sicherzustellen.

Für Ihre Stellungnahme zu der ausgesprochenen Beanstandung, den noch offenen Punkten und für die Darstellung der getroffenen Maßnahmen bis zum

1. Juli 2017

wäre ich dankbar.



Für eine weitere datenschutzrechtliche Beratung stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen

Andrea Voßhoff