



Die Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

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

[REDACTED]  
Bundesstelle für Flugunfall-  
untersuchung

[REDACTED]  
Hermann-Blenk-Straße 16  
38108 Braunschweig

nachrichtlich:  
Bundesstelle für Flugunfall-  
untersuchung

[REDACTED]  
Hermann-Blenk-Straße 16  
38108 Braunschweig

nachrichtlich:  
Bundesministerium für Verkehr und digitale Infrastruktur

[REDACTED]  
Robert-Schuman-Platz 1  
53175 Bonn

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

[REDACTED]  
INTERNET [www.datenschutz.bund.de](http://www.datenschutz.bund.de)

DATUM Bonn, 18.08.2017

GESCHÄFTSZ. 21-506-5/020#0027

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

BETREFF **Datenschutzrechtliche Beratung und Kontrolle der Bundesstelle für Flugunfall-  
untersuchung (BFU) gemäß §§ 24 Abs. 1 und 26 Abs. 3 Bundesdatenschutzge-  
setz (BDSG)**

HIER Beratungs- und Kontrollbesuch am 19. und 20. April 2017

BEZUG Mein Ankündigungsschreiben vom 13. März 2017 - 21-506-5/020#0027 -

Sehr geehrter [REDACTED]

am 19. und 20. April 2017 haben meine Mitarbeiter [REDACTED]  
in Ihrem Haus einen Beratungs- und Kontrollbesuch durchgeführt. Während des Be-



suchs standen meinen Mitarbeitern von Ihrer Seite [REDACTED]

[REDACTED] sowie Sie persönlich als Ansprechpartner zur Verfügung. Für die gewissenhafte Vorbereitung des Besuchs, die vor Ort gewährte Unterstützung sowie die offene und konstruktive Gesprächsatmosphäre darf ich mich bedanken.

Gegenstand des Besuchs war die Erörterung datenschutzrechtlicher Aspekte im Zusammenhang mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die BFU nach dem Gesetz über die Untersuchung von Unfällen und Störungen bei dem Betrieb ziviler Luftfahrzeuge (Flugunfall-Untersuchungs-Gesetz – FIUUG) nebst ergänzenden nationalen bzw. internationalen Regelungen.

Im Rahmen des Besuchs haben Sie sowie Ihre Mitarbeiterinnen und Mitarbeiter die Arbeitsweise der BFU sehr anschaulich dargestellt. Die Nachvollziehbarkeit der Aufgabenerledigung der BFU unter datenschutzrechtlichen Gesichtspunkten wurde durch die Vorlage von einschlägigen Unterlagen wesentlich erleichtert. Hier sind insbesondere das Datenschutzkonzept nebst Dienstanweisung (Stand jeweils Mai 2015), der aktuelle 1. Jahresdatenschutzbericht 2014 – 2016, die Leitlinie zur Informationssicherheit (Stand August 2012) nebst ergänzenden Sicherheitsrichtlinien (z.B. Internetnutzung, IT-Nutzung, Telearbeit und Mobiles Arbeiten, VPN-Nutzung u.a.), Schutzkonzepte (z.B. Virengefahr) sowie weiteren Dienstanweisungen (z.B. Gästeliste und WLAN-Zugang) zu nennen. Weiterhin standen zur Durchsicht mehrere Ordner mit Untersuchungsvorgängen sowie darüber hinaus mehrere durch meine Mitarbeiter zufällig ausgewählte Sachakten aus verschiedenen Jahrgängen zur Verfügung. Die Möglichkeit zur Einsichtnahme in elektronische Vorgänge war im Besprechungsraum über Beamer-Präsentation sowie in der 24/7/365-Leitstelle und in Einzelbüros an Bildschirmarbeitsplätzen gegeben. [REDACTED] konnten sich persönlich von einer insgesamt klaren Organisationsstruktur sowie einer durchgängig geordneten Aktenführung sowohl in Papier- als auch in elektronischer Form überzeugen. Dabei gelten die angesprochenen Richtlinien, Anweisungen u.ä. nicht nur für die unmittelbar Beschäftigten bei der BFU, sondern richten sich auch an die externen Beauftragten für zeitnahe Beweissicherungen bei Vorortuntersuchungen sowie die 130 Beauftragten an Verkehrsflughäfen zur Unterstützung der BFU-Unfalluntersucher. Gleiches gilt für den Einsatz externer Kräfte zur Aufrechterhaltung des 24/7/365 Bereitschaftsdienstes.



SEITE 3 VON 7 Im Einzelnen möchte ich auf folgende Themen näher eingehen:

## 1. Stellung und Einbindung der behördlichen Beauftragten

Die Aufgaben als [REDACTED] in zugleichfunktion mit seinen Aufgaben als Untersuchungsführer (U 15) ausgeführt. Dabei wurde bislang weder eine Vertretungsregelung noch eine gesonderte Freistellungsregelung zwischen der Behördenleitung und dem bDSB getroffen. Die sehr spezifischen Aufgabenstellungen als Untersuchungsführer sowie die damit verbundenen unvorhersehbaren Einsatzzeiten der Mitarbeiterinnen und Mitarbeiter dürfen nicht dazu führen, dass [REDACTED] seine Aufgaben als bDSB nicht in der gebotenen Weise ausüben kann. Es muss sichergestellt sein, dass der bDSB autonom darüber entscheiden kann, wann die Funktion als bDSB Vorrang hat. Diese aus der Weisungsfreiheit gem. § 4f Abs. 3 Satz 2 BDSG resultierende Entscheidungsfreiheit des bDSB darf nicht dadurch unterlaufen werden, dass die sonstigen dienstlichen Aufgaben einen Umfang annehmen, der die Ausübung der Funktion als bDSB faktisch unmöglich macht. Es ist daher unabdingbar, dem bDSB gem. § 4f Abs. 5 BDSG Hilfspersonal bereitzustellen, das eine angemessene Vertretung bei Verhinderung des bDSB ermöglicht. Zudem bedarf es der Festlegung einer prozentualen Freistellung des bDSB von seinen sonstigen Aufgaben, um hier für beide Seiten mehr Rechtssicherheit zu schaffen.

Während die organisatorische Einbindung des bDSB den gesetzlichen Vorgaben nach § 4f Absatz 3 Satz 1 und 2 BDSG entspricht, konnte ich eine entsprechende Darstellung und formelle Einbindung der Funktion der IT-Sicherheitsbeauftragten nicht erkennen. Nach dem Umsetzungsplan Bund (UP-Bund) sowie entsprechend dem BSI-Standard 100-2 besteht eine allgemeine Organisationspflicht zur Einrichtung und Bestellung der unabhängigen Funktion des IT-Sicherheitsbeauftragten. Meine Mitarbeiter konnten sich im Gespräch mit Ihrer IT-Sicherheitsbeauftragten, [REDACTED] von einem tatsächlich vorhandenen Informationssicherheitsmanagement (ISMS) überzeugen. Insoweit rege ich an, den Organisationsplan sowie ggf. weitere einschlägige Dokumente entsprechend zu ergänzen bzw. anzupassen.

## 2. Besuchermanagement

Besucher der BFU gelangen nur durch persönliche Abholung in den Eingangsbereich der Bundesstelle. Dort erfolgt eine persönliche Ausweisung durch Dienstausweis und



schriftliche Erfassung der Namen und Dienststellen der Besucher. Jeder Besucher erhält einen anonymen Besucherausweis, der während des Aufenthalts dauerhaft zu tragen ist. Die Hinterlegung oder Ablichtung des Ausweises ist dazu nicht erforderlich, was ich begrüße.

### **3. Personenbezogene Daten in Untersuchungsakten**

Es liegt in der Natur der Sache, dass bei Flugunfalluntersuchungen in der zivilen Luftfahrt in nicht unerheblichem Maße personenbezogene Daten nach dem BDSG erhoben werden. Bei der Einsichtnahme in die vorgelegten Unfallakten wurde deutlich, dass es sich hierbei oftmals um Gesundheitsdaten handelt. Als besondere Arten personenbezogener Daten nach § 3 Absatz 9 BDSG unterliegen diese einem besonderen Schutzbedarf. In den Gesprächen mit meinen Mitarbeitern haben Sie dargelegt, dass eine strukturierte und teilweise auch mit eingeschränkten Zugriffen praktizierte Arbeitsweise im Umgang mit den genannten sensiblen Daten durchgängig eingehalten wird. Diese Feststellung gilt gleichermaßen für den Umgang mit Papierakten als auch mit elektronischen Daten. So begrüße ich es ausdrücklich, dass sich die Zugriffsrechte individuell auf den jeweils zuständigen Personenkreis beschränken, ein verpflichtendes Verfahren zur Behandlung von Papierakten über Postfächer auch im Vertretungsfall geregelt ist und der Austausch von medizinischen Daten und Befunden in versiegelten Verschlussmappen erfolgt bzw. Dateien neben den eingeschränkten Zugriffsrechten nochmals passwortgeschützt in den Verfahrensakten abgelegt werden. Für den theoretischen Fall von gleichzeitigen Einsätzen in Vertretungssituationen rege ich jedoch den Einsatz von verschließbaren Postfächern an. Damit kann dem besonderen Schutzbedarf sensibler Daten nach § 3 Absatz 9 BDSG noch besser Rechnung getragen werden.

Bei der Besichtigung der Archivräume habe ich festgestellt, dass die Sicherung des Zugangs durch ein stabiles Vorhängeschloss erfolgt. Dieses Schloss ist allerdings als Zahlenschloss ausgeführt, welches keine besonders große Zugangshürde darstellt. Der Archivbereich sollte mit einem schlüsselbasierten Zugangsschutz versehen werden, um damit den Zugang noch wirksamer zu erschweren.

### **4. Erhebung, Verarbeitung und Nutzung von Daten nach dem FIUUG sowie internationalen Rechtsgrundlagen**

Bei dem Besuch in Ihrem Haus konnten sich meine Mitarbeiter über die Erhebung,



Verarbeitung und Nutzung von Daten nach dem FIUUG, der Luftverkehrs-Ordnung (LuftVO), der Verordnung (EU) Nr. 996/2010 des europäischen Parlaments und des Rates vom 20. Oktober 2010 nebst weiteren Verordnungen sowie dem Chicagoer Abkommen aus dem Jahr 1957 (ICAO Annex 13) umfassend informieren. Neben der unter Punkt 3 genannten internen Erhebung und Verarbeitung von Daten bestehen nach den genannten Vorschriften umfassende internationale Meldepflichten für Vorfälle in der zivilen Luftfahrt, die der künftigen Vermeidung von Unfällen und Störungen sowie der Verbesserung der Flugsicherheit dienen. Im Rahmen des Besuchs wurde exemplarisch die Datenerhebung und Verarbeitung beim ECCAIRS-Verfahren sowie bei der Vergabe einer Ident-Nummer für die der BFU gemeldeten Ereignisse (Tagebuch) näher betrachtet.

Der Wirkeinsatz des ECCAIRS-Verfahrens basiert auf einem Konzept der BFU aus dem Jahr 2010. Das detailliert dokumentierte und im Rahmen des Besuchs näher erläuterte Verfahren dient ganz überwiegend international durchzuführenden statistischen Erhebungen.

Ich begrüße die dabei festzustellende restriktive Nutzung personenbezogener Daten und die konsequente Einhaltung des Grundsatzes der Datensparsamkeit.

## **5. Verfahrensverzeichnis**

Das Verfahrensverzeichnis der BFU stand im Rahmen des Besuchs in Papierform zur Einsichtnahme bereit. Bei der Durchsicht mussten meine Mitarbeiter feststellen, dass einige Beschreibungen nicht vollständig bzw. mit handschriftlichen Ergänzungen und Notizen versehen waren. Eine Stichprobe ergab, dass z.B. das Verfahrensverzeichnis hinsichtlich der Administration des Active Directory nicht ordnungsgemäß geführt ist. Ich bitte diesbezüglich um die erforderlichen Ergänzungen des Verfahrensverzeichnisses und Vorlage eines geeigneten Nachweises darüber.

## **6. Informationssicherheit**

Bei der Durchsicht der Leitlinien, Richtlinien, Konzepte und Dienstanweisungen ist aufgefallen, dass sich das Notfallkonzept aus Juli 2011 offensichtlich noch im Entwurfsstadium befindet und wohl bislang nicht verabschiedet wurde. Insbesondere vor dem Hintergrund, eine ständige Erreichbarkeit in einem 24/7/365-Betrieb sicherstellen zu müssen, halte ich es für unabdingbar, dass ein dem BSI-Standard 100-4 ent-



sprechendes Notfallmanagement festgeschrieben und etabliert wird. Ich rege an, dies im Rahmen der von Ihnen zeitnah vorgesehenen Organisationsuntersuchung zu berücksichtigen.

## **7. Maßnahmen zur weiteren Erhöhung der Sicherheit**

Wie in dem Jahresdatenschutzbericht 2014 – 2016 Ihres bDSB unter Punkt 9 dargelegt und von diesem im persönlichen Gespräch näher erläutert, haben Sie bereits für die Jahre 2017 und 2018 Handlungs- und Optimierungsbedarf zu einer weiteren Erhöhung der Sicherheit in Datenschutz- und Informationssicherheitsfragen identifiziert. Ich begrüße ausdrücklich die dort genannten Maßnahmen. Zu den bereits erfolgten Umsetzungen bzw. weiteren geplanten Maßnahmen bitte ich mich zu gegebener Zeit zu informieren.

## **8. Fazit**

Im Ergebnis fasse ich meine Feststellungen wie folgt zusammen:

Im Rahmen meines Beratungs- und Kontrollbesuchs habe ich bei der Stellung und Einbindung der behördlichen Datenschutz- und IT-Sicherheitsbeauftragten (Ausführungen zu Ziffer 1. des Berichts) Handlungsbedarf identifiziert. Dies gilt auch für organisatorische Fragen im Umgang mit der Aktenbehandlung in den Postfächern sowie den Archivräumen (siehe Ziffer 3. des Berichts). Zudem halte ich es, wie unter den vorstehenden Ziffern 5 und 6 näher ausgeführt, für erforderlich, dass die notwendigen Dokumentationspflichten zum Verfahrensverzeichnis sowie zu dem Notfallkonzept umgesetzt und festgeschrieben werden.

Zu den Feststellungen des Prüfberichts bitte ich innerhalb von acht Wochen Stellung zu nehmen.

Mit freundlichen Grüßen  
Im Auftrag





Die Bundesbeauftragte  
für den Datenschutz und  
die Informationsfreiheit

SEITE 7 VON 7 Dieses Dokument wurde elektronisch versandt und ist nur im Entwurf gezeichnet.