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

Präsidenten des
Bundesinstituts für Risikobewertung
Herrn Professor Dr. Dr. Hensel
Postfach 12 69 42
D - 10609 Berlin

nachrichtlich:

Bundesministerium für Ernährung
und Landwirtschaft
Behördliche Datenschutzbeauftragte
Frau
Rochusstraße 1
D - 53123 Bonn

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

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL ref4@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 09.05.2016
GESCHÄFTSZ. **IV-502/032#0100**

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

BETREFF **Informations-, Beratungs- und Kontrollbesuch im Bundesinstitut für Risikobewertung am 23. und 24. November 2015**

Sehr geehrter Herr Professor Hensel,

gemäß §§ 24, 26 Bundesdatenschutzgesetz (BDSG) haben meine Mitarbeiter RD Kolb, OAR Kühn und ORR Dr. Kiometzis (zeitweilig) am 23. und 24.11.2015 einen datenschutzrechtlichen Informations-, Beratungs- und Kontrollbesuch am Standort Berlin (Max-Dohrn-Straße 8-10) des Bundesinstituts für Risikobewertung (BfR) durchgeführt.

Gegenstand des Besuchs war die Erörterung datenschutzrechtlicher Aspekte im Zusammenhang mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch das BfR und hiermit zusammenhängender Fragen der Datensicherheit. Beispielhaft für die Forschungstätigkeit des BfR wurde meinen Mitarbeitern das Projekt Kinder-Ernährungsstudie zur Erfassung des Lebensmittelverzehrs (KiESEL) vorgestellt.

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Gesprächspartner meiner Mitarbeiter waren Frau , Frau , die zurzeit vertretungsweise die Funktion der behördlichen Datenschutzbeauftragten Ihres Hauses wahrnimmt, Frau , Herr , Herr und Herr .

Für die gewissenhafte Vorbereitung des Besuchs, die vor Ort gewährte Unterstützung und eine offene und konstruktive Gesprächshaltung seitens Ihrer Mitarbeiterinnen und Mitarbeiter möchte ich mich bedanken.

In meinem Ankündigungsschreiben vom 28.10.2015 hatte ich darauf hingewiesen, dass ein Schwerpunkt des Kontrollbesuchs den Umgang des BfR mit personenbezogenen Daten im Rahmen von Forschungsprojekten betrifft. Wie sich anlässlich der insbesondere mit Frau und Frau geführten Gespräche zum Aufgabenprofil des BfR herausstellte, so erhebt, verarbeitet und nutzt das BfR bei seiner Forschungstätigkeit nur in begrenztem Umfang personenbezogene Daten.

Die Gespräche offenbarten eine gewisse Unsicherheit hinsichtlich der Benennung von Arbeitsbereichen und Projekten, in denen personenbezogene Daten eine Rolle spielen. Dieser Eindruck wurde bestätigt durch die Einsichtnahme in Arbeitsunterlagen der behördlichen Datenschutzbeauftragten, Frau . Danach ist von ihr eine Bestandsaufnahme vorbereitet worden, in welchen Arbeitsbereichen des Hauses personenbezogene Daten verarbeitet und genutzt werden. Dies soll im Wege einer Hausabfrage ermittelt werden, die aber bislang noch nicht abgeschlossen worden ist.

Im Einzelnen möchte ich auf folgende Themen näher eingehen:

1. Stellung und Einbindung der behördlichen Datenschutzbeauftragten

Die Aufgaben als behördliche Datenschutzbeauftragte wurden bisher durch Frau in Zugleichfunktion mit anderen Aufgaben innerhalb des Referates „Organisation“ wahrgenommen.
Der Aufgabenbereich ist seit kurzem vertretungsweise von Frau übernommen worden, die ebenfalls einer weiteren Tätigkeit innerhalb des Organisationsreferates nachgeht. Eine zeitlich definierte Aufteilung der beiden Aufgabenbereiche ist nicht erkennbar.

Frau erhält nach ihrer Darstellung die für die Wahrnehmung der Aufgaben als behördliche Datenschutzbeauftragte notwendige Unterstützung durch die Hausleitung des BfR. Dabei ist allerdings zu berücksichtigen, dass sie zum Zeitpunkt des Besuchs erst recht kurze Zeit im Amt war und insoweit noch nicht über konkrete Erfahrungen berichten konnte. Über die Bereitstellung einer angemes-

senen räumlichen und sachlichen Ausstattung, die z. B. auch eine ungestörte Beratung zulässt, konnten sich meine Mitarbeiter überzeugen. Die Teilnahme an für den Nachweis der Fachkunde erforderlichen Weiterbildungsmaßnahmen wird ihr ermöglicht.

Die organisatorische Einbindung der behördlichen Datenschutzbeauftragten unmittelbar unterhalb der Dienststellenleitung, wie sie Ihrem Organisationsplan zu entnehmen ist, entspricht den gesetzlichen Vorgaben (§ 4f Absatz 3 Satz 1 und 2 BDSG). Demgegenüber weist der Geschäftsverteilungsplan diese Funktion nicht als eigenständigen Aufgabenbereich aus. Die Aufgaben der behördlichen Datenschutzbeauftragten sind dort auch nicht in einem anderen Zusammenhang wiedergegeben. Ich gehe davon aus, dass es sich hierbei um ein redaktionelles Versehen handelt. Im Interesse sowohl des Stellenwerts der Funktion der behördlichen Datenschutzbeauftragten für die gesamte Organisation als auch der derzeitigen Funktionsträgerin bitte ich, den Geschäftsverteilungsplan insoweit anzupassen.

Bei dieser Gelegenheit empfehle ich, den zeitlichen Mindestumfang für die Wahrnehmung der Aufgaben der behördlichen Datenschutzbeauftragten festzuschreiben und eine feste Vertretung zu benennen. Allein unter Berücksichtigung der Mitarbeiterzahl des BfR von über 700 Beschäftigten dürften diese Aufgaben eine Vollzeittätigkeit ausfüllen. Eine genauere Festlegung des Zeitumfangs der Wahrnehmung der Aufgaben als behördliche Datenschutzbeauftragte im BfR wird sicherlich das Ergebnis der bereits erwähnten Bestandsaufnahme zu den datenschutzrelevanten Tätigkeiten im BfR ermöglichen. Schon aus diesem Grund bitte ich um eine Durchführung und Auswertung dieser Erhebung. Über das Ergebnis bitte ich mich zu unterrichten. Unabhängig davon, welcher Zeitanteil für die Durchführung der Aufgaben als behördliche Datenschutzbeauftragte in Ihrem Institut als sachgerecht erachtet wird, weise ich darauf hin, dass die Tätigkeit als behördliche Datenschutzbeauftragte grundsätzlich Vorrang vor der Wahrnehmung anderer Aufgaben hat.

Im Zusammenhang mit der Ankündigung des Besuchs ist meinen Mitarbeitern aufgefallen, dass eine unmittelbare Kontaktaufnahme mit der behördlichen Datenschutzbeauftragten von außen mangels entsprechender Angaben auf der Internetseite des BfR (E-Mail-Adresse und/oder telefonische Durchwahl) nicht möglich ist. Zu den Kernaufgaben der behördlichen Datenschutzbeauftragten gehört es, zu datenschutzrechtlich relevanten Fragestellungen im Kontext der Aufgabenerledigung der Behörde zu beraten und Auskünfte zu erteilen. Um dieser gesetzlichen Aufgabe gerecht werden zu können, müssen Funktion und Person der behördlichen Datenschutzbeauftragten bekannt und jederzeit eine ungehinderte

Kontaktaufnahme mit ihr möglich sein. Dies gilt in gleichem Maße für die eigenen Mitarbeiterinnen und Mitarbeiter wie für Anfragen von außerhalb der Dienststelle, da im Zuge der Aufgabenerfüllung der Behörde auch Persönlichkeitsrechte von Personen außerhalb der eigenen Organisationsstruktur betroffen sein können. Soweit noch nicht geschehen, bitte ich dies durch Aufnahme einer Kontaktadresse der behördlichen Datenschutzbeauftragten auf der Internetseite Ihres Instituts nachzuholen. Die Angabe kann auf eine funktionale E-Mail-Adresse ohne Namensangabe beschränkt bleiben.

In der Gesamtschau haben meine Mitarbeiter den Eindruck gewonnen, dass der Bedeutung und der Funktion der behördlichen Datenschutzbeauftragten innerhalb der organisatorischen und operationalen Abläufe des BfR offenbar noch nicht so entsprochen wird, wie es erforderlich wäre. Dies ließe sich mit einem vergleichsweise geringen Aufwand verbessern. Darüber hinaus rege ich an, einen Besuch bei der behördlichen Datenschutzbeauftragten in den Laufzettel für neu eingestellte Mitarbeiterinnen und Mitarbeiter aufzunehmen, damit diese – je nach Arbeitsbereich – frühzeitig für zentrale datenschutzrechtliche Herausforderungen sensibilisiert werden können. Auch eine routinemäßige Einbindung der behördlichen Datenschutzbeauftragten in regelmäßig durchgeführte, organisationsübergreifende Besprechungen sollte zumindest für diejenigen Themen erwogen werden, bei denen eine datenschutzrechtliche Relevanz nicht von vornherein ausgeschlossen werden kann. Aufgrund ihrer Weisungsungebundenheit obliegt dabei die Entscheidung über den Datenschutzbezug eines Besprechungsthemas der behördlichen Datenschutzbeauftragten, die insoweit rechtzeitig und umfassend zu informieren ist.

Zusammenfassend bitte ich also zu prüfen, ob die Wahrnehmung der Aufgaben des behördlichen Datenschutzes aufgrund der Größe des Instituts nicht eine Vollzeitkraft rechtfertigt. Die amtierende Datenschutzbeauftragte ist namentlich und mit Aufgabenbeschreibung in den Geschäftsverteilungsplan aufzunehmen. Ihre Funktion sollte mit Kontaktdaten – ggfs. ohne Namensnennung – auch auf der Internetseite des BfR wiedergegeben sein, damit sie im BfR bekannt ist und eine ungehinderte Kontaktaufnahme für BfR-Angehörige, aber auch für Außenstehende, jederzeit möglich ist.

2. Besuchermanagement

Besucher des BfR werden durch den Pförtner bei der besuchten Arbeitseinheit angemeldet, die die Abholung an der Pforte sicherstellt. Dort erfolgt eine namentliche Erfassung und es wird ein Besucherausweis ausgegeben. Die Hinterlegung

des Personalausweises ist dazu nicht erforderlich und es wird auch keine Ausweiskopie erstellt, was ich begrüße. Im Gebäude Max-Dohrn-Straße ist keine Videoüberwachung installiert.

3. Datenschutzkonzept

Das BfR verfügt über kein Datenschutzkonzept. Die Erarbeitung und Anwendung eines solchen Konzepts ist jedoch bei einer öffentlichen Stelle des Bundes mit über 700 Beschäftigten unerlässlich. Es dient als maßgebliche Orientierungshilfe für eine datenschutzkonforme Vorgehensweise in der Dienststelle insgesamt und bildet die Arbeitsgrundlage für die Aufgabenerfüllung der behördlichen Datenschutzbeauftragten. Sobald Sie den Entwurf für ein Datenschutzkonzept des BfR erarbeitet haben, darf ich Sie um Übersendung zwecks Prüfung bitten.

4. Bestandsaufnahme Datenschutz im BfR

Wie unter Ziffer 1 angesprochen, hat die behördliche Datenschutzbeauftragte des BfR im November 2011 damit begonnen, eine Bestandsaufnahme der datenschutzrelevanten Tätigkeiten im BfR zu erstellen. Ich bitte um die Übermittlung einer Sachstandsdarstellung über die bis heute eingeleiteten Schritte zur Umsetzung dieser Bestandsaufnahme.

5. Forschungsprojekte

Frau hat meinen Mitarbeitern den Forschungsbereich des BfR vorgestellt.

Anhand des Projektes Kinder-Ernährungsstudie zur Erfassung des Lebensmittelverzehrs (KiESEL) hat sie den Umgang mit personenbezogenen Daten erläutert. Dieses Forschungsprojekt gehört danach zu denjenigen Forschungsvorhaben des BfR, bei denen personenbezogene Daten erhoben werden. In dem hierzu erstellten Verfahrensverzeichnis sind die erforderlichen Datenschutzvorkehrungen dargestellt. Sie erfüllen die datenschutzrechtlichen Erfordernisse und geben keinen Anlass zu Anmerkungen.

6. Vorabkontrolle (§ 4d Abs. 5 BDSG)

Die Einbindung der behördlichen Datenschutzbeauftragten vor Inbetriebnahme von automatisierten Datenverarbeitungsverfahren gemäß § 4d Abs. 5 BDSG erfolgt nach ihrer Darstellung zuverlässig. Diese regelkonforme Sicherstellung der Vorabkontrolle durch die behördliche Datenschutzbeauftragte begrüße ich.

7. IT-Sicherheit

Unter dem Blickwinkel des Umgangs mit personenbezogenen Daten ist mit Herrn in seiner Funktion als IT-Sicherheitsbeauftragter und Herrn als Leiter der Fachgruppe Informationstechnik die Sicherheitsarchitektur des IT-Bereichs des BfR ausführlich erörtert worden. Auf meine Bitte hin haben meine Mitarbeiter in diesem Zusammenhang auch den kurz zuvor veröffentlichten Jahresbericht des Bundesrechnungshofs (BRH) und die darin enthaltenen Bemerkungen aus Prüfungen der IT des BfR in den Jahren 2014 und 2015 zur Sprache gebracht. Die Feststellungen des BRH sind aus der Sicht des Datenschutzes von hoher Relevanz. Zu den vom BRH in seinem Jahresbericht festgestellten IT-Sicherheitsmängeln beim BfR haben sich Ihre Mitarbeiter wie folgt eingelassen:

Die fehlende BSI-Zertifizierung der für den Fernzugriff der Telearbeitsplätze eingesetzten Verschlüsselungstechnik sei dem BfR bekannt gewesen; gleichwohl habe sie aber den fachlichen Anforderungen des BSI entsprochen. Inzwischen seien die zurzeit 43 betroffenen Telearbeitsplätze mit zugelassenen Geräten aufgerüstet. Dies werde auch für künftig neu zu schaffende Telearbeitsplätze sichergestellt.

Die Standortverschlüsselung habe man nach dem Bezug der neuen Liegenschaft in der Max-Dohrn-Straße 8-10 im Jahr 2011 für eine ca. sechsmonatige Testphase aufgrund der anfangs für massenhafte verschlüsselte IP-Telefonie noch nicht ausgelegten BSI-zertifizierten Netzwerkkomponenten abschalten müssen. Dies sei aufgrund der umzugsdingt notwendigen Priorisierung bei der Einführung der neuen Technik nicht anders möglich gewesen. Das Problem sei zwischenzeitlich gelöst.

Die vom BRH angeführten Mängel hinsichtlich des IT-Sicherheitsmanagements – Vervollständigung und Aktualisierung des Sicherheitskonzepts sowie Aufbau einer tragfähigen Sicherheitsorganisation – seien dagegen noch nicht behoben. Die Umsetzung werde durch den für Februar/März 2016 erwarteten zusätzlichen Mitarbeiter prioritär erfolgen. Mit diesem soll auch ein umfangreicher Fragebogen zur IT-Sicherheit im Haus, der im Entwurf vorliegt, abschließend abgestimmt und anschließend eingesetzt werden.

Nach den Feststellungen meiner Mitarbeiter verfügt das BfR nicht über einen IT-Grundschutz, der den Anforderungen des Umsetzungsplans Bund im Rahmen der Cyber-Sicherheitsstrategie für Deutschland entspricht. Eine vollständige Umsetzung der IT-Grundschutz-Anforderungen ist aber aus Datenschutzgründen dringend geboten. Bisher wurden lediglich eine Sicherheitsrichtlinie und Konzepte für einzelne Arbeitsbereiche des BfR erstellt sowie – mit Unterstützung eines externen Dienstleisters – einzelne Schutzmaßnahmen implementiert. Auf dieser Grundlage konnte das BfR etwa für den Austausch von elektronischen Dokumenten mit und den Zugriff auf Datenbanken der European Chemicals Agency (ECHA) ein IT-Sicherheitsaudit der ECHA erfolgreich durchlaufen. Zu begrüßen ist auch die Inanspruchnahme des Beratungsangebots des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in diesem Zusammenhang. Ich empfehle Ihnen jedoch, mit Beratung durch das BSI das notwendige Sicherheitsmanagement im Sinne des Umsetzungsplans Bund jetzt zu vervollständigen.

Mangels einer spezifische Dienstanweisung zur Regelung der Rechte und Pflichten des IT-Sicherheitsbeauftragten erscheinen auch das Aufgabenprofil und die Rolle des amtierenden IT-Sicherheitsbeauftragten nicht im erforderlichen Maße festgelegt. Ansätze dazu lassen sich lediglich einer IT-Sicherheitsleitlinie aus dem Jahr 2008, dem aktuellen Geschäftsverteilungsplan (Stand 13.11.2015) sowie einzelnen Verfahrensregelungen zur IT-Sicherheit entnehmen. Ausweislich des Geschäftsverteilungsplanes ist die Funktion des IT-Sicherheitsbeauftragten als „Stabsstelle IT-Sicherheit" unmittelbar beim Präsidenten angesiedelt. Der hier eingesetzte Mitarbeiter nimmt diese Funktion jedoch nur anteilig neben einem weiteren Aufgabengebiet wahr. Die ebenfalls ausgewiesene „Vertretung" ist nicht namentlich benannt.

Die befragten Mitarbeiter des BfR räumten ein, auf diese Weise den Anforderungen an eine belastbare IT-Sicherheitsorganisation und insbesondere dem Umsetzungsplan Bund nicht im erforderlichen Umfang nachkommen zu können. Zwischenzeitlich habe man daher eine zusätzliche Vollzeitstelle für den IT-Sicherheitsbeauftragten geschaffen, ausgeschrieben und einen geeigneten Bewerber gefunden. Die Stellenbesetzung soll bis März 2016 erfolgen. Diesem Mitarbeiter werde der vollständige Aufbau und die fortlaufende Optimierung des IT-Sicherheitsmanagements obliegen.

Auch unter Berücksichtigung der positiven Ansätze ist das IT-Sicherheitsmanagement des BfR nicht ausreichend. Obwohl die „IT-Sicherheitsleitlinie für das Bundesinstitut für Risikobewertung (BfR)" mit Stand 09.07.2008 feststellt, dass die „Verarbeitung und der Austausch von Fachinformationen und Daten sowie deren Qualität und zeitgerechte Bereitstellung ... für die Erfüllung des gesetz-

lichen Institutsauftrags elementar" und alle „wesentlichen Aufgaben und Prozesse ... ohne IT nicht effizient leistbar" seien, liegt das nach dieser Leitlinie als „Maßnahme" zu erstellende und umzusetzende IT-Sicherheitskonzept auch nach Ablauf von sieben Jahren nach Erlass der Leitlinie noch nicht vor. Im eigenen Interesse der Gewährleistung eines belastbaren und den Anforderungen des Umsetzungsplans Bund genügenden Sicherheitsmanagements für den IT-Betrieb und die dabei verarbeiteten personenbezogenen Daten sollte die Leitung des BfR jetzt vordringlich für den Aufbau dieser wichtigen Rahmenbedingung Sorge tragen. Den Entwurf eines vollständigen IT-Sicherheitskonzepts bitte ich mir vor seiner Implementierung rechtzeitig zuzuleiten. Sollte im Zuge der Erstellung konkreter Beratungsbedarf entstehen, bin ich gerne bereit, Unterstützung zu leisten.

Unabhängig davon behalte ich mir vor, im Rahmen meiner Zuständigkeit insbesondere den Bereich der IT-Sicherheit des BfR in absehbarer Zeit einer erneuten Vor-Ort-Prüfung zu unterziehen.

Über die Umsetzung der im Prüfbericht angesprochenen Maßnahmen zu Verbesserung des Datenschutzes im BfR bitte ich mir zeitnah zu berichten.

Mit freundlichen Grüßen

Andrea Voßhoff