Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

Herrn
Michael Ebeling
[redacted]

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

TELEFON (0228) 997799-317
TELEFAX (0228) 997799-550
E-MAIL ref3@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.datenschutz.bund.de

DATUM Bonn, 15.06.2015
GESCHÄFTSZ. **III-400-4 II#0284**

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

BETREFF **Prüf- und Kontrollberichte bei gesetzlichen Krankenkassen**
BEZUG Ihre Anfrage per E-Mail vom 16.05.2015

Sehr geehrter Herr Ebeling,

Ihrem Antrag nach § 1 Informationsfreiheitsgesetz (IFG) vom 16. Mai 2015, mit dem Sie Auskunft zu den zu datenschutzrechtlichen Prüf- und Kontrollberichten bei den gesetzlichen Krankenkassen oder ihren Dienstleistern im Zusammenhang mit der Einführung/Ausstellung der Elektronischen Gesundheitskarte (eGK) beantragt haben, gebe ich statt. Ich übersende Ihnen daher in der Anlage die entsprechenden Auszüge aus den Kontrollberichten.

Diese Auskunft ergeht gebührenfrei.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

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

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

2. Entwurf 12674/2013

Peter Schaar
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

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

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

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL Ref3@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 21.05.2013
GESCHÄFTSZ. **III-363/001#0747**

An den
Vorstand der
Siemens Betriebskrankenkasse
Herrn Dr.
Postfach 830959
81709 München

nachrichtlich:
Bundesversicherungsamt
Friedrich-Ebert-Allee 38
53113 Bonn

BETREFF **Datenschutzrechtlicher Beratungs- und Kontrollbesuch nach § 81 Abs. 2 SGB X i.V.m. § 24 Abs. 1 BDSG vom 3. bis 5. Juli 2012**

Sehr geehrter Herr Dr.

in der Zeit vom 3. bis 5. Juli 2012 haben meine Mitarbeiter, Herr Oberamtsrat und Frau Verwaltungsangestellte einen Beratungs- und Kontrollbesuch bei der Siemens Betriebskrankenkasse (SBK) durchgeführt. Für die – zunächst – gute Gesprächsatmosphäre und die Unterstützung meiner Mitarbeiter danke ich Ihnen.

Gegenstand meiner Kontrolle war u.a. die Organisation des Datenschutzes bei der Siemens BKK, dessen organisatorischer Aufbau von der Bestellung eines behördlichen Datenschutzbeauftragten nach § 81 Abs. 4 Satz 1 SGB X i. V. m. § 4f BDSG

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

Eine detaillierte Prüfung der Datenverarbeitung im Zusammenhang mit dem vorgestellten Projekt behalte ich mir vor.

6. Die elektronische Gesundheitskarte

Die zuständigen Mitarbeiter in der Hauptverwaltung berichteten, dass zum Kontrollzeitpunkt ca. 500 000 elektronische Gesundheitskarten (eGK) bereits ausgegeben waren und bis Ende 2012 alle Gesundheitskarten ausgegeben sein sollen. Bis zum Kontrollzeitpunkt haben ca. 600 Versicherte die Abgabe eines Lichtbildes verweigert.

Die Frage meiner Mitarbeiter, zu welchem Zweck und zur Erfüllung welcher Aufgabe der Versichertenstatus auf der eGK vermerkt sei, konnte vor Ort nicht beantwortet werden. Allerdings soll nach Ihren Angaben bei einer Statusänderung keine neue eGK ausgestellt werden.

Für eine detaillierte Stellungnahme, insbesondere zur Frage, zu welchem Zweck und zur Erfüllung welcher Aufgabe der Versichertenstatus von der SBK auf der eGK gespeichert wird und aus welchem Grund die SBK dies für Ihre Aufgaben für erforderlich hält, wäre ich dankbar.

7. Aufgabenerledigung durch Dritte und Auftragsdatenverarbeitung

Für verschiedene Dienstleister wurde von der SBK ein Stufenkonzept entwickelt, in dem die Dienstleister in der Stufe 1 – ohne jeglichen Zugriff auf Sozialdaten – bis zur Stufe 5 – Dienstleister mit Zugriff auf Kontaktdaten, Grunddaten und ausführliche Sozialdaten – klassifiziert sind. Da in der Kürze der Zeit während des Kontroll- und Beratungsbesuchs eine detaillierte Prüfung der Aufgabenerledigung durch Dritte nicht möglich war, bleibt diese einer Nachkontrolle vorbehalten.

In Ihrer Stellungnahme bitte ich jedoch auch darauf einzugehen, inwieweit die in § 80 Abs. 2 Satz 4 SGB X vorgesehene regelmäßige datenschutzrechtliche Kontrolle der Vertragspartner der SBK, die mit der Verarbeitung von Sozialdaten beauftragt worden sind, bisher durch die internen Datenschutzbeauftragte wahrgenommen wurde.

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Peter Schaar
Bundesbeauftragter für den Datenschutz
und die Informationsfreiheit

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

Vorsitzenden des Vorstandes
Kaufmännische Krankenkasse - KKH
Herrn [redacted]
30144 Hannover

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

TELEFON (0228) 997799-100
TELEFAX (0228) 997799-550
E-MAIL Ref3@bfdi.bund.de

INTERNET www.datenschutz.bund.de

DATUM Bonn, 12.12.2013

BETREFF **Datenschutzrechtlicher Beratungs- und Kontrollbesuch nach § 81 Absatz 2 SGB X in Verbindung mit §§ 24 bis 26 BDSG**

Sehr geehrter Herr [redacted]

in der Zeit vom 21. bis 24. Oktober 2013 haben meine Mitarbeiter Frau RD'n [redacted], Herr ORR [redacted], Frau OAR'n [redacted] und Frau RI'n [redacted] einen Beratungs- und Kontrollbesuch in Ihrem Haus durchgeführt. Für die freundliche und kooperative Aufnahme meiner Mitarbeiter danke ich Ihnen. Besonders freut mich, dass bereits vor Ort einige vorgetragene Lösungsvorschläge angenommen und direkt umgesetzt wurden.

Bei meinem Besuch habe ich Folgendes festgestellt:

1. IT-gestütztes Bearbeitungsmanagement (Rechte-/Rollenkonzept, Löschkonzept)

In Ihrem Haus werden beinahe alle Aufgaben mit eigenen Mitteln erledigt, dies führt zu einem grundsätzlich hohen Datenschutzniveau.

Jedoch bestehen Probleme bei der Datenlöschung. Ein alle Anwendungen umfassendes Konzept zur Löschung nicht mehr erforderlicher Daten bei der Verarbeitung von Versichertendaten existiert in Ihrer Softwarelandschaft bislang nicht. Lediglich in einigen Fachverfahren in begrenzten Bereichen gibt es Löschverfahren. Eine große Anzahl von Daten bleibt auf unbestimmte Zeit und für eine Vielzahl von Personen

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

III-361/006#1301

Bonn, den 12.12.2013
Bearbeiter: OAR'n
Hausruf:

Betr.: Datenschutzrechtlicher Beratungs- und Kontrollbesuch nach § 81 Absatz 2 SGB X in Verbindung mit §§ 24 bis 26 BDSG

1)

Vermerk

In der Zeit vom 21.10.2013 bis 24.10.2013 führten ORR , OAR'in und RI'in einen Beratungs- und Kontrollbesuch nach § 81 Abs. 2 SGB X in Verbindung mit §§ 24 bis 26 BDSG durch. Beim Besuch des Pflegezentrums hat weiterhin Frau RD'n teilgenommen.
Das Mitglied des Vorstands, Herr , begrüßte die Vertreter des BfDI.
Der Besuch fand in einer kooperativen Atmosphäre statt. Die Gesprächspartner waren offen und erteilten bereitwillig Auskunft. Die Mitarbeiter gewährten umfassend Einblick in die elektronische Vorgangsbearbeitung und in Papierunterlagen (soweit noch vorhanden.)
Es wird keine Beanstandung vorgeschlagen.

I. Allgemeines zur KKH

a) Aufbau und Organisation der KKH
Die Kaufmännische Krankenkasse (KKH) betreut mit gut 4.000 Mitarbeitern ca. 1.8 Millionen Versicherte.
Die KKH ist dezentral organisiert. Die Hauptverwaltung in Hannover mit ca. 800 Mitarbeitern vereinigt alle zentralen Bereiche in sich. Ihre Aufgabe ist die Entwicklung und Optimierung der Geschäftsprozesse. Die operativen Geschäftsvorfälle sind auf wenige beschränkt (z.B. Abschluss der Verträge mit Leistungserbringern im Hilfsmittelbereich).
Unterhalb der Zentrale sind zahlreiche Regional- (13) und Kompetenzzentren (22) auf fachlich verschiedene Bereiche spezialisiert (bspw. Hilfsmittel- und Pflegezentren s.u.). Diese Zentren sind im ganzen Bundesgebiet verteilt.
Der Kontakt mit den Kunden vor Ort findet vor allem in den 110 Servicezentren statt, welche ebenfalls bundesweit verteilt sind.

Gegenwärtig wird in der KKH eine größere Umorganisation vorbereitet. Im Zuge dieser Umorganisation werden eine Reihe von Service-, Regional- und Kompetenzzentren zusammengelegt bzw. geschlossen und Aufgaben weiter zentriert.
Das Auftaktgespräch fand in der Hauptverwaltung der KKH in Hannover statt. Dort waren neben einem der beiden Vorstände, Herrn [redacted] und dem Datenschutzbeauftragten, Herrn [redacted] Vertreter aus verschiedenen Bereichen der Hauptverwaltung (interne Revision, Organisation, Verantwortlicher für Beziehung zu externen Dienstleistern sowie Verantwortliche für die IT-Sicherheit und IT-Anforderungsmanagement) zugegen.

Die Quintessenz des Auftaktgesprächs ist, dass die KKH Tätigkeiten sehr zurückhalten auslagert (Outsourcing) und die meisten Kompetenzen und Ressourcen selbst vorhält. Es gibt punktuelle Kooperationen mit Dienstleistern bspw. Call Center im Bereich Evaluierung, Scanvorgänge bei Krankengeld-Arbeitsunfähigkeit und bei der digitalen Aufbereitung von Bildern für die neue elektronische Gesundheitskarte.
Aus wirtschaftlichen Gründen hat die KKH den Einsatz von Hilfsmittelberatern bis auf wenige, nachvollziehbare Einzelfälle zurückgefahren. Begründet wird dies vor allem damit, dass keine Wirtschaftlichkeitsvorteile festgestellt werden konnten, die andere Krankenkassen wiederholt ins Feld führen.Daneben bestanden Zweifel an der Qualifikation der Hilfsmittelberater.

b.) Einsatz der Informationstechnologie bei der KKH
Die Aufgaben im Bereich Informationstechnologie (IT) werden von der KKH fast vollständig in eigener Verantwortung ohne Einschaltung von Dienstleistern bewältigt. So werden auch die Fachanwendungen der Sachbearbeiter im eigenen Haus entwickelt und betreut. Dasselbe gilt für die Betreuung der Hardware.
Der Einsatz des IT-Programms „iskv 21c", welches bei vielen Krankenkassen verwendet wird, ist nicht geplant. Zudem hat sich die KKH bewusst gegen die Nutzung sogenannter Cloud-Dienste ausgesprochen.
Die Beschäftigten haben Zugriff auf die IT-Anwendungen BVS (Bildschirmunterstützter Versichertenservice, greift auf die Informationen aller Datenbanken zu, in denen die Daten der Versicherten gespeichert werden) und die grafische Benutzeroberfläche KSC (Kundenservicecockpit), welches im Jahre 2007 bei der KKH eingeführt wurde.

Die KKH räumt ein, dass ein umfassendes Konzept zur Löschung nicht mehr erforderlicher Daten in der eigenen Softwarelandschaft nicht existiert. In einigen Fachverfahren in begrenzten Bereichen existieren Löschverfahren, allerdings wird eine große Anzahl von Daten auf unbestimmte Zeit und für eine Vielzahl von Personen einsehbar gespeichert. Die KKH führt diesen Umstand auf das mangelnde Bewusstsein zur Datenlöschung bei der Programmierung der (Grund-)Software zurück. Hierbei ist allerdings zu bemerken, dass diese Programmierung teilweise schon Jahrzehnte zurückliegt und diese Problematik grundsätzlich bei allen gesetzlichen Krankenkassen vorliegt.

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

An den
Vorstand der mhplus Betriebskranken-
kasse
Herrn [redacted]
Franckstraße 8
71636 Ludwigsburg

nachrichtlich:
Bundesversicherungsamt
Friedrich-Ebert-Allee 38
53113 Bonn

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

TELEFON (0228) 997799-313
TELEFAX (0228) 997799-550
E-MAIL ref3@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.datenschutz.bund.de

DATUM Bonn, 31.03.2014
GESCHÄFTSZ. **III-363/071#0809**

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

BETREFF **Datenschutzrechtlicher Beratungs- und Kontrollbesuch nach § 81 Absatz 2 SGB X in Verbindung mit §§ 24 bis 26 BDSG am 16. und 17. Januar 2014**
HIER Bericht der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
BEZUG Beratungs- und Kontrollbesuch am 16. und 17. Januar 2014
Ihre Schreiben vom 4. Februar und 12. März 2014
ANLAGEN -1- Orientierungshilfe DIN 66399

Sehr geehrter Herr [redacted]

in der Zeit vom 16. bis 17. Januar 2014 haben meine Mitarbeiter Herr RD [redacted], Herr ORR [redacted] und Frau RI'n [redacted] einen Beratungs- und Kontrollbesuch in Ihrem Haus durchgeführt. Für die freundliche und kooperative Aufnahme meiner Mitarbeiter danke ich Ihnen. Meinen Mitarbeitern wurde Zugang zu allen gewünschten Informationen und Räumlichkeiten gewährt sowie zu allen Fragen offen Auskunft erteilt.

Bei dem Besuch habe ich Folgendes festgestellt:

1. Private Zusatzversicherungen – Zusammenarbeit mit der Süddeutschen Krankenversicherung -SDK

Ein Schwerpunkt meiner Prüfung war die Vermittlung privater Zusatzversicherungen durch die mhplus nach § 194 Absatz 1a SGB V.

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

2.5. mhplus-App

Die von der mhplus angebotene Applikation (App) für das Mobiltelefon, bietet folgende Funktionalitäten:

- Filialsuche
- Arztsuche (über Jameda)
- eGK Fotoupload
- Berechnung des Body-Mass-Index (BMI)
- Pollenfluginformationen
- ICD10-Schlüssel-Rechercheformular
- Verweis an die SDK
- Einsicht in die auf Twitter veröffentlichte News
- FAQ und Impressum

In den Standortdaten (für die Arzt- und Filialsuche), dem eGK Foto und dem persönlichen BMI sehe ich personenbezogene (Gesundheits-)Daten. Ob weitere personenbezogene Daten (bspw. Telefonnummer) erhoben werden, konnte bei dem Besuch nicht abschließend geklärt werden.
Ich bitte daher um Erläuterung, welche (weiteren) Daten über die App bei den Nutzern erhoben werden. Weiterhin bitte ich um Erklärung, welche Daten an welche (anderen bspw. Jameda) Stellen übermittelt werden. Auch interessiert mich, ob und wie die erhobenen Daten wieder gelöscht werden. Die von Ihnen freundlicherweise nachgereichten Ausschreibungsunterlagen für einen Wartungsvertrag treffen hierzu keine erschöpfenden Aussagen. Für den BMI-Rechner wird lediglich ausgeführt, dass die errechneten Werte in einer Langzeittabelle gespeichert werden können.
Ferner bitte ich um Übersendung des Datenschutzkonzeptes für die App.
Negativ ist mir zudem aufgefallen, dass die App über keine Datenschutzerklärung nach § 33 BDSG und § 13 TMG verfügt.

3. Kompetenzzentrum Krankengeld - AU-Fallmanagement

Der Prüfungsschwerpunkt im Kompetenzzentrum Krankengeld war die Anforderung medizinischer Unterlagen für den MDK. Positiv ist mir hierbei aufgefallen, dass die Standardprozesse eine direkte Übersendung medizinischer Daten durch die Leistungserbringer an den MDK vorsehen. Hierzu wird den Leistungserbringern mit der Anforderung der medizinischen Daten ein an den MDK adressierter Rückumschlag übersandt. Gleichwohl habe ich in den Akten medizinische Daten (Antworten von Arztanfragen) von Versicherten gefunden, über die nur der MDK zulässigerweise verfügen darf. Ihre Beschäftigten führen dies darauf zurück, dass Ärzte und Versicherte die Daten auf eigene Initiative an die mhplus übersenden.
Dies führt dazu, dass die an Sie direkt übersandten medizinischen Daten in Ihrem Dokumentenmanagementsystem (iskv21c) elektronisch erfasst und gespeichert werden. Eine Löschung der einmal gespeicherten Dokumente dort sei nicht möglich.