Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Ministerialdirigent
Michael Heyn
Abteilungsleiter 1

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

Deutsche Rentenversicherung Bund
-Direktorium-
10704 Berlin

nachrichtlich:
Deutsche Rentenversicherung Bund
-Behördliche Datenschutzbeauftragte-
[redacted] o.V.i.A.

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON [redacted]
E-MAIL Referat17@bfdi.bund.de
BEARBEITET VON [redacted]
INTERNET www.bfdi.bund.de
DATUM Bonn, 31.01.2024
GESCHÄFTSZ. 17-351/005#1193

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

BETREFF **Datenschutzrechtlicher Beratungs- und Kontrollbesuch vom 25. - 28. September 2023**
HIER Ergebnis meiner Kontrolle
BEZUG Kontrollankündigung vom 4. September 2023

Sehr geehrte Damen und Herren,

vom 25. – 28. September 2023 habe ich einen Beratungs- und Kontrollbesuch im Reha-Zentrum Ückeritz der Deutschen Rentenversicherung Bund (DRV Bund) durchgeführt.

Gegenstand des Beratungs- und Kontrollbesuchs gemäß Art. 58 Abs. 1 lit. b) Datenschutz-Grundverordnung (DSGVO) waren:

- Rollen- und Berechtigungskonzept im Klinikinformationssystem (KIS)
- Datenschutzrechtliche Anforderungen IT-/Diagnostikgeräte
- Patientenaufnahme
- Einhaltung datenschutzrechtlicher Vorgaben Patientenstation / Sozialberatung
- Patientenarchiv und IT (inkl. Datenträger- und Dokumentenvernichtung)
- Begehung TK- und Serverraum

Weitere Sachverhalte außerhalb des oben genannten Kontrollgegenstandes wurden nicht geprüft.

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

1. Ergebnis meiner Kontrolle:

Die Kontrolle hat keine wesentlichen datenschutzrechtlichen Defizite hinsichtlich des Kontrollgegenstandes ergeben. Insbesondere wurde festgestellt, dass alle Mitarbeitenden der Klinik hinreichend mit den einschlägigen datenschutzrechtlichen Regelungen vertraut waren und dahingehend auch regelmäßig sensibilisiert werden. Hierbei wurden zu den einzelnen Prüfpunkten folgende Feststellungen getroffen:

- Rollen- und Berechtigungskonzept im Klinikinformationssystem

Das Rollen- und Berechtigungskonzept für das Klinikinformationssystem in Version 1.14 vom 03.11.2021 weist einen hohen Reifegrad auf. Insgesamt ist das Konzept geeignet, die spezifischen Rollen im Krankenhausinformationssystem datenschutzgerecht zu gestalten. Die DRV Bund verfügt über ein klinikübergreifendes IT-Sicherheitskonzept, welches den datenschutzrechtlichen Anforderungen entspricht. Eine besondere Spezifikation in Bezug auf das Klinikinformationssystem befindet sich in Erstellung und wird dem BfDI nach Fertigstellung vorgelegt.

- Datenschutzrechtliche Anforderungen IT-/Diagnostikgeräte

IT:
Ich konnte mich an mehreren Computern vergewissern, dass ausreichende technische und organisatorische Maßnahmen getroffen worden sind, die den unberechtigten Zugriff auf personenbezogene Daten verhindern. Beispiele für diese Maßnahmen sind:

- Passwortschutz mit automatischer Sperrung des Zugriffs bei Inaktivität
- Gesperrte Schnittstellen wie USB-Ports und optische Laufwerke
- Eingeschränkte Zugriffe auf Laufwerke
- Anwender verfügen über sehr eingeschränkte Rechte zur Veränderung von Systemeinstellungen und können beispielsweise keine Software installieren

Ich konnte nicht feststellen, dass personenbezogene Daten in Systemen verarbeitet wurden, die nicht dafür vorgesehen sind. Dazu habe ich stichprobenhaft mehrere Mailpostfächer und Gruppenlaufwerke überprüft.

Diagnostikgeräte:
Die vorhandenen Diagnostikgeräte verfügen zwar in Teilen über Schnittstellen (beispielsweise über USB-Ports), jedoch sind diese nicht freigeschaltet, so dass kein Zugriff auf die Hardware erlangt werden kann. Auf den vorhandenen Diagnosegeräten werden

keine medizinischen oder personenbezogenen Daten der Patienten gespeichert, so dass Unbefugte auch bei physischem Besitz der Geräte keinen Zugriff auf sensible Daten erhalten können.

- Patientenaufnahme

Die Patientenpostfächer im Eingangsbereich enthalten keine Klarnamen. Diese sind durch eine Kennziffer pseudonymisiert, was ich begrüße. Zudem sind die Arbeitsplatz-PCs im Empfangsbereich zusätzlich durch eine Sichtschutzfolie gegen die Einsicht Dritter geschützt. Auf den Diagnosegeräten fand keine Speicherung von Patientendaten statt.

- Einhaltung datenschutzrechtlicher Vorgaben Patientenstation

Die Patientenzimmer sind lediglich mit Nummern versehen und erlauben keinen Rückschluss auf personenbezogene Daten, wie z.B. die Namen der Patienten. Die Visite erfolgt diskret in einem separaten Raum.

- Patientenarchiv und IT (inkl. Datenträger- und Dokumentenvernichtung)

Die Archivierung von Akten und Dokumente im Patientenarchiv entspricht den datenschutzrechtlichen Anforderungen. Die Einhaltung der entsprechenden Löschfristen wird anhand einer farblichen Markierung an der Akte (entsprechend dem Kalenderjahr der Vernichtung) sichergestellt. Es wurden keine Akten oder Dokumente vorgefunden, die zum Zeitpunkt der Kontrolle die Löschfrist von 10 Jahren überschritten haben.

- Begehung TK- und Serverraum

Der Zutritt zum TK- und IT-Raum ist nur ausgewählten Mitarbeitenden möglich, so dass ein Zugriff durch unbefugte Dritte auf die IT nicht möglich ist. Die vorhandenen Racks sind abgeschlossen, so dass der physische Zugriff auf die Daten ausgeschlossen ist. Der Raum ist durch seine Lage gegen Umwelteinflüsse wie Hochwasser geschützt und durch eine Brandmeldeanlage wurde das Risiko der Zerstörung von Daten durch ein Feuer begrenzt.

2. Empfehlung

Abschließend möchte ich folgende Praxisempfehlungen aussprechen:

Das Reha-Zentrum Ückeritz bietet auf seinen Flyern und Handreichungen noch die Möglichkeit der Kontaktaufnahme per Fax an. Dieser Umstand erhöht die Gefahr, dass potenzielle Patienten vorab sensible Daten per Fax übermitteln. Ein Faxgerät hat hinsichtlich des Schutzziels Vertraulichkeit das gleiche Sicherheitsniveau wie eine unverschlüsselte E-Mail, die zu Recht als digitales Pendant zur offen einsehbaren Postkarte angesehen wird. Fax-Dienste enthalten in der Regel keinerlei Sicherungsmaßnahmen um die Vertraulichkeit der Daten zu gewährleisten. Insbesondere bei der Übertragung besonderer Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 DSGVO ist die Nutzung von Fax-Diensten unzulässig.

Für den Versand personenbezogener Daten müssen daher alternative, sichere und damit geeignete Verfahren, wie etwa Ende-zu-Ende verschlüsselte E-Mails, sichere Portallösungen oder auch die herkömmliche Post genutzt werden.

Eine dahingehende Abänderung der Printmedien wurde bereits vor Ort zugesagt, was ich ebenfalls begrüße.

3. Hinweis zur Veröffentlichung

Erlauben Sie mir abschließend noch den folgenden Hinweis:
Der BfDI strebt ein modernes Informationsmanagement zwischen Bürger und Staat an, das eine Begegnung auf Augenhöhe ermöglichen soll. In Verfolgung dieses Ziels werden Kontrollberichte und/oder die jeweiligen Bescheide im rechtlich zulässigen Rahmen veröffentlicht. Sofern die kontrollierte Stelle dies wünscht, wird auch deren Stellungnahme veröffentlicht. Sofern der Kontrollbericht und/oder der darauf eventuell folgende Bescheid Namen einzelner natürlicher Personen enthalten, werden diese vor Veröffentlichung geschwärzt. Die Veröffentlichung erfolgt mit Bestandskraft des Bescheids bzw. in Fällen ohne Bescheid ca. einen Monat nach Übersendung des Kontrollberichts.

Sofern Bedenken gegen die geplante Veröffentlichung bestehen, bitte ich, mir diese mitzuteilen.

Über eine eventuelle Pflicht zur Herausgabe nach den Regelungen des Informationsfreiheitsgesetzes des Bundes (IFG) ist im Einzelfall gesondert zu entscheiden.

Mit freundlichen Grüßen
im Auftrag

Michael Heyn