Abgeordnetenhaus BERLIN

Drucksache 18 / 24 893
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Marcel Luthe

vom 07. September 2020 (Eingang beim Abgeordnetenhaus am 10. September 2020)

zum Thema:
Datenschutz und Charité – Erfolgsbilanz der Datenschutzbeauftragten

und **Antwort** vom 29. September 2020 (Eingang beim Abgeordnetenhaus am 29. Sep. 2020)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Der Regierende Bürgermeister von Berlin
Senatskanzlei - Wissenschaft und Forschung -

Herrn Abgeordneten Marcel Luthe

über

den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

A n t w o r t
auf die Schriftliche Anfrage Nr. 18/24 893
vom 07. September 2020
über Datenschutz und Charité – Erfolgsbilanz der Datenschutzbeauftragten

---

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Die Anfrage betrifft Sachverhalte, die der Senat nicht ohne Beiziehung der Charité – Universitätsmedizin Berlin (Charité) beantworten kann. Sie wurde daher um Stellungnahme gebeten.

1a) Im Datenschutzbericht Berlin 2009 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„Erste Prüfungen in vier großen Berliner Krankenhäusern offenbarten erhebliche Gefahren bei der Nutzung von KIS: In einem Krankenhaus bestand die inakzeptable Situation, dass dem gesamten ärztlichen und pflegerischen Personal die Einsicht in die Daten aller Personen möglich war, die seit Einführung des KIS in dem Krankenhaus behandelt wurden. Die Mehrheit der Häuser folgt dem Prinzip, dass der Zugriff auf Patientendaten pauschal allen Ärztinnen und Ärzten, Pflege- und Funktionskräften eingeräumt wird, die in Zukunft wahrscheinlich oder möglicherweise mit der Behandlung der Patientin oder des Patienten zu tun haben könnten (Prinzip des „weißen Kittels“). Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten dagegen, dass ein Zugriff auf Patientendaten grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Patientinnen und Patienten behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die vorgefundenen Zugriffsmöglichkeiten gehen jedoch deutlich über den erforderlichen Umfang hinaus und sind als datenschutzrechtlich unzulässig abzulehnen. Die Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten durch die Krankenhäuser hat sich an der konkreten Behandlungssituation der einzelnen Patientinnen und Patienten und nicht an der administrativen und funktionalen Gliederung des Krankenhauses zu orientieren:

• Der Zugriff auf die Daten ist nach der Erforderlichkeit für die Aufgabenerfüllung der zugreifenden Person zu differenzieren. Dabei ist nach Behandlungsrolle, -ort und -zeit zu unterscheiden.

• Patientinnen und Patienten sind zu jedem Zeitpunkt ihrer Behandlung sowohl fachlich als auch räumlich einer Ärztin oder einem Arzt bzw. einer Gruppe von Ärzten zugeordnet. Nach dieser Zuordnung bestimmen sich die

Schranken für den lesenden wie schreibenden Zugriff auf die Patientendaten. Diese Schranken schließen den Bereitschaftsdienst ein.

• Für das pflegerische Personal bedeutet die Orientierung am Behandlungszusammenhang, dass es grundsätzlich nur die Daten der Patientinnen und Patienten der Station einsehen kann, auf der es eingesetzt ist.

• Ein Notfallzugriff von Ärztinnen und Ärzten auf die Daten aller Patientinnen und Patienten, mit denen sie potenziell in Berührung kommen können, ist zu gewährleisten. Er unterliegt jedoch besonderen Kontrollerfordernissen.

• Der Zugriff auf die Akten entlassener Patientinnen und Patienten ist nach Ablauf eines angemessenen Zeitraums nach Abschluss einer Fallbehandlung nur einem eingeschränkten Personenkreis und nur für bestimmte, gesetzlich zulässige Zwecke oder mit Einverständnis der Patientinnen und Patienten z. B. für die klinische Forschung gestattet.

Darüber hinaus muss die Patientin oder der Patient nachvollziehen können, wer auf ihre oder seine Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Weiterhin ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Zur Erreichung dieser Zwecke hat regelmäßig eine Protokollierung sowohl schreibender als auch lesender Zugriffe auf Patientendaten zu erfolgen. (…)

Unsere Prüfungen haben ergeben, dass in Berliner Krankenhäusern teilweise weit über das für die medizinische Behandlung erforderliche Maß hinaus Zugriffe auf elektronische Patientenakten möglich sind. Dies ist mit datenschutzrechtlichen Vorgaben und der ärztlichen Schweigepflicht unvereinbar. Wir werden mit Nachdruck darauf hinwirken, dass Krankenhausinformationssysteme datenschutzgerecht gestaltet und betrieben werden.

Was ist in Bezug auf die monierten Punkte, insbesondere die festgestellten Verstöße gegen datenschutzrechtliche Vorgaben und die ärztliche Schweigepflicht an der Charité seither geschehen?

Zu 1a):
Sowohl die zitierte Passage, als auch das gesamte Kapitel des Berliner Datenschutzberichtes 2009 beziehen sich nicht explizit auf die Charité sondern auf „vier große Berliner Krankenhäuser“.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 1b):
Aus dem Berliner Datenschutzbericht 2009 und den zitierten Passagen ist kein konkreter Bezug zur Charité ersichtlich. Nachrichtlich kann jedoch mitgeteilt werden, dass bisher keine Ordnungsmaßnahmen gegenüber der Charité verhängt wurden.

2a) Im Datenschutzbericht Berlin 2010 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„Unsere Prüfungen haben gezeigt, dass in vielen Krankenhäusern die elektronischen Patientenakten einem zu weiten Kreis von Beschäftigten zugänglich sind. Wir wirken auf die Krankenhäuser ein, um sie zu einer Einschränkung dieser Zugriffsmöglichkeiten zu bewegen, und arbeiten in einer Arbeitsgruppe der Datenschutzkonferenz an der Etablierung von deutschlandweit geltenden Anforderungen an den Schutz von Patientendaten im Krankenhaus. Jeder, der in einem Krankenhaus behandelt wird, hat ein Anrecht darauf, dass sich nur diejenigen durch Einblick in die Patientenakte über den Gesundheitszustand informieren können, die an der Behandlung und Pflege beteiligt sind. Wer die behandelnden Ärztinnen und Ärzte in der Diagnostik und Therapie unterstützt oder die Abrechnung der erbrachten Leistungen durchführt, darf in die Patientenakte Einblick nehmen, jedoch nur, soweit dies für die jeweilige Tätigkeit erforderlich ist. Wie bereits berichtet, setzen einige Berliner Krankenhäuser ihrem Personal keine hinreichend engen Grenzen für den Zugriff auf Patientenakten. Es war und ist unser Ziel, diese Krankenhäuser dazu zu bewegen, die Grenzen so zu ziehen, dass

die Zugriffsmöglichkeiten im Rahmen des Erforderlichen bleiben. Selbstverständlich muss diese Einschränkung in einer Weise erfolgen, dass die Arbeitsfähigkeit der Ärzteschaft und anderen Beschäftigten nicht behindert oder beschränkt wird. Auf unsere Initiative begannen zwei Krankenhäuser mit besonders deutlichen Defiziten damit, Richtlinien zu erarbeiten, die den Bedarf an Zugriffen auf Patientenakten aus medizinischer Sicht mit klaren Grenzen umschreiben. (...)Krankenhauspersonal, das sich im eigenen Haus behandeln lässt, ist besonderen Risiken ausgesetzt. Auf unsere Initiative erprobt die Charité die Aufnahme von Beschäftigten als Patienten unter falschem Namen, wie dies in anderen Häusern bereits für Prominente praktiziert wird. Wir sind der Ansicht, dass diese Möglichkeit allen interessierten Beschäftigten offenstehen und bekannt sein muss. Auch dürfen ihnen aus der Wahrnehmung dieses Angebots keine zusätzlichen Bürden, etwa in der Abrechnung der für sie erbrachten Leistungen, erwachsen. Krankenhäuser haben festzulegen, in welchem Maße der Zugriff auf Patientendaten für die Behandlung erforderlich ist, und über dieses Maß hinausgehende Zugriffe durch eine Kombination von organisatorischen Maßnahmen und technischen Mitteln zu unterbinden. Um eine unberechtigte Offenbarung feststellen und ahnden zu können, sind die Zugriffe zu protokollieren."

Was ist in Bezug auf die monierten Punkte, insbesondere die fehlende Protokollierung von Zugriffen auf Gesundheitsdaten an der Charité seither geschehen?

Zu 2a):
In den bisherigen Anfragen wurde zu der Frage der Zugriffsprotokollierung und einer Offenlegung an Patientinnen und Patienten bereits abschließend unter Bezugnahme auf die DS-GVO Stellung genommen.

Die Charité hat ansonsten umfangreiche Zugriffsbeschränkungen umgesetzt. Für pflegerisches Personal erfolgte ein Zugriff nur im Behandlungszusammenhang; ein Notfallzugriff von Ärztinnen und Ärzten auf die Daten aller Patientinnen und Patienten ist grundsätzlich gewährleistet, wird indes protokolliert – und darüber hinaus wird nicht nur das „Ob" des Zugriffs, sondern auch das „Warum" des Zugriffs protokolliert.

Die Behandlung unter Pseudonym steht allen Beschäftigten der Charité frei.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 2b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

3a) Im Datenschutzbericht Berlin 2012 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„Manche Krankenhäuser wie die Charité fassen dagegen schon die regulären Berechtigungen so weit, dass mehr als zehnmal so viele Beschäftigte Zugriffsmöglichkeiten haben, als sie tatsächlich benötigen. Da in beiden Konstellationen das Tor zu Daten einer großen Zahl von Patienten auch dort offensteht, wo ihre Kenntnis nicht benötigt wird, muss Missbrauch festgestellt und sanktioniert werden.

Aufgrund eines Hinweises aus der Bevölkerung fanden wir auf dem Gelände einer ehemaligen Klinik in den Kellerräumen der dort leerstehenden Gebäude Aktenordner, die u.a. personenbezogene Unterlagen zu Patienten enthielten. Darunter waren OP-Berichte, gynäkologische Gutachten, die Informationen zu Erwerbsminderungen, Vaterschaften, Kunstfehlern und Geschlechtsumwandlungen enthielten, sowie andere Untersuchungs- und Arztberichte zu Schwangerschaften (z. T. zu Schwangerschaftsverläufen von drogenabhängigen Frauen), Geburten und Aborten. Die stark verwahrlosten Gebäude waren offen zugänglich und wurden offen-

sichtlich von Menschen genutzt. Jedenfalls waren die Aktenordner bewegt worden und lagen z. T. aufgeschlagen auf dem Boden. Soweit uns das bei der Sichtung vor Ort möglich war, stellten wir fest, dass die Unterlagen größtenteils aus den 1960er bis 1990er Jahren stammten. Die Klinik, die 1995 in den Räumlichkeiten ansässig war, existierte als solche nicht mehr. Rechtsnachfolgerin dieser Klinik sowie Rechtsnachfolgerin der Krankenhäuser, die z. T. als aktenführende Stellen aus den Akten hervorgingen, ist die Charité. Nachdem wir den Aktenfund dort mitgeteilt hatten, veranlasste das Krankenhaus unverzüglich die Räumung der Kellerräume und die Vernichtung der Patientenakten. Eine Benachrichtigung der Betroffenen erfolgte nicht. Gerade im Gesundheitsbereich wiederholen sich solche Aktenfunde mit erschreckender Regelmäßigkeit.

Die Charité hatte die Benachrichtigung der Betroffenen aus verschiedenen Gründen abgelehnt. Neben nicht tragfähigen Argumenten (z. B. dass Papierakten keine „Datenträger“ seien) teilte das Krankenhaus mit, dass keine schwerwiegenden Beeinträchtigungen für die Betroffenen drohten, da die Vorgänge z. T. 30 bis 40 Jahre alt und aufgrund des schlechten Aktenzustandes Namen und Wohnorte nur schwer lesbar gewesen seien. Diese Gefahrenprognose wurde von dem Krankenhaus jedoch insbesondere im Hinblick auf Daten zu Drogenabhängigkeiten, Erwerbsminderungen und Geschlechtsumwandlungen nicht ausreichend belegt. Zudem war es problematisch, dass das Krankenhaus sämtliche Patientenunterlagen aus den Kellerräumen vernichtet hatte, obwohl nicht ausgeschlossen werden konnte, dass auch Akten anderer verantwortlicher Stellen betroffen waren. Durch die Vernichtung der Akten war eine Benachrichtigung einzelner Betroffener nicht mehr möglich. Wir haben die Charité auf diese Missstände aufmerksam gemacht und darauf hingewiesen, dass zukünftig vor der Räumung von Standorten der Aktenbestand erfasst werden und nach der Räumung überprüft werden sollte, ob die Akten tatsächlich entfernt wurden. Auch sind Akten nach der Aufbewahrungsfrist erst zu vernichten, wenn feststeht, dass keine Benachrichtigungspflicht besteht. Akten anderer verantwortlicher Stellen dürfen keinesfalls vernichtet, sondern müssen der anderen Stelle übergeben werden. Bei einem Datenverlust muss anhand der Art der Daten, der möglichen Verwendungsszenarien und der Gesamtumstände des Falles eine differenzierte Prognose erstellt werden, ob für die Betroffenen schwerwiegende Beeinträchtigungen drohen.“

Was ist in Bezug auf die monierten Punkte, insbesondere die zu weitreichenden Zugriffsberechtigungen auf Patientendaten an der Charité seither geschehen?

Zu 3a):
Die Charité hat die Vorgaben zu einer datenschutzkonformen Räumung von Standorten hinsichtlich der Vernichtung dort vorhandener personenbezogener Daten entsprechend der Empfehlungen der BlnBDI unmittelbar nach dem Vorfall kurzfristig überarbeitet. Des Weiteren wird auf die Antwort zu Ziffer 2a) verwiesen.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 3b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der BlnBDI keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

4a) Im Datenschutzbericht Berlin 2014 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„Übergabe von Patientendaten an die Labor GmbH ohne Rechtsgrundlage. Mit Beschluss des Abgeordnetenhauses aus dem Jahr 2010 wurde die Labor Berlin-Charité Vivantes GmbH als Tochtergesellschaft der Charité Universitätsklinikum Berlin und der Vivantes Netzwerk für Gesundheit GmbH gegründet. Seit Beginn der Geschäftsaufnahme zum 1. Januar 2011 werden die Laboruntersuchungen von Patienten der Vivantes Netzwerk für Gesundheit GmbH und der Charité Universitätsmedizin Berlin durch die neue Labor GmbH durchgeführt. (…) Zusammen mit der Technik wurden dem neuen Laborunternehmen auch die Daten der vormals bei den beiden Krankenhäusern behandelten Personen übergeben. Diese Datenübermittlung hinter dem Rücken der Patienten stellt einen Verstoß gegen die ärztliche Schweigepflicht und den Datenschutz dar. Wir haben die

Labor GmbH aufgefordert, die Rückübertragung der unrechtmäßig erhobenen und gespeicherten Daten an die Vivantes Netzwerk für Gesundheit GmbH bzw. die Charité Universitätsmedizin Berlin in schriftlichen Vereinbarungen mit den genannten Stellen zu regeln und zu vollziehen."

Was ist in Bezug auf die monierten Punkte, insbesondere die Verstöße gegen die ärztliche Schweigepflicht durch Weitergabe von Patientendaten „hinter dem Rücken der Patienten" an der Charité seither geschehen?

Zu 4a):
Die Frage richtet sich an mehrere Beteiligte. Für die Charité ist auszuführen, dass diese der Aufforderung nachgekommen ist und die Rückübertragung vollzogen hat.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 4b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der BlnBDI keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

5a) Im Datenschutzbericht Berlin 2015 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„Wir haben die Einhaltung der gesetzlichen Vorgaben zur Einführung von neuen IT-Verfahren und Führung eines Verzeichnisses dieser Verfahren bei der Charité geprüft. Dabei mussten wir gravierende Defizite feststellen, die beanstandet wurden." (…) „Die Lücken weisen auf ein wesentlich größeres Problem: Sie deuten darauf hin, dass die Charité teilweise neue Verfahren in ungeregelter Weise einführt. Die vom Gesetzgeber vorgegebene und angesichts der Sensitivität der Daten und Komplexität der Informationstechnik notwendige systematische Vorgehensweise bei der Planung von Sicherheitsmaßnahmen wird nicht eingehalten. Damit steht die Sicherheit der Daten der Patienten und auch der Beschäftigten der Charité in erheblichem Zweifel." (…) „Ein laxes Vorgehen führt zu vermeidbaren und in ihrer Reichweite nicht abschätzbaren Risiken für die Patienten."

Was ist in Bezug auf die monierten Punkte, insbesondere die ungeregelte Einführung und Verwendung neuer IT-Verfahren mit der Folge unsicherer Verarbeitung von Patientendaten an der Charité seither geschehen?

Zu 5a):
Die Charité hat, um dem oben geäußerten Eindruck entgegen zu wirken, ein vollständiges Verzeichnis der (bestehenden) Verarbeitungstätigkeiten vorgelegt und die systematische Einführung und Verwendung neuer IT-Verfahren dokumentiert.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 5b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der BlnBDI keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

6a) Im Datenschutzbericht Berlin 2015 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„2015 mussten wir feststellen, dass die Charité den Überblick über die bei ihr betriebene Datenverarbeitung verloren hatte. Neue Verfahren wurden ungeregelt eingeführt. Die Sicherheit der verarbeiteten sensitiven Daten stand infrage." (…) „Die Zusammenstellung der Informationen dagegen, wie die Verarbeitung erfolgt, blieb selbst bei zentralen Verfahren nur skizzenhaft, obwohl Transparenz Voraussetzung dafür ist, dass sich Kranke, Probandinnen und Probanden, Beschäftigte und Studierende sicher sein können, dass mit ihren Daten rechtmäßig umgegangen wird. Die Verarbeitung von Daten durch die moderne Medizintechnik, die die Charité betreibt, blieb gleich völlig außen vor, womit eine gähnende Lücke bestehen blieb, sowohl in der Gewährleistung des Datenschutzes als auch der Informationssicherheit. In Bezug auf die Sicherheit der Daten musste die Charité bekennen, dass sie für keines der betriebenen Verfahren über ein dem Stand der Technik entsprechendes Sicherheitskonzept verfügt. Mehrere Anläufe zu einer Erarbeitung auch mit externer Unterstützung waren in den vergangenen Jahren im Sande verlaufen." (…) „Patientinnen und Patienten haben nicht die Wahl, auf andere Häuser auszuweichen, in denen möglicherweise dem Datenschutz und der Datensicherheit größere Aufmerksamkeit geschenkt wird. Der daraus resultierenden unabweisbaren Verantwortung kann die Charité nur mit substanziellen neuen Mitteln und dem entschlossenen Willen gerecht werden, die über lange Jahre aufgehäuften Defizite schnellstmöglich abzubauen."

Was ist in Bezug auf die monierten Punkte, insbesondere die „gähnende Lücke" beim Datenschutz und das fehlende Sicherheitskonzept an der Charité seither geschehen?

Zu 6a):
Seit 2015 wurden die Sicherheitskonzepte für die zentrale IT-Infrastruktur der Charité nach IT-Grundschutz erstellt und hierüber laufend der BlnBDI berichtet. Diese wurden durch die in 2019 erfolgreich durchgeführte Prüfung nach § 8a Abs. 1 S. 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) bestätigt.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 6b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der BlnBDI keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

7a) Im Datenschutzbericht Berlin 2017 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

"Das größte Universitätsklinikum Deutschlands bekommt seine vielfältigen Datenverarbeitungen für Zwecke der Krankenbehandlung, Ausbildung und Forschung nicht in den Griff." (...)

"Bei Verfahren, die wir stichprobenartig näher unter die Lupe genommen haben, haben wir selbst in Basisangaben Lücken entdeckt. So waren bei der Beschreibung der Patientenverwaltung Datenflüsse von und zu Einrichtungen wie dem Medizinischen Dienst der Krankenkassen und den Gesundheitsämtern nicht abgebildet. Zu einigen Verarbeitung-gen, auch besonders gefahrenträchtigen wie der Telemedizin, waren nur Überschriften zu finden. Welche einzelnen Vorgänge sich dahinter verbergen, war nicht zu erkennen. Eine zugesagte Übersicht über die Bestandteile weit gefasster Verfahrenskategorien erhielten wir nicht." (...)

"Wir mussten feststellen, dass Risiken zu eng gefasst wurden und die vorgegebenen Maßnahmen selbst diese Risiken nicht ausreichend mindern. Etablierte Vorgehensweisen wurden nicht einbezogen, eine Strukturierung entsprechend gängigen Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik nicht vorgenommen. Prozesse und Verantwortlichkeiten waren unzureichend definiert."(...)

"Im nächsten Schritt wandten wir uns den Medizingeräten zu, um dort die Zuständigkeiten und Vorgaben zum Schutz der Geräte insbesondere gegen unbefugten Zugang zu Wartungsschnittstellen zu prüfen. Wir erfuhren,

dass der Betrieb der Medizingeräte an die Charité Facility Management GmbH (CFM) ausgelagert worden war. Doch war diese Auslagerung nie so, wie durch das Berliner Datenschutzgesetz gefordert, vertraglich geregelt worden." (...)

"Zudem darf die Formulierung im Strafgesetzbuch, nach der Berufsgeheimnisträgerinnen und -träger Geheimnisse an mitwirkende Dritte offenbaren dürfen, nicht darüber hinwegtäuschen, dass nach wie vor die Regelungen des Datenschutzrechts zu beachten sind. Für die Übermittlung von (Gesundheits-)Daten ist also weiterhin eine Befugnis erforderlich (eine gesetzliche Grundlage oder eine Einwilligung) und für die Weitergabe im Rahmen eines Auftragsdatenverarbeitungsverhältnisses der Abschluss eines entsprechenden Vertrages."

Was ist in Bezug auf die monierten Punkte, insbesondere die fehlende vertragliche Regelung zur Auslagerung und die Datenflüsse zum medizinischen Dienst der Krankenkassen und der Gesundheitsämter an der Charité seither geschehen?

Zu 7a):
Die Charité hat die erforderlichen vertraglichen Regelungen zum Betrieb der Medizingeräte mit der Charité Facility Management GmbH (CFM) getroffen. Die Beschreibung der Datenflüsse von und zu Einrichtungen wie dem Medizinischen Dienst der Krankenkassen und den Gesundheitsämtern wurde in den Verarbeitungstätigkeiten des Medizinischen Leistungsmanagement abgebildet.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 7b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der BlnBDI keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

8a) Im Datenschutzbericht Berlin 2018 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„Vor Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 war die Charité verpflichtet, jedes Verfahren zur Verarbeitung von Patienten- oder Probandendaten einer Vorabkontrolle auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu unterziehen. Dieser Verpflichtung ist die Charité in der Vergangenheit nicht nachgekommen. Diese Forderung besteht mit der DS-GVO nunmehr in Form der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung für alle neu eingeführten Verfahren mit hohen Risiken und für die Verfahren fort, für die zuvor trotz Verpflichtung keine regelgerechte Vorabkontrolle durchgeführt wurde. Wir haben im Oktober 2018 geprüft, ob die Defizite aufgearbeitet wurden. Das Ergebnis war ernüchternd: Auch fünf Monate nach Wirksamwerden der DS-GVO hatte die Charité zu keinem Verfahren eine Datenschutz-Folgenabschätzung abgeschlossen. Lediglich bei zwei Verfahren haben die Arbeiten an der Durchführung einer Folgenabschätzung begonnen. Dabei schätzt die Charité selbst, dass sie für mehr als einhundert Verfahren solche Abschätzungen vornehmen muss.“ (…) „Der Charité fehlt es bereits an der systematischen Beschreibung der einzelnen Verfahren. Es gibt einen allgemeinen Risikokatalog, aber keine Konkretisierung für den jeweiligen Verarbeitungsvorgang. Ebenso gibt es einen allgemein gehaltenen und zudem unvollständigen Katalog von zentral anzuwendenden Maßnahmen. Gebraucht werden jedoch spezifische Vorgaben sowohl für den zentralen IT-Betrieb als auch für die Verarbeitungen in dezentraler Verant-

wortung. Ihre Zusammenfassung sollen diese Vorgaben und Maßnahmen dann in den gesetzlich vorgeschriebenen Datenschutzkonzepten finden. Deren Fehlen hat vor drei Jahren zur Beanstandung seitens unserer Behörde geführt. Nach wie vor liegt für kein Verfahren ein solches Konzept vor."

Was ist in Bezug auf die monierten Punkte, insbesondere die fehlenden Folgenabschätzungen an der Charité seither geschehen?

Zu 8a):
Für Datenschutz-Folgenabschätzungen (DSFA gemäß Art. 35 DS-GVO) wurde gemeinsam mit der BlnBDI in einem konstruktiven Dialog eine Muster-DSFA erarbeitet. Die von der Charité zu erstellenden DSFA erfolgen unter Verwendung dieses Musters entsprechend eines mit der BlnBDI abgestimmten zeitlichen und inhaltlichen Plans.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 8b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der BlnBDI keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

9a) Im Datenschutzbericht Berlin 2019 der Berliner Datenschutzbeauftragten wird zur Charité ausgeführt:

„Wir haben geprüft, ob die beiden großen Krankenhaus-Betreiberinnen in Berlin, die Charité und die Vivantes Netzwerk für Gesundheit GmbH, so mit gespeicherten Angaben über die Behandlung bereits entlassener Patientinnen und Patienten umgehen, wie es gesetzlich vorgeschrieben ist, insbesondere, ob sie den Zugriff auf die Daten spätestens ein Jahr nach Abschluss der Behandlung sperren und diese nach Ablauf der Aufbewahrungsfrist löschen. Krankenhäuser haben die Verpflichtung, medizinische Behandlungen zu dokumentieren. Hierbei werden völlig legitim große Mengen sensitiver Daten gespeichert. Diese müssen über einen gesetzlich vorgegebenen Zeitraum zwischen zehn und dreißig Jahren gespeichert bleiben. Innerhalb dieses Zeitraums sollen Zugriffe auf die Daten nach Abschluss der jeweiligen Behandlung nur noch möglich sein, wenn es dafür einen besonderen Bedarf gibt. Dementsprechend müssen die Zugriffsberechtigungen in dieser Zeitspanne stark eingeschränkt werden. Nach Ablauf der Fristen hingegen ist auch eine weitere Aufbewahrung nur noch zulässig, wenn es einen besonderen Grund dafür gibt. In beiden geprüften Krankenhäusern mussten wir feststellen, dass diese Anforderungen nicht erfüllt werden. In der Charité blieben Patientendaten auch nach Entlassung und Abrechnung der Behandlung auf Dauer im Zugriff der überwiegenden Mehrzahl der Beschäftigten, was eine grobe Verletzung der gesetzlichen Vorgaben darstellt. Vivantes schränkte den Zugriff deutlich stärker ein. Die Zugriffsmöglichkeiten waren von vornherein an den Bedürfnissen der Behandlung ausgerichtet. Zudem wurden sie nach dem Ende der Behandlung in den meisten Fällen zeitlich beschränkt. Doch griff diese Beschränkung nicht durchgehend und trat in einigen Fällen zu spät ein. Mit der gesetzlichen Vorgabe konfrontiert, haben beide Häuser unverzüglich Maßnahmen eingeleitet, um die Defizite abzustellen. Die Charité legte einen ambitionierten Plan mit Maßnahmen zur Ertüchtigung oder Auswechslung der geprüften technischen Systeme und Einrichtung der zeitlich definierten Zugriffsbeschränkungen vor. Bereits wenige Monate nach der Prüfung konnte sie vermelden, dass in einem der geprüften Systeme der Schutz der Patientendaten gegen einen unbegründeten Zugriff nunmehr den gesetzlichen Ansprüchen entspricht. Vivantes handelte ebenfalls schnell und legte einen Plan vor, mit dem die existierenden Zugriffsmöglichkeiten justiert und Lücken geschlossen werden sollen. Bei Daten aus der ambulanten Behandlung haben wir geprüft, ob sie nach Ablauf der Aufbewahrungsfrist von regelmäßig zehn Jahren gelöscht werden. Dabei fanden wir Defizite in beiden Häusern vor. Diese müssen jetzt durch eine nachholende Löschung und die Einrichtung regelmäßiger Löschroutinen aufgearbeitet werden. Den Häusern bleibt es dabei unbenommen, Patientinnen und Patienten,

die dies wünschen, auch eine längere Aufbewahrung anzubieten. Wir werden die Mängelbeseitigung bei Charité und Vivantes im Weiteren eng verfolgen und, sollten sich wider Erwarten inakzeptable Verzögerungen ergeben, von unseren Abhilfebefugnissen Gebrauch machen."

Was ist in Bezug auf die monierten Punkte, insbesondere die fehlende Sperrung von Zugriffen auf Patientendaten - und die fehlende Protokollierung dieser Zugriffe, siehe Datenschutzbericht 2009 zu Frage 1a) - an der Charité seither geschehen?

Zu 9a):
Zugriffe innerhalb der Aufbewahrungsfrist werden mit dem zwingend anzugebenden besonderen Grund protokolliert. Das Umsetzungsprojekt wird von der BlnBDI weiter eng verfolgt; es befindet sich nach einer pandemiebedingten leichten Verzögerung in der finalen Phase.

b) Sind bezüglich der Verstöße zu a) Ordnungsmaßnahmen verhängt worden? Falls ja, welche mit welchem konkreten Erfolg? Falls nein, weshalb nicht?

Zu 9b):
Es wurden keine Ordnungsmaßnahmen gegenüber der Charité verhängt. Der Senat kann zu den Ermessenserwägungen der BlnBDI keine Auskunft geben, da die BlnBDI bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig ist, keiner Beeinflussung von außen unterliegt und weisungsungebunden agiert (vgl. § 10 Abs. 2 BlnDSG). Im Übrigen befindet sich die Charité im ständigen Kontakt mit der BlnBDI, um die Verfahren zu verbessern.

10) Sind Verstöße gegen datenschutzrechtliche Schutzvorschriften im Sinne der DSGVO grundsätzlich schadenersatzpflichtig, also sowohl hinsichtlich eines materiellen wie auch immateriellen Schadens?

Zu 10):
Die Frage bezieht sich auf eine rechtliche Auskunft, die nicht vom parlamentarischen Fragerecht umfasst ist.

11) Seit wann ist Frau Janet Fahron schon Datenschutzbeauftragte der Charité?
https://www.charite.de/service/person/person/address_detail/fahron/

Zu 11):
Personenbezogene Fragen werden aus datenschutzrechtlichen Gründen nicht beantwortet.

Berlin, den 29. September 2020

In Vertretung

Steffen Krach

Der Regierende Bürgermeister von Berlin
Senatskanzlei - Wissenschaft und Forschung -