Beglaubigte Abschrift

12 Sa 186/19
4 Ca 6116/18
Arbeitsgericht Düsseldorf

Verkündet am 11.03.2020

Lochthowe
Regierungsbeschäftigte
als Urkundsbeamtin der Geschäftsstelle

LANDESARBEITSGERICHT DÜSSELDORF
IM NAMEN DES VOLKES

URTEIL

In dem Rechtsstreit

N. S., C. dahl 37, T.

Kläger und Berufungskläger

Prozessbevollmächtigte
I. & E. Rechtsanwälte, G.-F.-Str. 75 - 77, T.

g e g e n
N. N. Dienst der Krankenversicherung Nordrhein, vertreten durch die Geschäftsführung, C.Allee 52, E.

Beklagter und Berufungsbeklagter

Prozessbevollmächtigte
Rechtsanwälte N. X., L. straße 61, E.

hat die 12. Kammer des Landesarbeitsgerichts Düsseldorf
auf die mündliche Verhandlung vom 11.03.2020
durch den Vorsitzenden Richter am Landesarbeitsgericht Dr. Gotthardt als Vorsitzenden und den ehrenamtlichen Richter vom Brocke und den ehrenamtlichen Richter Bickhove-Swiderski

für Recht erkannt:

1. **Die Berufung des Klägers gegen das Urteil des Arbeitsgerichts Düsseldorf vom 22.02.2019 – 4 Ca 6116/18 – wird zurückgewiesen.**

2. **Die Kosten des Berufungsverfahrens werden dem Kläger auferlegt.**

3. **Die Revision wird zugelassen.**

…

T A T B E S T A N D:

Die Parteien streiten darüber, ob der Beklagte verpflichtet ist, dem Kläger eine Entschädigung und materiellen Schadensersatz wegen einer vom Kläger angenommenen Verletzung datenschutzrechtlicher Vorschriften und seines Persönlichkeitsrechts zu zahlen.

Der am 10.07.1956 geborene Kläger war seit dem 01.09.1999 bei dem Beklagten, dem N. Dienst der Krankenversicherung Nordrhein, der im Jahr 2018 an acht Standorten insgesamt 1.049 Beschäftigte hatte, tätig und zwar zuletzt im IT-Bereich als Systemadministrator und Mitarbeiter im Helpdesk. Örtlich befand sich der Arbeitsplatz des Klägers in E.. Der Kläger war schwerbehinderter Mensch mit einem GdB von 60. Er verdiente zuletzt monatlich 5.812,00 Euro brutto, wobei sich dieser Betrag zusammensetzte aus dem Bruttogehalt vom 5.446,00 Euro, der Familienzulage von 306,00 Euro und 40,00 Euro vermögenswirksamen Leistungen. Bei dem Beklagten war ein Datenschutzbeauftragter bestellt.

Im Jahr 2018 erstellte der Beklagte für die gesetzlichen Krankenkassen insgesamt 663.467 Gutachten. Die Datenverarbeitung erfolgte durch die Software Ismed3. Hierzu existierte eine Dienstvereinbarung zwischen dem Beklagten und dem Personalrat über den Einsatz von Ismed 3 (im Folgenden DV Ismed 3). In dieser hieß es u.a.:

> „…
> **2. Geltungsbereich**
> Die Dienstvereinbarung gilt für alle Mitarbeiter, die einen Zugang zur Software Ismed 3 haben.
> …
>
> **6. Persönliche Identifikation am System**
> Für den Anmeldevorgang und das Arbeiten mit Ismed 3 wird ein Softwarezertifikat benötigt. …
>
> **7. Zugriffsrechte**
> Der Zugriff auf die Software Ismed 3 erfolgt durch den Einsatz eines Softwarezertifikates.
> Die Zugriffsrechte in Ismed 3 werden über die Vergabe von Rechten und Rollen festgelegt (s. Anlage 2 - Rollenkonzept, Eskalationsroutinen und -regeln). …
>
> **8. Auswertungen**
> Im System werden personenbezogene Daten (wer führt welche Aktion durch) in der Attributhistorie und Prozesshistorie protokolliert und können zum Zwecke der Netz- und Betriebssicherheit genutzt werden.
> …

Ein Zugriff auf anonymisierte oder nicht anonymisierte Daten zum Zwecke der individuellen Verhaltens- und Leistungskontrolle erfolgt nicht, es sei denn das gesetzliche Beteiligungsverfahren ist zuvor durchgeführt worden.
…

9. Schulungen
Alle Mitarbeiter, die mit dem System arbeiten sollen, werden vor der Einführung der Software Ismed 3 geschult.

10. Datenschutz
Der Datenschutz wird auf der Grundlage der gesetzlichen Regelungen des Bundesdatenschutzgesetzes, Landesdatenschutzgesetzes, Sozialdatenschutzgesetzes usw. sichergestellt. Es werden geeignete organisatorische Maßnahmen zur Einhaltung der speziellen Anforderungen an den Mitarbeiterdatenschutz gem. § 35 SGB I getroffen.
…“

In der Anlage 2 „Rollenkonzept in Ismed 3“ zu DV Ismed 3 hieß es u.a.:

„Um gewisse Tätigkeiten durchführen zu können, benötigt jeder Mitarbeiter verschiedene Rechte innerhalb von Ismed 3. Die Summe verschiedener Einzelrechte spiegelt sich dabei in den Rollen wieder. Es gibt zur Zeit sechs Standardrollen in Ismed 3, die jedoch erweitert oder ergänzt werden können. Ein Benutzer kann mehrere Rollen besitzen, falls sein Aufgabengebiet dies verlangt. Die Rollen sind:

(1) Berufsgruppenbezogene Rollen

„Verwaltungskraft“ für Assistenzkräfte
Eine Verwaltungskraft kann beispielsweise Aufträge anlegen, Unterlagen erfassen, Gutachten bearbeiten und weiterleiten.
…
„Gutachter“ und „Gutachterfunktion“ für Gutachter:
Ein Gutachter erstellt zugewiesene Gutachten
Jeder Standort verfügt über einen Gruppenarbeitskorb für Gutachter. Die Rolle Gutachter steuert die Ansicht und die Zugriffsmöglichkeit auf den Gruppenarbeitskorb Gutachter.
Gutachter verfügen zusätzlich über die Rolle Gutachterfunktion, die ihnen die Freigabeberechtigung für Gutachten erteilt.
…

(2) Standortbezug
Zu jedem eingerichteten regionalen oder funktionalen Standort fächern sich die eingerichteten Gruppenarbeitskörbe auf. Sie werden für die Mitarbeiter erst sichtbar, wenn sie mindestens einen Auftrag erhalten.
…
- Die Administratoren und der Innenrevisor sind auf den virtuellen Standort „E. (Hverw.)“ als primäre Organisationseinheit eingerichtet.
- Für die Bearbeitung der Gutachten von Mitarbeitern und ihren Angehörigen ist ein virtueller Standort „Spezialfall“ eingerichtet.

…

(3) Zusatzrollen
Die individuelle Zusammenstellung der Rollen und Rechte eines Mitarbeiters weist immer mindestens einen Standortbezug auf (primäre Organisationseinheit) und bildet eine berufsgruppenbezogene Rolle ab. Darüber hinaus können an Mitarbeitergruppen mit Sonderaufgaben Zusatzrollen vergeben werden.
…“

Wegen der weiteren Einzelheiten wird auf die zur Akte gereichte Ablichtung der DV Ismed 3 nebst Anlage 2 Bezug genommen. Betrieb und Weiterentwicklung dieser Software oblagen einer Arbeitsgemeinschaft gemäß § 219 SGB V des Beklagten sowie der N. Dienste der Krankenversicherungen Bayern und Thüringen. Die Datenhaltung erfolgte im Rechenzentrum der C. GmbH in N.. Zweck der C. GmbH war die Entwicklung, Wartung und Zurverfügungstellung u.a. von Rechenzentrumsdienstleistungen für die gesetzliche Krankenversicherung. Die C. GmbH verarbeitete als Dienstleister ausschließlich Sozialdaten der gesetzlichen Krankenversicherung. Die Datenhaltung im Rechenzentrum der C. GmbH erfolgte mandantenbezogen, d.h. die Daten des Beklagten waren von denjenigen anderer andere medizinischer Dienste getrennt. Nach der IT-Sicherheitsrichtlinie des Beklagten war es Ziel, die Basisanforderung des Grundschutzkompendiums des Bundesamtes für Sicherheit und Informationstechnik zu erfüllen.

Der Kläger war seit dem 22.11.2017 ununterbrochen arbeitsunfähig erkrankt. Seit dem 24.05.2018 bezog er Krankengeld in Höhe von 88,34 Euro kalendertäglich von seiner Krankenkasse. Am 06.06.2018 beauftragte die Krankenkasse des Klägers bei dem Beklagten als medizinischem Dienst zur Beseitigung von Zweifeln an dessen Arbeitsunfähigkeit eine gutachtliche Stellungnahme. Für einen solchen Begutachtungsfall existierte bei dem Beklagten die „Dienstanweisung zum Schutz bei Sozialdaten der Beschäftigten des N. Nordrhein und ihrer Angehörigen (*im Folgenden DA Sozialdaten*). In dieser hieß es u.a.:

„1. Ziel und Zweck
… Die Dienstanweisung dient dem Zweck der gesetzlichen Verpflichtung gemäß § 35 Abs. 1 Satz 3 SGB I und § 94 Abs. 3 SGB XI nachzukommen und bereits den Anschein einer Interessenkollision zu vermeiden.

Dem N. Nordrhein ist es ein besonderes Anliegen, daraus resultierende Bevorzugungen oder Benachteiligungen zu vermeiden und einen besonderen Schutz der Sozialdaten zu gewährleisten.

Daher sollen Sozialdaten von Mitarbeitern und ihren Angehörigen am Dienstort des Beschäftigten weder erhoben noch gespeichert werden.

Dies setzt voraus, dass der Beschäftigte entsprechende Konstellationen gegenüber seiner Kranken-/Pflegekasse anzeigt. Der Hinweis an die Kranken/Pflegekasse erfolgt bei jedem Kontakt, z.B. auch bei Widersprüchen gegen Leistungsentscheidungen, da der Fall im N. bereits nach der Gutachtenerstellung abgeschlossen wurde und in diesem Fall sonst ohne erneuten Hinweis keine Kennzeichnung als Spezialfall erfolgt.
…

3. Begriffserläuterungen

3.1. Sozialdaten der Beschäftigten und ihrer Angehörigen
…

Sozialdaten der Beschäftigten bzw. ihrer Angehörigen fallen an, wenn der N. Nordrhein seitens der zuständigen Kranken- oder Pflegekasse beauftragt wird, die sozialmedizinischen Voraussetzungen für Leistungen nach dem SGB für einen N.-Beschäftigten bzw. seinen Angehörigen zu begutachten. Sie dürfen nicht mit „Mitarbeiterdaten“ verwechselt werden, die im Rahmen eines Arbeits-/Dienstverhältnisses entstehen oder verarbeitet werden.

3.2. Zugriffsberechtigte

Zugriffsberechtigt sind Mitarbeiter, die aufgrund ihrer arbeitsvertraglichen Tätigkeit von den Sozialdaten der Beschäftigten und Ihrer Angehörigen Kenntnis erhalten bzw. denen die Möglichkeit des Zugriffs auf diese Daten eingeräumt wurde (zuständige Gutachter und Assistenzmitarbeiter). Die Namen der zuständigen Mitarbeiter sind im beigefügten **„Zugriffskonzept“** hinterlegt.

4. Grundsatz
Beschäftigte und ihre Angehörigen dürfen grundsätzlich nicht an ihren Beschäftigungsort oder an ihrer Dienststelle begutachtet werden. Die diesbezüglichen Unterlagen dürfen dort nicht aufbewahrt, die anfallenden Sozialdaten dort nicht gespeichert werden. Für die Anwendung von Ismed 3 gilt folgende Regelung: Für alle Mitarbeiter, die am Standort E. tätig sind, sind die benannten Mitarbeiter der Organisationseinheit „Spezialfall“ in E. zuständig. Für Mitarbeiter der übrigen Standorte sind die benannten Mitarbeiter der Organisationseinheit „Spezialfall“ in E. zuständig.

Die Sozialdaten dürfen von den Zugriffsberechtigten nur zu den überlassenen Verarbeitungszwecken verwendet werden. Eine Weitergabe an unbefugte Dritte ist verboten.

5. Verfahren

5.1. Organisationseinheit Spezialfall

a) Ismed 3

…

Der betroffene Mitarbeiter oder Angehörige unterrichtet seine Krankenkasse im Vorfeld der Beauftragung des N. darüber, dass seine Unterlagen ausschließlich an das für die Bearbeitung von Spezialfällen zuständige BBZ abgegeben werden darf. Zum Versand der Auftragsunterlagen reicht er seiner Krankenkasse den gekennzeichneten Umschlag ein, der bereits zutreffend an die Organisationseinheit „Spezialfall“ adressiert ist.

Begutachtungsaufträge im Rahmen des SGB V (Krankenversicherung), die die Beschäftigten des N. Nordrhein oder ihre Angehörigen betreffen, müssen in der zuständigen Organisationseinheit „Spezialfall“ eingehen und dürfen ausschließlich dort bearbeitet werden.

Sollte der Auftrag zur Begutachtung eines Mitarbeiters oder des Angehörigen eines Mitarbeiters fälschlicherweise ohne gekennzeichneten Umschlag im BBZ eingehen, so erfolgt die Weiterleitung nach Maßgabe der beigefügten “Kurzinfo Spezialfall“. Das Setzen des Merkmals „Spezialfall“ übernimmt einen bereits angelegten Fall mit den zugehörigen Unterlagen in die Organisationseinheit „Spezialfall“. Der Fall ist für die übrigen Mitarbeiter nicht mehr sichtbar. Die auftraggebende Krankenkasse erhält eine Abgabenachricht.
…

5.2. SFB/Aktenlage

a) Ismed 3

Die eingehenden Fälle werden bei der Erfassung als „Spezialfall gekennzeichnet und ausschließlich durch die benannten Mitarbeiter der Organisationseinheit „Spezialfall“ bearbeitet. Die Fälle müssen als Produktart „SFB mit Stellungnahme“ bzw. „KH-SFB“ bearbeitet und im elektronischen Archiv hinterlegt werden.
…

5.4. Archivierung

a) Ismed 3

Nach Abschluss des Begutachtungsauftrages im Rahmen des SGV V (Krankenversicherung) den Auftrag mit der gutachterlichen Stellungnahme einschließlich der beim N. Nordrhein verbleibenden elektronischen medizinischen Unterlagen abschließen und im elektronischen Archiv hinterlegen.
…

5.5. Begutachtungsaufträge mit einer körperlichen Untersuchung bei Beschäftigten/Angehörigen des N. Nordrhein

…

Im Falle eines Begutachtungsauftrages im Rahmen des SGB V oder SGB XI, der bei einem Beschäftigten/Angehörigen eines Beschäftigten eine körperliche Untersuchung beinhalten würde, erfolgt die Begutachtung durch den Sozialmedizinischen Dienst der Knappschaft.

a) Ismed 3

Falls der Gutachter bei einem Spezialfall feststellt, dass eine körperliche Untersuchung unumgänglich ist, werden die Unterlagen den Assistenzkräften der Organisationseinheit „Spezialfall“ zur weiteren Veranlassung übergeben.

Der Gutachter schließt den Fall ab mit dem Schlüssel:

„90 Zur Begutachtung empfohlen“ (vgl. **„Schulungsunterlage Spezialfall“**).

Der Abschluss erfolgt als Produktart „SFB ohne Stellungnahme“.

Der Arzt und die Assistenzkraft der Organisationseinheit „Spezialfall“ übergeben den Auftrag an den Leitenden Arzt der Knappschaft, der diejenige Dienststelle der Knappschaft mit der Untersuchung beauftragt, der dem Wohnort des Begutachtenden am nächsten gelegen ist und veranlasst nachfolgend auch die Rücksendung des Gutachtens.

Die elektronische Archivierung erfolgt durch die Assistenzkräfte der Organisationseinheit „Spezialfall“, die das Gutachten zum Auftrag nachscannen.

Die tatsächliche Erstellung des Gutachtens durch die Bundesknappschaft ist von der Organisationseinheit „Spezialfall“ zu überwachen.
…“

Wegen der weiteren Einzelheiten wird auf die zur Akte gereichte Ablichtung der DA Sozialdaten sowie die Kurzinfo Spezialfall zu Ismed 3, zum Arbeitsablauf und zum Umschlag „Spezialfall“ und die Schulungsunterlage Spezialfall Bezug genommen. Weiter wird Bezug genommen auf das vom Beklagten in Ablichtung zur Akte gereichte Verzeichnis der Verarbeitungstätigkeit gemäß Art. 30 Abs. 1b DSGVO zur Verarbeitungstätigkeit „Begutachtung von eigenen Beschäftigten und deren Angehörigen“ nebst Anlagen. Insgesamt erhielten 36 Personen Zugriff auf den geschützten Bereich. Es handelte sich dabei um ärztliche Mitarbeiter, Assistenzkräfte und Mitarbeiter der IT-Technik. Die Zugriffsberechtigung für die Bearbeitung der Spezialfälle war gemäß Anlage 3 zum Schriftsatz des Beklagten vom 16.10.2019, auf die wegen der Einzelheiten Bezug genommen wird, aufgeteilt in „Teilbereich Ambulante Versorgung“ mit den Beratungs- und Begutachtungszentren (BBZ) E. und E., denen jeweils Ärzte und Assistenzkräfte zugeordnet waren, „Teilbereich Stationäre Versorgung“ mit den BBZ E. und E., denen jeweils Ärzte, Kodierfachkräfte und Assistenzkräfte zugeordnet waren, „Teilbereich MFB Behandlungsfehler mit dem BBZ N.“ und in „Teilbereich IT Abteilung“ mit der Zentrale in E. mit neun Mitarbeitern des IT-Bereiches. Einer dieser neun Mitarbeiter

war der Kläger. Die IT-Abteilung war nicht nur für E. zuständig, sondern übergreifend, d.h. u.a. auch für das BBZ in E.. Sämtliche Mitarbeiter des geschützten Bereichs waren auf das Sozialgeheimnis verpflichtet. Sie wurden schriftlich bei ihrer Einstellung darauf verpflichtet und auf die strafrechtlichen und arbeitsrechtlichen Rechtsfolgen einer Verletzung hingewiesen. Im Rahmen von regelmäßigen Schulungen wurden die Mitarbeiter des Beklagten im Hinblick auf die Bedeutung des § 35 SGB I und die Einhaltung des Sozialdatenschutzes geschult.

Am 12.06.2018 kam es im Rahmen eines BEM-Verfahrens zu einem Gespräche zwischen dem Kläger, seiner Ehefrau und dem BEM-Beauftragten des Beklagten dessen Inhalt zwischen den Parteien ebenso streitig ist wie die Frage, wer die Initiative zu dem BEM ergriffen hat.

Der Gutachtenauftrag der Krankenkasse des Klägers war auf postalischem Weg im BBZ E. des Beklagten eingegangen. Der Auftrag wurde durch den zuständigen Sachbearbeiter unmittelbar händisch dem elektronischen sog. geschützten Bereich zugeordnet. Einen Umschlag Spezialfall hatte der Kläger gegenüber der Krankenkasse nicht verwandt. Das Gutachten wurde von der Ärztin Dr. med. I., die im BBZ E. tätig und Mitarbeiterin des geschützten Bereichs war, durchgeführt. In diesem Zusammenhang rief sie am 21.06.2018 den behandelnden Arzt des Klägers an und bat diesen um Auskunft Zwecks Verifizierung der Arbeitsunfähigkeit des Klägers. Von diesem Telefonat unterrichtete der behandelnde Arzt den Kläger. Das am 22.08.2018 erstellte Gutachten enthielt u.a. folgende Angaben:

> **„Diagnose(n):** F32.2 - Schwere depressive Episode ohne psychiotische Symptome
> …
>
> Herr N. S., geb. 10.07.1956
>
> **Unterlagen / med. Unterlagen:**
> …
>
> Behandlertelefonat am 21.08.2018
>
> **Beurteilung / Beantwortung der Fragen des Auftraggebers:**
> Nach Rücksprache mit dem behandelnden Psychiater ist mit der Rückkehr an den Arbeitsplatz in ca. zwei Monaten zu rechnen bei bereits eingetretener Teilstabilisierung.
> Weitere Maßnahmen seien zur Wiederherstellung des beruflichen Leistungsvermögens nicht erforderlich.
> Der Versicherte sei bereits im Gespräch mit dem AG.
>
> …
>
> **Ergebnis:** Aus medizinischer Sicht auf Zeit AU
> …“

…

Wegen der weiteren Einzelheiten wird auf die zur Akte gereichte Ablichtung des Gutachtens (Bl. 89, 90 d.A.) Bezug genommen. Das Gutachten vom 22.06.2018 wurde elektronisch im geschützten Bereich des Beklagten abgespeichert. Die Auftragsdaten mit den Stammdaten und die Begutachtungsdaten wurden getrennt in zwei Datenbanken gespeichert. Ein Zugriff von den Auftragsdaten zu den Begutachtungsdaten erfolgte über einen in der Oracle Verschlüsselungsbibliothek hinterlegten Schlüssel. Ohne diesen konnten Auftragsdaten nicht einzelnen Versicherten zugeordnet werden. Nur im Falle eines hergestellten Auftragsbezugs konnten durch einen zugriffsberechtigten User über die Oracle Verschlüsselungsbibliothek eine automatisierte Zuordnung der Begutachtungsdaten zum Auftrage erfolgen. Der Zugriff zum System konnte zudem nur durch einen berechtigten User erfolgen, was vom System technisch geprüft wurde. Der Begutachtungsauftrag wurde bis zum Abschluss als offener Auftrag geführt und dann archiviert. Ein erneuter Zugriff konnte nur über das Verschlüsselungs-Package in der Verschlüsselungsbibliothek erfolgen. Technisch konnten auch nach dem Abschluss auf das Gutachten vom 22.06.2018 betreffend den Kläger jedenfalls die neun IT-Mitarbeiter des geschützten Bereichs zugreifen. Personen, die bei dem Beklagten Personalentscheidungen trafen oder daran mitwirkten, hatten keinen Zugriff und erhielten auch keine Kenntnis.
Am 01.08.2018 rief der Kläger seine Kollegin, die IT-Mitarbeiterin T. an. Frau T. war zu diesem Zeitpunkt als Mitarbeiterin des Bereichs IT grundsätzlich berechtigt, auf die sog. Spezialfälle zuzugreifen. Der Kläger bat Frau T. nachzusehen, ob ein Gutachten über ihn vorliege. Frau T. überprüfte dies händisch und teilte dem Kläger mit, dass dies der Fall sei. Der Kläger bat Frau T. sodann unter Hinweis auf die langjährige kollegiale Zusammenarbeit, das Gutachten abzufotografieren und ihm zu senden. Dies tat Frau T.. Es handelte sich bei der übermittelten Bilddatei um den hier zur Akte gereichten Screenshot. Von diesem Sachverhalt hatte der Beklagte Kenntnis erlangt, nachdem er den Sachverhalt nach dem Termin vor der erkennenden Kammer am 13.11.2019 durch den Innenrevisor unter Beteiligung des Personalrats ermittelt hatte. Außer dem Zugriff von Frau T. am 01.08.2018 hatten ausweislich der Protokolldatei des Gutachtens des Klägers auf dieses nur Beschäftigte zugegriffen, die unmittelbar mit der Bearbeitung des Falles oder der Gutachtenerstellung betraut waren.

Mit Schreiben vom 15.08.2018 forderte der Kläger durch seine Prozessbevollmächtigten von dem Beklagten die Zahlung einer Entschädigung in Höhe von 20.000,00 Euro. Der Beklagte lehnte dies mit Schreiben vom 03.09.2018 ab.

Der Bezug des Krankgeldes durch den Kläger endete am 15.05.2019.

Der Beklagte sprach gegenüber dem Kläger fristlose Kündigungen vom 05.12.2019 und vom 12.12.2019 aus. Die erste fristlose Kündigung erfolgte noch vor Ablauf der dem Kläger vom Inklusionsamt gesetzten Frist zur Stellungnahme bis zum 06.12.2019. In der vorherigen Anhörung gegenüber dem Kläger hat der Beklagte die Kündigungen

damit begründet, dass er die hier vorliegende Klage mit dem Ziel materiellen und immateriellen Schadensersatz zu verlangen führe, weil eine Kollegin auf das Gutachten zugegriffen habe. Dies sei mit dem Hinweis erfolgt, dass er ohne die Datenschutzverletzung wesentlich früher arbeitsfähig gewesen sei. Die Kollegen wüssten jetzt, welche Erkrankung der Kläger habe und er, der Beklagte, habe nicht alles dafür getan, seine vertraulichen Daten zu schützen. Die Vorwürfe seien nach dem tatsächlichen Sachverhalt nicht haltbar. Durch diese Verhaltensweise sei das Vertrauensverhältnis erschüttert. Der Kläger hat gegen beide Kündigungen Kündigungsschutzklage bei dem Arbeitsgericht Düsseldorf erhoben. Beide Kündigungsschutzverfahren waren im Zeitpunkt der letzten mündlichen Verhandlung am 11.03.2020 anhängig und nicht rechtskräftig entschieden. Der Beklagte hörte seinen Personalrat zu einer fristlosen und hilfsweise ordentlichen Kündigung von Frau T. an.

Der Kläger hat gemeint, ihm stehe ein Anspruch aus Art 82 Abs. 1 DSGVO zu, den er auch auf § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG stützen könne. Der Beklagte habe sein Persönlichkeitsrecht schwerwiegend verletzt. Als sein Arbeitgeber habe er die Aufgaben des medizinischen Dienstes nicht wahrnehmen und sich so seine Gesundheitsdaten verschaffen dürfen. Er habe zu dem Schutz dieser Daten unzureichende Vorkehrungen getroffen. Dies belege bereits die telefonische Anfrage von Frau Dr. I. bei dem ihn behandelnden Arzt. Es handele sich dabei um eine Kollegin, mit der er immer mal wieder zu tun gehabt habe, auch wenn diese am Standort E. tätig war. Diese habe nicht ohne seine Einwilligung mit dem ihn behandelnden Arzt Kontakt aufnehmen dürfen. Wenn überhaupt, habe die Kontaktaufnahme schriftlich im sog. Umschlagverfahren zu erfolgen gehabt. Die telefonische Anfrage lasse Raum dafür, mehr in Erfahrung zu bringen als bei einer schriftlichen Anfrage und lasse auf ein vorsätzliches Handeln des Beklagten schließen. Bei telefonisch erbetenen Auskünften gebe das spätere Speichern nicht „automatisch“ den Inhalt des zuvor Besprochenen vollständig und zutreffend wieder. Und der Umstand, dass eine Kollegin aus dem geschützten Bereich telefonisch nachfragte, gebe ihm berechtigten Anlass zur Sorge, dass mehr erfragt wurde, als aus den gespeicherten Daten ersichtlich. Außerdem hätten die erhobenen Gesundheitsdaten überhaupt erst dem geschützten Bereich zugeordnet werden müssen und seien davor auch außerhalb dieses Bereiches einsehbar gewesen. Es hätten nicht nur die IT-Mitarbeiter als seine unmittelbaren Kollegen, sondern sämtliche Mitarbeiter des geschützten Bereichs Zugriff auf das Gutachten vom 22.08.2018 gehabt. Bereits die Einsehbarkeit stelle eine schwere Persönlichkeitsverletzung dar, weil der Betroffene nicht wisse, wer Einsicht genommen hat. Der Beklagte als Arbeitgeber müsse den Datenschutz auch gegenüber den Kollegen sicherstellen, wie er es ja auch gegenüber den Mitarbeitern außerhalb des geschützten Bereichs tue. Von einer entsprechenden Lücke des Datenschutzes habe der Beklagte gewusst, ohne Abhilfe zu schaffen. Die ehemalige Personalratsvorsitzende habe den Datenschutzbeauftragten des Beklagten darauf hingewiesen. Der Kläger hat gemeint, auch nicht-körperliche Untersuchungen hätten an einen Dritten wie die Knappschaft vergeben werden müssen, was zumindest des Öfteren in der Vergangenheit geschehen sei. Hinzu komme, dass er psychisch erkrankt sei. Gerade diese Gesundheitsdaten seien besonders sensibel, weil sie dem höchstpersönlichen Bereich zuzuordnen seien und

…

nicht automatisch nach außen erkennbar seien. Die Verbreitung einer solchen Erkrankung innerhalb der Belegschaft sei eine ganz erhebliche Belastung. Der Umstand, dass den Personalverantwortlichen kein unmittelbares Zugriffsrecht zustehe, sei unerheblich, weil die Informationen über seinen psychischen Zustand sich hinter vorgehaltener Hand wie ein Lauffeuer verbreiten und so auch die Personalabteilung erreichen würden. Der Kläger hat gemeint, § 35 SGB I betreffe nicht den hier in Rede stehenden Sachverhalt.
Der Kläger hat behauptet, er sei zunächst von einer ebenfalls in dem „besonders geschützten EDV-technischen Bereich“ tätigen Person in einem Telefonat darauf hingewiesen worden, dass für zumindest ca. 10 der dortigen Mitarbeiter und unmittelbaren Kollegen, Gesundheitsdaten über ihn einsehbar seien, betreffend die Diagnose einer psychischen Erkrankung (Seite 4 der Klageschrift vom 28.09.2018). Auf weitere Darlegungen zu dem Telefonat komme es nicht an, weil dieses Telefonat kein den Anspruch begründendes Tatbestandsmerkmal sei, sondern lediglich aufzeige, wie er davon erfahren habe, dass es ein ihn betreffendes Gutachten zu seinem psychischen Gesundheitszustand gebe, das ebenfalls von seinen Kollegen im geschützten Bereich ohne weiteres einsehbar war (Seite 7 des Schriftsatzes vom 07.01.2019). Es müsse also Einblick genommen worden sein in die ihn betreffenden Daten, was im Übrigen auch dadurch bestätigt werde, dass er von einem Kollegen über die Existenz des von dem Beklagten eingeholten Gutachten über ihn informiert worden sei. Dieser Kollege habe ihm auch einen Screenshot des Gutachtens geschickt (Seite 8 des Schriftsatzes vom 07.06.2019).
Der Kläger hat im Übrigen gemeint, dass auch Spannungen mit dem Arbeitgeber zu seiner psychischen Erkrankung beigetragen hätten, die daraus resultierten, dass der Beklagte sich ungeachtet eines ärztlichen Attests geweigert habe, ihn in einem anderen Arbeitsbereich in der Verwaltung einzusetzen. Letztlich komme es darauf für dieses Verfahren nicht an. Dies stehe auf einem anderen Blatt.

Der Kläger hat beantragt,

den Beklagten zu verurteilen, ihm eine Entschädigung nach billigem Ermessen des Gerichts, mindestens jedoch 20.000,00 Euro zu zahlen.

Der Beklagte hat beantragt,

die Klage abzuweisen.

Er ist der Ansicht gewesen, er dürfe auch im Fall des Klägers seinen gesetzlichen Aufgaben nachkommen. Von dem Auftrag der Krankenkasse des Klägers zur Begutachtung habe er aufgrund der Zuordnung zum geschützten Bereich erst durch die Klage erfahren. Die telefonische Kontaktaufnahme und Erhebung von Daten durch die

Ärztin Dr. I. sei gemäß § 276 SGB V erfolgt, der eine Offenbarungspflicht des behandelnden Arztes enthalte. Wenn der behandelnde Arzt der Meinung gewesen sei, Frau Dr. I. habe sich nicht ausreichend identifiziert, so hätte er die Auskunft verweigern können. Die anrufenden Ärzte würden sich durch entsprechende Angaben ausweisen. Bei Zweifeln werde dem behandelnden Arzt ein Rückruf angeboten. Die Bezugnahme auf das Umschlagverfahren gehe fehl, weil es wegen datenschutzrechtlicher Bedenken nicht mehr existiere. Den Umgang mit den hier in Rede stehenden Daten regele § 35 SGB I, der auch nach der neuen DSGVO nicht geändert worden sei.
Der Beklagte hat bestritten, dass eine Mitarbeiterin aus dem geschützten EDV-technischen Bereich den Kläger darauf hingewiesen habe, dass jemand aus dem besonders geschützten Bereich auf die Gesundheitsdaten unberechtigt habe zugreifen können. Der Kläger benenne diese Person nicht.
Da der Kläger sich zu dem Ergebnis des BEM nicht geäußert habe, hat die Beklagte den Kläger mit Schriftsatz vom 03.01.2019 aufgefordert, einen Rentenantrag zu stellen. Sie selbst habe im Übrigen keine Zweifel an der Arbeitsunfähigkeit des Klägers gehabt und auch keinen Gebrauch von § 5 N.-T gemacht. Gemäß § 36 N.-T dürfe sie den Kläger aber zum Rentenantrag auffordern, wenn die Voraussetzungen der verminderten Erwerbsfähigkeit vorliegen.

Das Arbeitsgericht hat die Klage auf Entschädigung mit Urteil vom 22.02.2019 abgewiesen. Über den nach Schluss der mündlichen Verhandlung am 18.01.2019 gestellten Antrag des Klägers, festzustellen, dass der Beklagte verpflichtet sei, ihm den materiellen Schaden zu ersetzen, der ihm aus der mit der Klage geltend gemachten Verletzung seines Persönlichkeitsrechts entstanden sei und noch entstehen werde, hat das Arbeitsgericht nicht entschieden, weil es keinen Grund für eine Wiedereröffnung der mündlichen Verhandlung gesehen hat. Gegen das ihm am 07.03.2019 zugestellte Urteil hat der Kläger am 14.03.2019 Berufung eingelegt und diese - nach Verlängerung der Berufungsbegründungsfrist bis zum 07.06.2019 - am 07.06.2019 begründet.

Der Kläger ist der Ansicht, dass das Arbeitsgericht nicht ausreichend den Umstand gewürdigt habe, dass es hier um Gesundheitsdaten gehe, die von einer Arbeitskollegin erhoben und von Arbeitskollegen eingesehen werden konnten. Soweit das Arbeitsgericht die Erlaubnis und Erforderlichkeit der Datenerhebung mit Art. 6 Abs. 1 Buchstabe c DSGVO i.V.m. §§ 275, 276 SGB V begründet habe, habe es den Begriff der „Erforderlichkeit“ nur im Sinne einer Bedingung geprüft. Erforderlichkeit i.S.v. Art. 6 Abs. 1 Buchstabe c DSGVO sei erkennbar als Verweis auf die Einhaltung des Verhältnismäßigkeitsgrundsatzes zu verstehen. Das Verständnis des Arbeitsgerichts, dass ohne Datenerhebung keine Begutachtung möglich sei, genüge dem nicht. Es müsse darauf geschaut werden, um was für eine Kategorie von Daten es sich handele und nur dann könne im Rahmen einer Gesamtabwägung beurteilt werden, ob die Schwere des Eingriffs noch in einem zu tolerierenden Verhältnis zu den rechtfertigenden Gründen stehe. Und aus der Zulässigkeit der Erhebung der Daten folge noch nicht, dass deren weitere Verarbeitung rechtmäßig sei. Selbst wenn die Kollegen zur Erfüllung ihrer Aufgaben grundsätzlich auf seine Daten zugreifen müssten, sage dies nichts über deren weitere Verarbeitung und Speicherung sowie geeignete diesbezügliche Vorkehrungen

gegen Datenmissbrauch aus. Es gehe gerade darum, dass die Kollegen des geschützten Bereichs das Gutachten einsehen konnten, was zumindest für seine unmittelbaren Kollegen ohne weiteres möglich gewesen sei, weil bei dem Vorgang des automatischen Datenabgleichs Name, Anschrift und ICD-Nummer sichtbar seien. Er, der Kläger, sei davon ausgegangen, dass bei Mitarbeitern des geschützten Bereichs die Begutachtung durch die Knappschaft erfolge.
Zu berücksichtigen sei weiter, dass es sich nicht um irgendwelche Daten handele, sondern um die besonders gemäß Art. 9 DSGVO geschützten Gesundheitsdaten. Hier würden noch einmal strengere Anforderungen gelten. Es müssten besondere Vorkehrungen und ein erhöhter Schutz gewährleistet sein. Dies gelte insbesondere für Bedingungen und Garantien aus Art. 9 Abs. 3 DSGVO. Zwar gestatte Art. 9 DSGVO unter dieser Bedingung die Erhebung von Gesundheitsdaten zur Beurteilung der Arbeitsfähigkeit der Beschäftigten. Dies habe die hiesige Situation aber nicht im Blick, denn typischerweise begutachte der Medizinische Dienst die Arbeitsfähigkeit von anderswo beschäftigten Personen. Dann sei die Verschwiegenheit des Arztes eine recht sichere Garantie dafür, dass Kollegen des Arbeitnehmers als auch dessen Kollegen davon nichts erfahren. Es gebe insoweit von vornherein kein betriebliches Miteinander. Nur auf diesen Normalfall sei Art. 9 Abs. 2 Buchstabe h DSGVO zugeschnitten. Nur dann reiche der Bezug zur Schweigepflicht. Hier sei es anders. Dass seine Kollegin Dr. I. der ärztlichen Schweigepflicht und dem Sozialgeheimnis unterliege, ändere nichts daran, dass sie seine Gesundheitsdaten als Kollegin nichts angehen. § 35 SGB I ändere daran nichts.
Wie der Beklagte aus der Zwickmühle herauskomme, müsse nicht er aufzeigen. Aber es gebe den Weg der Begutachtung über die Knappschaft. Außerdem lasse es sich der DSGVO entnehmen, dass zum Schutz auch bestimmte technische Maßnahmen geschaffen werden könnten, wie z.B. die Pseudonymisierung.
Die allgemeinen organisatorischen Vorkehrungen des Beklagten zum Datenschutz hätten mit dem hier in Rede stehenden Sachverhalt nichts zu tun. Diesbezüglich habe der Beklagte nichts unternommen. Dass er als Arbeitgeber keine Einsicht nahm, sei ebenso unerheblich wie die Verpflichtung der Kollegen auf den Sozialdatenschutz. Gerade aus den Aspekten der Datenminderung und der Datensparsamkeit sei nicht nachvollziehbar, dass ausgerechnet seine engsten Kollegen die Daten einsehen konnten. Es hätte eines weiteren Sicherungsmechanismus, wie z.B. des Vier-Augenprinzips bedurft bzw. der externen Begutachtung mit allenfalls nachfolgender Speicherung. In einer E-Mail vom 03.07.2018 habe die ehemalige Personalratsvorsitzende ihm bestätigt, dass es eine Lücke im Verfahren gebe, wenn der Auftrag im Datenaustausch ankomme, d.h. dem Beklagten online von der C. GmbH übermittelt werde. Die Software merke nicht, wenn es sich um Daten eines Mitarbeiters handele. So könne es dazu kommen, dass auch Mitarbeiter außerhalb des geschützten Bereichs diese Daten einsehen und eben auch eine Kollegin von ihm mit dem Gutachten betraut werde. Es hätte bereits beim Dateneingang eines Gegenlaufes des Mitarbeiterverzeichnisses bedurft. Die Personalratsvorsitzende habe allgemein einen besseren Schutz der Mitarbeiterdaten gefordert, weil diese zumindest von den Personen im geschützten Bereich eingesehen werden könnten.

Der Kläger ist der Ansicht, dass gerade die Einhaltung der Schriftlichkeit dem Schutz der Gesundheitsdaten diene, weil im persönlichen Gespräch eher die Preisgabe weiterer, nicht benötigter Informationen bestehe, ohne dass dies nachvollzogen werden könne. Dies gelte erst rechte, wenn der Gutachter ein Arbeitskollege sei. Der Beklagte hingegen scheine eher das Verhalten der Person aus dem Kollegenkreis zu beanstanden, ihn durch Übermittlung des Screenshots des Gutachtens informiert habe. Hier werde der „Whistleblower“ zum Übeltäter, was von der Verantwortlichkeit des Beklagten ablenke. Er wolle diese Person aus verständlichen Gründen nicht nennen. Dies ändere aber nichts an der Zugriffsmöglichkeit. Andernfalls hätte die Person ihm nicht das Gutachten übermitteln können (Seite 11 des Schriftsatzes vom 06.11.2019).
Im Hinblick auf den geltend gemachten materiellen Schadensersatz behauptet der Kläger, dass er ohne die streitgegenständliche Persönlichkeitsverletzung nach der Einschätzung des behandelnden Arztes seine Tätigkeit bei dem Beklagten ab dem Monat Dezember 2018 hätte wieder aufnehmen können. Ohne die Persönlichkeitsverletzung wäre er jedenfalls noch im Spätsommer 2018 wieder ausreichend psychisch belastbar gewesen für die von der Beklagten angebotene stufenweise Wiedereingliederung. Er wäre dem Rat seines Arztes gefolgt und hätte aktiv um eine Wiedereingliederung gebeten, die dann auch durchgeführt worden wäre. Innerhalb weniger Wochen wäre seine Einsatzfähigkeit wieder hergestellt gewesen. Im Übrigen müsse in Parallele zum Arzthaftungsrecht und zum Schadensersatzanspruch bei Verletzung der Verkehrssicherungspflicht der Beklagte nachweisen, dass derselbe Schaden auch bei ordnungsgemäßem Handeln eingetreten sei.
Der Kläger weist mit Schriftsatz vom 17.12.2019 darauf hin, dass es sich um eine zivilprozessuale Auseinandersetzung handele. Der Streitgegenstand, auf den er den Schadensersatz stütze, werde alleine von ihm als klagender Partei bestimmt. Was zunächst den haftungsbegründenden Tatbestand anbelange, komme es auf die von dem Beklagten zuletzt in den Fokus gerückte Betrachtung, wer und warum auf sein Gutachten zugegriffen habe, überhaupt nicht an. Er habe im Übrigen an keiner Stelle behauptet, ein Arbeitskollege habe aus eigener Initiative in das Gutachten geschaut und dieses aus eigener Initiative übermittelt. Hierauf habe er den haftungsbegründenden Tatbestand zu keiner Zeit gestützt. Er habe dafür auf einen vorgelagerten Sachverhalt, nämlich das Telefonat von Frau Dr. I. mit seinem behandelnden Arzt abgestellt. Seine Klage werde darauf gestützt, dass der Beklagte es aufgrund unzureichender Sicherheitsstrukturen innerhalb des eigenen Organisationsbereiches zu verantworten habe, dass sein Fall Frau Dr. I. als Kollegin aus dem geschützten Bereich zugewiesen wurde. Die Haftung des Beklagten sei von Beginn an aus dem Telefonat mit seinem Arzt abgeleitet worden. Eine spätere Einsichtnahme in das Gutachten könne an dem zuvor verwirklichten haftungsbegründenden Tatbestand nichts ändern. Zwar könne eine Haftung auch auf mehrere Verletzungshandlungen gestützt werden. Das habe er aber nicht getan. Mit seiner Klage habe er den Tatbestand eines auf das Gutachten erfolgten Zugriffs gerade nicht als haftungsbegründenden Tatbestand geltend gemacht. Seine Ausführungen zu der Einsichtnahme durch eine im geschützten Bereich tätige Person und die betreffend die Übermittlung des Screenshots seien ausschließlich zum Zwecke der Illustration erfolgt, dass im Hause der Beklagten völlig unzureichende Si-

cherheitsvorkehrungen gegen ein späteres unberechtigtes Aufrufen der Daten gegeben seien. Ein Mitarbeiter des geschützten Bereichs könne das Gutachten eines Arbeitskollegen aufrufen. Es fehlte dazu an Schutzvorkehrungen und an Kontrollen. Von einem Funktionieren der Sicherheitssysteme, wie der Beklagte annehme, könne nicht ansatzweise die Rede sein, wenn für den Fall der Begutachtung eines N.-Mitarbeiters keine Vorkehrungen für eine Ausgliederung getroffen seien. Der Beklagte versuche stattdessen ihn und Frau T. zu den Tätern abzustempeln und mundtot zu machen.
Der Umstand, dass sich durch das Telefonat mit Frau T. bestätigt habe, dass das Gutachten im geschützten Bereich ohne weiteres einsehbar sei, sei noch einmal zusätzlich bei der Bemessung des Schadensumfangs zu berücksichtigen. Dies gelte auch dafür, dass der Beklagte sich nicht entschuldige, sondern zum Gegenangriff übergehe und ihm unter Ausblendung des Sachvortrags Prozessbetrug vorwerfe. Er mache die offensichtlich unwirksame Kündigung auch im Rahmen dieses Verfahrens als weitere Rechtsverletzung geltend, die bei der Zuerkennung des ihm einheitlich zuzusprechenden Entschädigungsanspruchs anspruchserhöhend zu berücksichtigen sei. Gleiches gelte für die gegenüber Frau T. durch den Beklagten angedrohte fristlose Kündigung, die bei ihm - wenn auch der Sache nach unberechtigte - Gewissensbisse ausgelöst habe. Dürften einzelne vertraute Arbeitnehmer nicht über Datenschutzversäumnisse sprechen, wären diese umso schwieriger nachweisbar. Angesichts seiner Herabwürdigung sei die Festsetzung eines empfindlichen Entschädigungsbetrages erforderlich, weil der Beklagte versuche, den Spieß umzudrehen und das Opfer zum Täter mache.
Soweit das Landesarbeitsgericht in seinem Beweisbeschluss vom 13.11.2019 darauf abgestellt habe, dass er im Dezember 2018 wieder voll arbeitsfähig sei, wenn es nicht zu der Speicherung des sozialmedizinischen Gutachtens im geschützten Bereich gekommen wäre, entspreche dies nicht seinem Sachvortrag. Der Beweisbeschluss sei dahingehend abzuändern, dass es heißen müsse, wenn es nicht zu dem von Frau Dr. I. getätigten Anruf bei seinem behandelnden Arzt gekommen wäre. Die Primärschädigung liege in einer ihm gegenüber begangenen Verletzung immaterieller Rechte mit Folge eines daraus resultierenden einheitlichen immateriellen Ersatzanspruchs, der auf sich überlagernden Rechtsgrundlagen beruhe, nämlich Art. 82 i.V.m. Art. 9 DSGVO, Art. 1 GG i.V.m. § 823 Abs. 2 BGB und § 823 Abs. 1 BGB. Und selbstverständlich habe sein Arzt ihn über den Anruf von Frau Dr. I. unterrichten dürfen.
Im Termin am 11.03.2020 hat der Klägervertreter auf Nachfrage des Gerichts erklärt, dass er anspruchsbegründend für den haftungsbegründenden Tatbestand des Streitgegenstandes materieller Schadensersatz immer nur auf das Telefonat von Frau Dr. I. abgestellt habe. Er habe haftungsbegründend nicht auf einen Anruf bei einer Kollegin betreffend die Speicherung des Gutachtens abgestellt. Die Speicherung des Gutachtens solle nicht haftungsbegründend, sondern haftungsausfüllend als weitere Folge des haftungsbegründenden Umstandes des aus seiner Sicht unzulässigen Telefonats von Frau Dr. I. und auch der unzulässigen Begutachtung durch diese Person berücksichtigt werden. Es sei aber so, dass er die Speicherung des Gutachtens als Entschädigungstatbestand geltend machen möchte, soweit es die Entschädigung für immateriellen Schaden betreffe, d. h. als einen Datenschutzverstoß, der eine solche Entschädigung seiner Ansicht nach auch, neben den weiteren von ihm geltend gemachten Gründen, begründe.

…

Der Kläger beantragt,

das Urteil des Arbeitsgerichts Düsseldorf vom 22.02.2019 - 4 Ca 6116/18 - abzuändern und

1. **den Beklagten zu verurteilen, an ihn eine angemessene Entschädigung nach billigem Ermessen, mindestens jedoch 20.000,00 Euro zu zahlen;**

2. **den Beklagte zu verurteilen, an ihn einen materiellen Schadensersatz in Höhe des ihm entfallenden Verdienstes zu zahlen in Höhe von jeweils 5.812,00 Euro brutto abzüglich 2.653,00 Euro netto für die Monate Dezember 2018, Januar 2019, Februar 2019, März 2019, April 2019 und Mai 2019 sowie jeweils 5.812,00 Euro brutto für die Monate Juni 2019, Juli 2019, August 2019, September 2019 und Oktober 2019 nebst Zinsen in Höhe von 5 Prozentpunkten über dem Basiszinssatz seit Rechtshängigkeit;**

3. **für den Zeitraum bis Oktober 2019 hilfsweise festzustellen, dass der Beklagte verpflichtet ist, ihm den materiellen Schaden zu ersetzen, der ihm aus der mit der Klage geltend gemachten Verletzung seines Persönlichkeitsrechts entstanden ist und / oder noch entstehen wird und**

4. **für den Zeitraum ab November 2019 festzustellen, dass der Beklagte verpflichtet ist, ihm den materiellen Schaden zu ersetzen, der ihm aus der mit der Klage geltend gemachten Verletzung seines Persönlichkeitsrechts entstanden ist und / oder noch entstehen wird.**

Der Beklagte beantragt,

die Berufung zurückzuweisen.

Er verteidigt das Urteil des Arbeitsgerichts. Grundlage für die Datenerhebung seien §§ 275, 276 SGB V. Er habe im Übrigen alle Vorkehrungen getroffen, dass keine Personen Kenntnis von den Mitarbeiterdaten erhalten, die diese nicht erhalten dürfen. Bei normalem Datenverkehr werde der IT-Mitarbeiter nicht tätig, sondern nur bei Fehlermeldungen. Dies dürfte beim Kläger nicht vorgekommen sein. Technisch liefen mehrere 100.000 Gutachten durch das System, ohne dass ein IT-Mitarbeiter eingreifen müsse. Nur bei Fehlern müsse der Mitarbeiter den Fehler der Datenübertragung beheben und beheben. Eine inhaltliche Kenntnisnahme des Gutachtens sei dazu weder erforderlich noch erlaubt.

Der Beklagte meint, eine telefonische Kontaktaufnahme der begutachtenden Ärztin mit dem behandelnden Arzt verletzte den Datenschutz nicht, weil zwei Geheimnisträger kommunizierten. Der Begutachtungsauftrag der Krankenkasse mache die Datenerhebung erforderlich. § 276 Abs. 2 SGB V regele auch die Übermittlungsverpflichtung eines Leistungserbringers. Es sei gerade gesetzliches Ziel gewesen, zu einem unmittelbaren Austausch zu kommen. Im Übrigen habe sie den Grundsatz der Datensparsamkeit eingehalten. Sie habe nur die Daten erhoben, die für die Begutachtung des Klägers erforderlich seien. Im Übrigen arbeiteten Frau Dr. I. in E. und der Kläger in E.. Beide hätten nicht im gleichen geschützten Bereich gearbeitet.
Soweit der Kläger den oder die Kollegin, welche ihm einen Screenshot gesendet hat, als Whistleblower bezeichne, treffe dies nicht zu. Keiner ihrer Beschäftigten werde in Kenntnis des Sozialdatenschutzes aktiv und unaufgefordert mit dem Kläger Kontakt aufnehmen, um ihm den Screenshot oder andere Daten aus der Akte des Klägers zu übermitteln. Vorstellbar sei allerdings, dass der Kläger mit einem Kollegen oder einer Kollegin aus dem Kreis der besonders Zugriffsberechtigten Kontakt aufgenommen habe und diesen verleitet habe, in das System zu schauen, ob und wenn ja welche Daten von ihm dort gespeichert seien. Dazu möge der Kläger sich erklären.
Nach Kenntnis des Anrufs des Klägers bei Frau T. meint der Beklagte, es liege schon keine Datenschutzverletzung im Verhältnis zum Kläger vor, weil er Frau T. autorisiert habe, in seine Daten Einsicht zu nehmen. Dass Frau T. im Verhältnis zu ihm, dem Beklagten, gegen jede Dienstanweisung verstoßen habe, ändere daran nichts. Ohne das Telefonat mit Frau T. hätte niemand auf das Gutachten Zugriff gehabt. Es wäre dunkel und geschützt im System verblieben. Dies alles zeige, dass die Vorwürfe des Klägers nach allem nicht haltbar seien. Vielmehr habe der Kläger durch seinen Sachvortrag wahrheitswidrig suggeriert, dass in einem Telefonat ein Kollege ihn auf das Gutachten angesprochen habe.
Im Hinblick auf den materiellen Schadensersatz behauptet der Beklagte, dass der Vortrag des Klägers zur angeblichen Genesung nach Wiedereingliederung ohne die angebliche Pflichtverletzung jeglicher Grundlage entbehre. Schließlich sei ihm eine Wiedereingliederung im Rahmen des BEM angeboten worden. Darauf habe der Kläger nicht reagiert. Er, der Beklagte, habe sich bei der Wiedereingliederung nahezu vollständig an die Empfehlungen des behandelnden Arztes des Klägers gehalten. Einzig und alleine der Kläger habe die Wiedereingliederung abgelehnt. Er habe schlicht nicht mehr im Bereich der Administration und des Helpdesk eingesetzt werden wollen. Es fehle auch jeder Sachvortrag zu einer adäquat kausalen Verursachung des geltend gemachten Schadens durch die angebliche Datenschutzverletzung. Diese solle zu einem Zeitpunkt erfolgt sein, zu dem der Kläger bereits über mehrere Monate aufgrund derselben Diagnose und Krankheit arbeitsunfähig war. Im Hinblick auf den nicht haltbaren Vortrag des Klägers sei die Einholung eines medizinischen Sachverständigengutachtens nicht erforderlich. Die Klage sei mutwillig. Hätte die Kenntnis von dem Anruf von Frau Dr. I. bei seinem behandelnden Arzt ihn weiter arbeitsunfähig gemacht, hätte der Arzt des Klägers dieses Telefonat für sich behalten müssen.

Wegen der weiteren Einzelheiten wird auf die gewechselten Schriftsätze nebst Anlagen und Sitzungsprotokolle in beiden Instanzen sowie den Hinweisbeschluss vom

25.09.2019, den Beweisbeschluss vom 13.11.2019 und den Beschluss vom 16.01.2020 Bezug genommen.

E N T S C H E I D U N G S G R Ü N D E:

A. Die zulässige Berufung des Klägers ist unbegründet, weil die zulässigen Klageanträge unbegründet sind. Der Kläger kann von dem Beklagten weder eine Entschädigung für einen immateriellen Schaden verlangen noch Ersatz der von ihm geltend gemachten materiellen Schäden.

I. Der Kläger kann von dem Beklagten keine Entschädigung für einen immateriellen Schaden verlangen. Der diesbezügliche Klageantrag zu 1. ist zulässig aber unbegründet.

1. Der Klageantrag zu 1. ist zulässig.

a) der Klageantrag zu 1. ist hinreichend bestimmt i.S.v. § 253 Abs. 2 Nr. 2 ZPO. Dazu genügt es für den hier geltend gemachten Entschädigungsanspruch, dass der Kläger die Tatsachen benennt, die das Gericht bei der Bestimmung des Betrags heranziehen soll und eine Größenordnung der geltend gemachten Forderung benennt. Diese Anforderungen sind erfüllt. Auf die zutreffenden Ausführungen des Arbeitsgerichts zu B.I.1 der Entscheidungsgründe wird gemäß § 69 Abs. 2 ArbGG zunächst Bezug genommen. Ergänzend darauf hinzuweisen, dass im Rahmen der hier geführten Zivilprozesse nicht etwa Datenschutzverstöße von Amts wegen zu prüfen sind, sondern der Kläger durch seinen Sachvortrag im Rahmen der Dispositionsmaxime den Streitgegenstand bestimmt, der auf einen etwaigen Verstoß im oben genannten Sinn zu prüfen ist. Darauf hat der Kläger zu Recht hingewiesen.

aa) Die Einheitlichkeit des Klageziels genügt nicht, um einen einheitlichen Streitgegenstand anzunehmen. Vielmehr muss auch der Klagegrund identisch sein (BAG 19.11.2019 - 3 AZR 281/18, juris Rn. 45). Zum Anspruchsgrund sind alle Tatsachen zu rechnen, die bei einer natürlichen, vom Standpunkt der Parteien ausgehenden und den Sachverhalt seinem Wesen nach erfassenden Betrachtung zu dem zur Entscheidung gestellten Tatsachenkomplex gehören, den der Kläger zur Stützung seines Rechtsschutzbegehrens dem Gericht vorträgt. Vom Streitgegenstand werden damit alle materiell-rechtlichen Ansprüche erfasst, die sich im Rahmen des gestellten Antrags aus dem zur Entscheidung unterbreiteten Lebenssachverhalt herleiten lassen. Das gilt unabhängig davon, ob die einzelnen Tatsachen des Lebenssachverhalts von den Parteien vorgetragen worden sind oder nicht, und auch unabhängig davon, ob die Parteien die im Vorprozess nicht vorgetragenen Tatsachen des Lebensvorgangs damals bereits kannten und hätten vortragen können (BAG 19.11.2019 a.a.O. Rn. 45).

bb) Zu dem einheitlichen Lebenssachverhalt, den der Kläger der erkennenden Kammer zur Entscheidung betreffend den Entschädigungsanspruch unterbreitet hat, gehört der Umstand, dass das Gutachten im Auftrag der Krankenkasse durch die Ärztin Dr. I. erfolgte, die ebenso wie er, dem geschützten Bereich zugeordnet ist. Er beanstandet weiter, dass die Ärztin ohne seine Einwilligung mit dem ihn behandelnden Arzt und dies nicht schriftlich im Umschlagverfahren sondern telefonisch Kontakt aufgenommen hat. Anders als zum materiellen Schadensersatzanspruch rügt er weiter, dass die Speicherung des Gutachtens im geschützten Bereich erfolgte mit der Folge der Einsehbarkeit des Gutachtens durch seine Kollegen. Dabei hat der Kläger hinreichend deutlich gemacht, dass es für den angeblichen Datenschutzverstoß auf die abstrakte Einsehbarkeit ankommen soll, nicht aber auf die tatsächliche Einsichtnahme in das Gutachten durch Frau T.. Die vom Kläger genannten Umstände betreffen zur Überzeugung der Kammer bei wertender Betrachtung einen einheitlichen Tatsachenkomplex, nämlich diejenigen Umstände, die bei „normaler“ Bearbeitungsweise des Gutachtenauftrags anfallen, d.h. von der Verteilung des Gutachtens an Frau Dr. I., der Durchführung des Gutachtens durch diese und die abschließende Speicherung des Gutachtens. Es handelt sich dabei um eine einheitliche Tätigkeit der Verarbeitung der personenbezogenen Daten des Klägers i.S.v. Art. 4 Nr. 2 DSGVO.

b) Die sachliche Zuständigkeit der Arbeitsgerichtsbarkeit im Hinblick darauf, dass der Beklagte einerseits im Rahmen des Krankenversicherungsrechts als medizinischer Dienst gehandelt hat und andererseits zwischen ihm und dem Kläger ein Arbeitsverhältnis besteht, hatte die Kammer gemäß § 17a Abs. 5 GVG nicht mehr zu prüfen. Eine ausschließliche abweichende sachliche gerichtliche Zuständigkeit ist nicht gegeben. Art. 82 Abs. 6 DSGVO i.V.m. Art. 79 Abs. 2 DSGVO betrifft alleine die hier nicht zweifelhafte internationale Zuständigkeit, während die innerstaatliche Zuständigkeit sich nach den Rechtsvorschriften der Mitgliedstaaten richtet (Bergt in Kühling/Buchner, DS-GVO, BDSG, 2. Aufl. 2018, Art. 79 DS-GVO Rn. 15).

2. Der Klageantrag zu 1. ist unbegründet. Der geltend gemachte Schadensersatzanspruch steht dem Kläger weder aus Art. 82 Abs. 1 DSGVO noch aus § 823 Abs. 1 BGB wegen der Verletzung seiner Gesundheit noch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG i.V.m. wegen Verletzung seines allgemeinen Persönlichkeitsrechts zu.

a) Der Kläger kann von dem Beklagten keine Entschädigung gemäß Art. 82 Abs. 1 DSGVO für den ihm angeblich entstandenen immateriellen Schaden verlangen.

aa) Gemäß Art. 82 Abs. 1 DSGVO hat jede Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immateriellen Schaden entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Es handelt sich bei den Ansprüchen auf Ersatz des materiellen und des immateriellen Schadens um zwei unterschiedliche Streitgegenstände (vgl. insoweit zu § 15 Abs. 1 und 2 AGG BAG 16.02.2012 - 8 AZR 697/10, juris Rn. 21). Mit dem Klageantrag zu 1. machte der Kläger den auf Zahlung einer Entschädigung für den

angeblichen immateriellen Schaden gerichteten Gegenstand geltend. Eine solche Entschädigung setzt gemäß Art. 82 Abs. 1 DSGVO nach seinem Wortlaut voraus, dass ein Verstoß gegen die DSGVO gegeben ist. Es kann offen bleiben, ob damit nur Verstöße gegen die DSGVO selbst oder auch Verstöße gegen nationales Recht gemeint sind, welche der Präzisierung der DSGVO dienen (vgl. dazu unter Bezugnahme auf Erwägungsgrund 146 HK-DS-GVO/BDSG/Schwartmann/Keppeler/Jacquemain, 2018, Art. 82 DS-GVO Rn. 5). Es liegt zur Überzeugung des Gerichts in beiderlei Hinsicht kein Verstoß vor. Es kann offen bleiben, ob der Anwendungsbereich des Unionsrechts im Hinblick darauf, dass es hier - auch - um Rechtsnormen des Krankenversicherungsrechts geht, überhaupt eröffnet ist. Dies ist unbeachtlich, weil die Geltung der DSGVO im Recht der gesetzlichen Krankenversicherung gemäß § 35 Abs. 2 SGB I kraft bundesgesetzlicher Anordnung entsprechend gilt (dazu BSG 18.12.2018 - B 1 KR 40/17 R, juris Rn. 29 ff.; BSG 18.12.2018 - B 1 KR 31/17 juris Rn. 14 f.).

bb) Die Verarbeitung der personenbezogenen Daten durch die Gutachtenerstellung betreffend den Kläger, die - wie sich aus Art. 82 Abs. 2 Satz 1 DSGVO ergibt - in den Anwendungsbereich des Anspruchs auf Entschädigung aus Art. 82 Abs. 1 DSGVO fällt, ist rechtmäßig erfolgt. Sie verstößt weder gegen die Vorschriften der DSGVO noch gegen diese ausfüllendes nationales Recht. Zur Überzeugung der Kammer besteht deshalb kein Entschädigungsanspruch des Klägers aus Art. 82 Abs. 1 DSGVO.

(1) Prüfungsmaßstab für die Rechtmäßigkeit der Erhebung der Gesundheitsdaten des Klägers sind Art. 6 DSGVO und Art. 9 DSGVO. Beide Vorschriften kommen nebeneinander zur Anwendung. Art. 6 DSGVO enthält die allgemeinen Rechtmäßigkeitsvoraussetzungen für eine Datenverarbeitung, die grundsätzlich nur dann gegeben ist, wenn eine der in Art. 6 Abs. 1 DSGVO genannten Bedingungen erfüllt ist. Für Gesundheitsdaten, um die es hier geht, enthält Art. 9 DSGVO ein Verbot mit Erlaubnisvorbehalt (Art. 9 Abs. 2 DSGVO) und bei der Verarbeitung für bestimmte Zwecke zusätzliche Voraussetzungen (Art. 9 Abs. 3 DSGVO). Im Hinblick darauf, dass Art. 9 DSGVO besondere zusätzliche Anforderungen für die Verarbeitung u.a. von Gesundheitsdaten enthält und zugleich Art. 6 DSGVO in Art. 6 Abs. 4 Buchstabe c DSGVO auf Art. 9 DSGVO Bezug nimmt, geht die Kammer davon aus, dass neben dem Ausnahmetatbestand für die Rechtmäßigkeit der Datenverarbeitung von Gesundheitsdaten zugleich die allgemeinen Rechtmäßigkeitsanforderungen aus Art. 6 DSGVO erfüllt sein müssen. Anders ist dies nur dann, wenn die inhaltliche Regelung in Art. 9 DSGVO einen Rückgriff auf Art. 6 DSGVO nicht zulässt (Albers/Veit in Wolff/Brink BeckOK, Datenschutzrecht, 31. Edition 01.11.2019 Art. 9 DS-GVO Rn. 24; dahingehend auch HK-DS-GVO/BDSG/Jaspers/Schwartmann/Mühenbeck a.a.O. Art. 9 DS-GVO Rn. 20; Wedde in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 9 DSGVO Rn. 3).

(2) Die Rechtmäßigkeit der Datenverarbeitung ergibt sich nicht aus der Einwilligung des Klägers (Art. 6 Abs. 1 Satz 1 Buchstabe a DSGVO bzw. Art. 9 Abs. 2 Buchstabe

a DSGVO). Eine solche liegt nicht vor. Dies bedeutet indes nicht, dass die Datenverarbeitung unrechtmäßig war. Die Erstellung des Gutachtens war im vorliegenden Fall ohne Einwilligung des Klägers rechtmäßig.

(3) Es sind zunächst die allgemeinen Anforderungen aus Art. 6 DSGVO erfüllt. Dies hat das Arbeitsgericht in seinen Entscheidungsgründen zur Überzeugung der Kammer zutreffend gewürdigt, worauf diese bereits mit ihrem Beschluss vom 25.09.2019 hingewiesen hat. Die Kammer sieht keinen Anlass, die rechtlichen Aspekte innerhalb der Anwendung von Art. 6 DSGVO und dem dazu ergangenen nationalen Recht anders zu würdigen als das Arbeitsgericht und macht sich dessen Ausführungen insoweit ausdrücklich und weitgehend zu Eigen.

(3.1.) Nach Art. 6 Abs. 1 Satz 1 Buchstabe c DSGVO ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Nach Art. 6 Abs. 2 DSGVO können die Mitgliedsstaaten in Bezug auf die Verarbeitung zur Erfüllung von Art. 6 Abs. 1 Satz 1 Buchstabe c DSGVO spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX DSGVO. Die Rechtsgrundlage für die Verarbeitungen gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c DSGVO wird dementsprechend auch durch das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt (Art. 6 Abs. 3 Satz 1 Buchstabe b DSGVO). In dieser Rechtsgrundlage muss der Zweck der Verarbeitung festgelegt sein (Art. 6 Abs. 3 Satz 2 DSGVO). Sie kann zudem spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften der DSGVO enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX DSGVO (Art. 6 Abs. 3 Satz 3 DSGVO). Das Recht der Mitgliedsstaaten muss dabei ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen (Art. 6 Abs. 3 Satz 4 DSGVO). Diese Anforderungen sind erfüllt.

(3.2.) Die Verarbeitung der personenbezogenen Daten des Klägers im Zusammenhang mit der Erstellung des Gutachtens war zur Erfüllung einer rechtlichen Verpflichtung im Sinne von Art. 6 Abs. 1 Satz 1 Buchstabe c DSGVO erforderlich. Gemäß § 275 Abs. 1 Satz 1 Nr. 3 Buchstabe b SGB V sind die Krankenkassen in den gesetzlich

bestimmten Fällen oder wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, verpflichtet, bei Arbeitsunfähigkeit zur Beseitigung von Zweifeln an der Arbeitsunfähigkeit eine gutachtliche Stellungnahme des N. Dienstes einzuholen. Diese Voraussetzungen sind gegeben, auch wenn ein Beispielsfall des § 275 Abs. 1a Satz 1 SGB V nicht vorliegt. Die Aufzählung ist nicht („insbesondere“) abschließend (Berchtold/Huster/Rehborn, Gesundheitsrecht, 2. Aufl. 2018, § 275 SGBV Rn. 26). Für die Ausfüllung des Begriffs der Erforderlichkeit der Einholung einer gutachtlichen Stellungnahme des N. Dienstes der Krankenkasse dienen als Handlungsdirektiven sowohl die Optimierung der Leistungsgewährung als auch die Prüfung der Leistungsvoraussetzungen (Becker/Kingreen, SGB V, Gesetzliche Krankenversicherung, 6. Aufl. 2018 § 275 Rn. 7). Der Kläger war hier seit dem 22.11.2017 ununterbrochen arbeitsunfähig erkrankt. Er bezog ab dem 24.05.2018 Krankengeld. Es ist mithin der Aspekt der „Dauer der Arbeitsunfähigkeit“ gemäß § 275 Abs. 1 Satz 1 SGB V angesprochen. Es ist nicht zu beanstanden, wenn die Krankenkasse dann zeitnah (vgl. § 275 Abs. 1a Satz 2 SGB V) zur Prüfung der Leistungsvoraussetzungen den N. Dienst der Krankenkasse einschaltet.

(3.3.) Die Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten des Klägers ist in § 276 Abs. 2 Satz 1 und Satz 3 SGB V festgelegt. Sie genügt den Anforderungen des Art. 6 Abs. 3 Sätze 2 und 4 DSGVO.

(3.3.1.) Der Medizinische Dienst darf nach § 276 Abs. 2 Satz 1 SGB V Sozialdaten erheben und speichern, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen nach § 275 SGB V bis 275d SGB V erforderlich ist. Die rechtmäßig erhobenen und gespeicherten Sozialdaten dürfen nach § 276 Abs. 2 Satz 3 SGB V nur für die in § 275 SGB V genannten Zwecke verarbeitet oder genutzt werden, für andere Zwecke, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist. Sozialdaten sind nach § 67 Abs. 2 Satz 1 SGB X personenbezogene Daten (Art. 4 Nr. 1 DSGVO), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Zu den in § 35 SGB I genannten Stellen gehört auch der Medizinische Dienst, und zwar bislang als Arbeitsgemeinschaft der Leistungsträger i.S.v. § 35 Abs. 1 Satz 4 SGB I (§ 278 Abs. 1 Satz 1 SGB V i.d.F. bis zum 31.12.2019) und seit dem 01.01.2020 als im Sozialgesetzbuch genannte öffentlich-rechtliche Vereinigung (§ 278 Abs. 1 Satz 1 SGB V i.d.F. ab dem 01.01.2020, wonach der Medizinische Dienst keine Arbeitsgemeinschaft mehr ist sondern als Körperschaft des öffentlichen Rechts errichtet ist). Personenbezogene Daten sind nach Art. 4 Nr. 1 Halbsatz 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

(3.3.2) § 276 Abs. 2 Sätze 1 und 3 SGB V genügen den Anforderungen des Art. 6 Abs. 3 Sätze 2 und Satz 4 DS-GVO. Sie legen mit den Prüfungen, Beratungen und gutachtlichen Stellungnahmen nach § 275 SGB V den Zweck der Verarbeitung fest. Dabei handelt es sich um ein im öffentlichen Interesse liegendes Ziel. Die Vorschriften stehen auch in einem angemessenen Verhältnis zu diesem Zweck. Sie erlauben die Erhebung und Speicherung personenbezogener Daten nur, soweit dies für diesen

Zweck erforderlich ist, und die Verarbeitung und Nutzung personenbezogener Daten nur bei rechtmäßiger Erhebung und Speicherung für die in § 275 SGB V genannten Zwecke oder für andere Zwecke, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist.

(3.4.) Die Verarbeitung der Daten des Klägers im Zusammenhang mit der Gutachtenerstellung durch den Beklagten im Auftrag seiner Krankenkasse erfüllt die Voraussetzungen von § 276 Abs. 2 Sätze 1 und 3 SGB V.

(3.4.1.) Der Beklagte hat die personenbezogenen Daten des Klägers für eine gutachtliche Stellungnahme nach § 275 Abs. 1 Satz 1 Nr. 3 Buchstabe b SGB V erhoben und gespeichert. Dafür war die Datenerhebung und -speicherung erforderlich. Erforderlich ist eine Erhebung von Sozialdaten, wenn ohne die Erhebung die entsprechende Aufgabenstellung nicht verwirklicht werden kann (jurisPK-SGB V/Strack 3. Aufl. § 276 Rn. 13). So liegt es hier. Ohne die Erhebung und Speicherung der Daten hätte die gutachtliche Stellungnahme nicht erstellt werden können. Eine Einwilligung des Klägers für die Ermittlung der Angaben durch den diesen behandelnden Arzt ist nicht erforderlich (Becker/Kingreen a.a.O. § 276 Rn. 4). Dies steht mit Art. 6 DSGVO in Einklang, weil die Datenerhebung gemäß Art. 6 Abs. 1 Satz 1 Buchstabe c DSGVO ohne Einwilligung des Betroffenen rechtmäßig ist.

(3.4.2.) Entgegen der Ansicht des Klägers durfte der Beklagte sich durch Frau Dr. I. telefonisch an den diesen behandelnden Arzt wenden und diesen zum Zwecke der Gutachtenerstellung um Auskunft bitten. Rechtsgrundlage ist § 276 Abs. 2 Satz 2 SGB V. Haben die Krankenkassen oder der Medizinische Dienst für eine gutachtliche Stellungnahme oder Prüfung nach § 275 Abs. 1 bis Abs. 3 SGB V erforderliche versichertenbezogene Daten bei den Leistungserbringern angefordert, so sind die Leistungserbringer nach dieser Vorschrift verpflichtet, diese Daten unmittelbar an den N. Dienst zu übermitteln. Das vom Kläger herangezogene Umschlagsverfahren hat mit der Frage eines Anrufs von Frau I. unmittelbar bei dem behandelnden Arzt nichts zu tun. Es ist richtig, dass das Umschlagsverfahren nicht mehr zulässig ist. Dies betraf allerdings die Problematik, dass die Krankenkassen für den N. Dienst bei den Leistungserbringern Unterlagen anfordern konnten. Insoweit war nicht sichergestellt, dass die Daten den Krankenkassen und nicht nur dem N. Dienst bekannt wurden (vgl. dazu Becker/Kingreen a.a.O. § 276 Rn. 6; Heberlein in BeckOK Sozialrecht, Rolfs/Giesen/Kreikebohm/Udsching, 55. Edition 01.12.2019, § 276 SGB V Rn. 68 ff.). Darum geht es hier nicht. Gemäß § § 276 Abs. 2 Satz 2 SGB V hat dann, wenn die Anfrage vom N. Dienst kommt (aber auch von der Krankenkasse, worum es hier nicht geht), der Leistungserbringer, d.h. der behandelnde Arzt (vgl. dazu Heberlein in BeckOK Sozialrecht a.a.O. § 276 SGB V Rn. 53) die Daten unmittelbar an den N. Dienst zu übermitteln. Genauso ist es hier gewesen. Frau Dr. I. hat für den Beklagten als Medizinischem Dienst die Daten zum Zwecke der Gutachtenerstellung betreffend die Arbeitsunfähigkeit des Klägers gemäß § 275 Abs. 1 SGB V unmittelbar erfragt und dieser hat sie unmittelbar an den Beklagten als medizinischem Dienst telefonisch mitgeteilt, d.h. übermittelt. Zu der Form der Übermittlung enthält § 276 Abs. 2 Satz 2 SGV

keine inhaltlichen Anforderungen und schließt eine unmittelbare telefonische Übermittlung nicht aus. Es mag zwar sein, dass regelmäßig Behandlungsunterlagen überlassen werden (Becker/Kingreen, a.a.O. § 276 Rn. 6 „idR“; Heberlein in BeckOK Sozialrecht a.a.O. § 276 SGB V Rn. 84: „Regelmäßig werden die Daten an die üblichen schriftlichen Unterlagen gebunden sein“). Dies bedeutet aber nicht, dass nicht im Einzelfall die mündliche telefonische Auskunft ausreichend sein kann. Entscheidend ist, dass die Pflicht zur Übermittlung von Informationen sich auf jene erstreckt, die zur sachgerechten Erledigung des Gutachtenauftrags erforderlich sind (Heberlein in BeckOK Sozialrecht a.a.O. § 276 SGB V Rn. 84). Insoweit kann es für den Gutachtenzweck ausreichend sein, wenn angesichts des Sachverhalts eine kurze telefonische Nachfrage bei dem behandelnden Arzt ausreicht. Wenn dies zur Überzeugung der Gutachterin ausreicht, um den Zweck der Begutachtung zu erfüllen, ist kein Grund ersichtlich, etwaige Unterlagen schriftlich anzufordern. Dies hat auch im Interesse des Versicherten Vorteile, weil einfache Zweifelsfälle wie hier zeitnah und zügig beantwortet werden können. Der Anruf der Gutachterin bei dem behandelnden Arzt erfolgte am 21.06.2018. Das Gutachten wurde nur einen Tag später am 22.06.2018 erstellt mit dem Ergebnis, dass auf Zeit Arbeitsunfähigkeit besteht, mithin etwaige Zweifel ausgeräumt waren. Die rein hypothetische Möglichkeit, dass ein Arzt entgegen seiner ärztlichen Verpflichtung andere und nicht zum Gutachten gehörende Fragen stellt, führt nicht dazu, die telefonische Auskunft in einfachen Fällen zu verbieten, zumal der Inhalt des Telefonats - wie auch geschehen - zu dokumentieren ist. Für dieses Ergebnis spricht weiter, dass die Übermittlungspflicht des Leistungserbringers an das Erheben der Daten durch den medizinischen Dienst anknüpft, welche als angeforderte Daten zu übermitteln sind. Das Erheben von Daten ist indes weit zu verstehen (§ 67 Abs. 1 SGB X i.V.m. Art. 4 Nr. 2 DSGVO). Und letztlich kann man § 276 Abs. 2 Satz 2 SGB V als gesetzliche Regelung verstehen, die eine Auskunftspflicht des Arztes i.S.v. § 100 Abs. 1 Satz 1 Nr. 1 SGB X begründet (vgl. auch Becker/Kingreen a.a.O. § 276 Rn. 6). Eine Auskunft muss nicht schriftlich erfolgen.

(3.5) Der Beklagte durfte die personenbezogenen Daten erheben und speichern, obwohl er Arbeitgeber des Klägers ist. Dies folgt im Umkehrschluss aus § 35 Abs. 1 Satz 3 SGB I. Danach dürfen Sozialdaten der Beschäftigten und ihrer Angehörigen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden. Diese Verpflichtung setzt voraus, dass Sozialdaten der Beschäftigten überhaupt erhoben und gespeichert werden dürfen.

(3.6.) Die rechtmäßig erhobenen und gespeicherten personenbezogenen Daten des Klägers sind nur für die in § 275 SGB V genannten Zwecke verarbeitet oder genutzt worden. Sie sind zur Erstellung der gutachtlichen Stellungnahme vom 22.06.2018 verwandt worden.

(3.7.) Die Verarbeitung der personenbezogenen Daten des Klägers genügte der spezifischen Bestimmung des § 276 Abs. 2 Satz 7 SGB V.

…

(3.7.1.) Nach dieser Vorschrift ist durch technische und organisatorische Maßnahmen sicherzustellen, dass die Sozialdaten nur den Personen zugänglich sind, die sie zur Erfüllung ihrer Aufgaben benötigen. Dies ist eine spezifische Bestimmung zum Schutz des Sozialgeheimnisses, das die Verpflichtung umfasst, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden (§ 35 Abs. 1 Satz 2 SGB I und für den Beklagten i.V.m. § 35 Abs. 1 Satz 4 SGB I). Diese Verpflichtung verlangt eine mitarbeiterbezogene Betrachtung. Der Medizinische Dienst der Krankenkasse ist keine datenschutzrechtliche „Kompetenzeinheit“, sondern mitarbeiterbezogen differenziert zu betrachten (vgl. Krauskopf/Pewestorf, Soziale Krankenversicherung, Stand September 2019, § 97 SGB XI Rn. 32 zum Bereich der Daten in der Pflegeversicherung). § 35 Abs. 1 Satz 3 SGB I bestimmt als konkrete Ausgestaltung dieser Verpflichtung (Gutzler in BeckOK Sozialrecht a.a.O. § 35 SGB I Rn. 33) ergänzend, dass die Sozialdaten der Beschäftigten und ihrer Angehörigen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden dürfen.

(3.7.2.) Diesen Anforderungen genügt der Beklagte. Die personenbezogenen Daten waren nur Personen zugänglich, die sie zur Erfüllung ihrer Aufgaben benötigten. Es ist richtig, dass der Kläger gerügt hat, dass die Anfrage zu dem Gutachten nicht unmittelbar im geschützten Bereich eingegangen ist. Der Gutachtenauftrag ging bei dem Beklagten auf postalischem Weg ein und wurde vom zuständigen Sachbearbeiter unmittelbar händisch dem geschützten Bereich zugeordnet. Dies ist ein zur Aufgabenerfüllung notwendiger Vorgang. Die Bearbeitung des Gutachtens innerhalb des geschützten Bereichs erfolgte sodann mit dem System Ismed 3. Hierauf konnte nicht beliebig zugegriffen werden, sondern erforderlich war ein entsprechendes Zugriffsrecht, das durch den Einsatz eines Softwarezertifikats erfolgte (Ziffern 6 und 7 DV Ismed 3). Die Zugriffsrechte wurden dabei über die Vergabe von Rechten und Rollen festgelegt. Ausweislich des Rollenkonzepts zu Ismed 3 spiegelte sich die Summe verschiedener Einzelrechte dabei in den Rollen wieder. Es gab zunächst die berufsgruppenbezogene Rollen. Dadurch wird sichergestellt, dass jede Berufsgruppe nur auf die Daten zugreifen kann, welche sie für ihre berufungsgruppenspezifischen Aufgaben benötigt. So kann z.B. eine Verwaltungskraft für Assistenzkräfte Aufträge anlegen, Unterlagen erfassen, Gutachten bearbeiten und weiterleiten. Ein Gutachter erstellt zugewiesene Gutachten. Er verfügt zusätzlich über die Gutachterfunktion, welche die Freigabeberechtigung für Gutachten erteilt. Daneben gibt es eine standortbezogene Berechtigung. Hierbei gab es für die Bearbeitung von Gutachten von Mitarbeitern und ihren Angehörigen den virtuellen Standort „Spezialfall“. Auf die personenbezogenen Daten im Zusammenhang mit der Erstellung und Speicherung des Gutachtens des Klägers konnten nur die 36 Mitarbeiter des geschützten Bereichs, d.h. derjenigen Arbeitsorganisation, welche für die Bearbeitung der Gutachten von Mitarbeitern und ihren Angehörigen zuständig war, zugreifen. Richtig ist, dass es keine weitere interne örtliche Aufspaltung der Berechtigung bei den 36 Mitarbeitern des geschützten Bereichs gab, denn es gab nur einen virtuellen Bereich „Spezialfall“. Dies bedeutet aber nicht,

dass innerhalb des Bereichs „Spezialfall“ alle 36 Mitarbeiter auf alle Daten Zugriff hatten. Dies erfolgte durch die berufsgruppenspezifische Rolle. Jeder Mitarbeiter des geschützten Bereichs hatte nur im Rahmen der jeweiligen Aufgabe, die er als Berufsgruppe ausführen musste, Zugriff. Richtig ist, dass das Rollenkonzept selbst darüber hinaus keine weitere Unterteilung innerhalb des geschützten Bereichs vorsieht. Allerdings war die Zugriffsberechtigung noch einmal entsprechend von Ziffer 3.2 DA Sozialdaten i.V.m. dem Zugriffskonzept aufgeteilt. Dies genügt zur Überzeugung der Kammer. Es ist allerdings richtig, dass der Bereich der IT Abteilung im geschützten Bereich ein einheitlicher ist und unstreitig für den gesamten geschützten Bereich zuständig ist. Genau dies rügt der Kläger. Aufgrund der Aufgabenstellung der IT-Mitarbeiter konnten diese - wie der Zugriff durch Frau T. belegt - auf die gesamten Daten des geschützten Bereichs und damit auch auf das Gutachten des Klägers zugreifen. Diese grundsätzliche Zugriffsmöglichkeit auf den gesamten Datenbestand des geschützten Bereichs ist aber für die Aufgabenerfüllung als IT-Abteilung erforderlich. Der Beklagte hat insoweit zur Überzeugung der Kammer ausreichende organisatorische Maßnahmen i.S.v. § 276 Abs. 2 Satz 7 SGB V ergriffen. Einerseits werden die Beschäftigten des Beklagten auf das Sozialgeheimnis verpflichtet und entsprechend belehrt und geschult. Die Wahrung des Sozialgeheimnisses bedeutet auch innerhalb des Beklagten, dass die Sozialdaten nur Befugten zugänglich sind (§ 35 Abs. 1 Satz 2 i.V.m. Satz 4 SGB I). Außerdem hat der Beklagte die DA Sozialdaten erlassen, die in Ziffer 3.2 vorsieht, dass zugriffsberechtigt nur die Mitarbeiter sind, die aufgrund ihrer arbeitsvertraglichen Tätigkeit von den Sozialdaten Kenntnis erlangen. Die Zugriffsberechtigten wiederum dürfen gemäß Ziffer 4 Abs. 2 DA die Sozialdaten nur zu den überlassenen Verarbeitungszwecken verwenden. Damit ist für jeden IT-Mitarbeiter klar, dass er auf die Sozialdaten innerhalb des geschützten Bereichs zwar zugreifen kann, er dies aber nur dann tun darf, wenn dies zur arbeitsvertraglichen Tätigkeit erforderlich ist. Ein bloßer Zugriff aus reiner Neugier oder einem anderen nicht aufgabenbezogenen Grund ist nicht erlaubt und durch das Sozialgeheimnis und die DA Sozialdaten verboten. Der Umstand, dass es sich bei den anderen IT-Mitarbeitern um Kollegen des Klägers handelt sowie, dass er als IT-Mitarbeiter auch für Frau Dr. I. zuständig ist, ist eine Frage, die sich im Rahmen der Prüfung von Art. 9 DSGVO stellt. Personen, die Personalentscheidungen treffen oder daran mitwirken können, waren die hier in Rede stehenden Daten des Klägers nicht zugänglich.

(4) Zur Überzeugung der Kammer sind betreffend die Datenverarbeitung zu dem Gutachten des Klägers auch die besonderen Anforderungen, welche Art. 9 DSGVO an die Verarbeitung von Gesundheitsdaten stellt, erfüllt. Gerade hier setzt die Berufung des Klägers an. Er weist zu Recht auf die besondere Schutzbedürftigkeit der hier verarbeiteten Gesundheitsdaten hin, welche im Hinblick auf die Aspekte der Erforderlichkeit und Verhältnismäßigkeit besondere Anforderungen verlangen. Dies ist im Grundsatz richtig. Diese besonderen Anforderungen sind im konkreten Fall erfüllt.

(4.1) Art. 9 DSGVO enthält für die in Art. 9 Abs. 1 DSGVO genannten personenbezogenen Daten ein Verbot der Verarbeitung mit Erlaubnisvorbehalt in den in Art. 9 Abs. 2 und 3 DSGVO genannten Fällen. Hinzu kommt, dass die Mitgliedstaaten gemäß Art.

9 Abs. 4 DSGVO auch für Gesundheitsdaten zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten können. Bei den hier in Rede stehenden Daten des Klägers handelt es sich um Gesundheitsdaten. Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen (Art. 4 Nr. 15 DSGVO). Diese Kategorie von Daten ist hier betroffen, denn wie der Inhalt des Gutachtens belegt, geht es um die Bestätigung einer bestimmt bezeichneten Diagnose, der Angabe der dafür verwandten Informationen sowie das Ergebnis nämlich die Beurteilung der Arbeitsunfähigkeit aus medizinischer Sicht.

(4.2.) Die Verarbeitung der hier in Rede stehenden Gesundheitsdaten sind auf der Grundlage von Art. 9 Abs. 2 Buchstabe b DSGVO i.V.m. Art. 9 Abs. 2 Buchstabe h DSGVO rechtmäßig. Die beiden Vorschriften überschneiden sich zur Überzeugung der Kammer und sind jedenfalls im hier konkreten Fall der gutachtlichen Feststellung der Arbeitsunfähigkeit durch einen medizinischen Dienst der Krankenkasse kumulativ anzuwenden.

(4.2.1.) Gemäß Art. 9 Abs. 2 Buchstabe b DSGVO ist die Verarbeitung der Gesundheitsdaten zulässig, wenn sie erforderlich ist, damit der Verantwortliche die ihr aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen kann. Dies gilt dann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist. Das Recht der sozialen Sicherheit und des Sozialschutzes erfasst insbesondere die Erbringung von Sozialleistungen und damit auch dasjenige der gesetzlichen Krankenversicherung (HK-DS-GVO/BDSG/Jaspers/Schwartmann/Mühenbeck a.a.O. Art. 9 DS-GVO Rn. 125; Wedde in Däubler/Wedde/Weichert/Sommer a.a.O. Art. 9 DSGVO Rn. 68). Dies erfasst den hier in Rede stehenden Fall, wo es um die Überprüfung der Voraussetzungen für den Bezug von Krankengeld, nämlich die Arbeitsunfähigkeit durch den Beklagten als Medizinischem Dienst im Auftrag der Krankenkasse des Klägers geht. Inhaltlich enthält Art. 9 Abs. 2 Buchstabe b DSGVO zwei Voraussetzungen. Zum einen muss die Verarbeitung der Gesundheitsdaten im Sinne dieser Bestimmung erforderlich sein. Zum anderen bedarf es einer - hier - mitgliedstaatlichen Bestimmung, welche die Verarbeitung zulässt und die zugleich die besonderen Anforderungen in Form von geeigneten Garantien für Grundrechte und die Interessen der betroffenen Person vorsieht.

(4.2.2.) In Art. 9 Abs. 2 Buchstabe h DSGVO wird die Regelung von Art. 9 Abs. 2 Buchstabe b DSGVO in Bezug auf den Gesundheitsbereich bekräftigt (Weichert in Kühling/Buchner, DS-GVO, BDSG, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 60). Gerade betreffend die Gesundheitsdaten überschneiden sich beide Bestimmungen (Wedde in Däubler/Wedde/Weichert/Sommer a.a.O. Art. 9 DSGVO Rn. 68). Die Verarbeitung für

die Beurteilung der Arbeitsfähigkeit des Beschäftigten ist hier ausdrücklich angesprochen. Unerheblich ist insoweit, dass die Begutachtung hier die Frage der Arbeitsunfähigkeit als Leistungsvoraussetzung betrifft. Der Begriff der Arbeitsfähigkeit ist umfassend, d.h. auch im negativen Sinn zu verstehen. Die Beurteilung der Arbeitsfähigkeit bezieht sich nicht nur auf ein etwaiges Rechtsverhältnis zum Arbeitgeber, sondern erfasst auch dasjenige zum Sozialleistungsträger. Dies belegt der Gesamtzusammenhang des Ausnahmetatbestandes. Genannt ist auch die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich ebenso wie die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich. Erfasst sind insoweit auch die gesetzlichen Krankenkassen einschließlich des medizinischen Dienstes (Wedde in Däubler/Wedde/Weichert/Sommer a.a.O. Art. 9 DSGVO Rn. 124). Und von der ebenfalls genannten Arbeitsmedizin wird auch der Datenaustausch zwischen Sozialversicherungsträgern erfasst (Weichert in Kühling/Buchner, DS-GVO, BDSG, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 113 a.E.). Genannt ist in Art. 9 Abs. 2 Buchstabe h DSGVO auch die hier ebenfalls betroffene medizinische Diagnostik. Auch Art. 9 Abs. 2 Buchstabe h DSGVO verlangt eine - hier - mitgliedstaatliche Bestimmung, als Grundlage für die Verarbeitung und die entsprechende Erforderlichkeit. Artikel 9 Absatz 3 DSGVO schränkt den sehr weit gesteckten Tatbestand in personeller Hinsicht ein, indem der Umgang mit den sensiblen Daten allein (nach dem Unionsrecht oder dem Recht der Mitgliedstaaten) einem dem Berufsgeheimnis oder einer sonstigen Geheimhaltungspflicht unterliegenden Fachpersonal gestattet wird. Dies ist ein Beispiel für eine „geeignete Garantie“ bzw. „angemessene Maßnahme“, wie sie auch in anderen Zulässigkeitstatbeständen vorausgesetzt sind (Albers/Veit in BeckOK Datenschutzrecht a.a.O. Art. 9 DSGVO Rn. 80).

(4.2.3.) Die Vorschriften von Art. 9 Abs. 2 Buchstaben b und h DSGVO sind jedenfalls für den hier zu beurteilenden Fall der Überprüfung der Arbeitsunfähigkeit innerhalb eines Systems der sozialen Sicherheit kumulativ zu erfüllen. Dafür spricht, dass Art. 9 Abs. 2 Buchstabe b DSGVO innerhalb von Art. 9 Abs. 2 DSGVO die grundlegenden Anforderungen an die Verarbeitung der besonders sensiblen Daten innerhalb der des Rechts der sozialen Sicherheit regelt. Für besondere und spezifische Bereiche enthält dann überschneidend Art. 9 Abs. 2 Buchstabe h DSGVO gesonderte Anforderungen mit der besonderen Anforderung, die aus Art. 9 Abs. 3 DSGVO resultiert. Es ist nicht ersichtlich, dass die mitgliedschaftliche Regelung in dem Fall, der eine solche besondere Sicherung vorsieht, nicht zugleich den Anforderungen des Art. 9 Abs. 2 Buchstabe b DSGVO genügen soll, d.h. allgemein geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen muss. Dass mit Art. 9 Abs. 3 DSGVO bereits eine solche Garantie geregelt ist, ist dabei zu berücksichtigen.

(4.3.) Die Anforderungen, die Art. 9 Abs. 2 Buchstabe b und h DSGVO i.V.m. Art. 9 Abs. 3 DSGVO und i.V.m. den mitgliedstaatlichen Bestimmungen (Art. 9 Abs. 4 DSGVO) aufstellen, sind erfüllt.

(4.3.1.) Die Datenverarbeitung ist zunächst erforderlich im Sinne von Art. 9 Abs. 2 Buchstabe b DSGVO. Mit der Erforderlichkeit für die Erfüllung von Pflichten aus dem

Recht der sozialen Sicherheit und des Sozialschutzes sind insbesondere die Erbringung und Abrechnung von Sozialleistungen und die in diesem Kontext notwendigen Daten angesprochen (Albers/Veit in BeckOK Datenschutzrecht a.a.O. Art. 9 DSGVO Rn. 54). Die Begutachtung der Arbeitsunfähigkeit des Klägers zum Zwecke der Überprüfung im Hinblick auf die Leistung des Krankengeldes war, wie ausgeführt, aufgrund der Länge der Arbeitsunfähigkeit erforderlich. Die damit verbundene Diagnostik und Datenverarbeitung war ebenfalls erforderlich, weil andernfalls die gutachtliche Stellungnahme nicht hätte erstellt und die Voraussetzungen des Leistungsbezugs nicht hätten überprüft werden können.

(4.3.2) Es liegen mitgliedstaatliche Regelungen vor, welche die Verarbeitung der hier in Rede stehenden Gesundheitsdaten im Zusammenhang mit der Gutachtenerstellung betreffend die Arbeitsunfähigkeit des Klägers erlauben. Dies sind die bei der Prüfung im Rahmen von Art. 6 DSGVO genannten Vorschriften der § 275 Abs. 1 Satz 1 Nr. 3 Buchstabe b SGB V, § 276 Abs. 2 Sätze 1, 3 und 7 SGB V. Auf die diesbezüglichen obigen Ausführungen zu Art. 6 DSGVO wird Bezug genommen.

(4.3.3.) Die Voraussetzungen von Art. 9 Abs. 3 DSGVO sind erfüllt. Die Verarbeitung der Daten muss danach von Fachpersonal erfolgen, das nach dem Recht eines Mitgliedstaates oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt oder wenn die Verarbeitung nach dem Recht des Mitgliedstaates oder den Vorschriften zuständiger Stellen einer Geheimhaltungspflicht unterliegt. Dies ist zunächst für die Ärztin Dr. I. der Fall. Sie unterliegt der ärztlichen Schweigepflicht, bei der es sich um ein Berufsgeheimnis i.S.v. Art. 9 Abs. 3 DSGVO handelt, denn diese ist zum einen strafrechtlich gemäß § 203 Abs. 1 Nr. 1 StGB abgesichert und außerdem in den Heilberufsordnungen der Ärzte (vgl. dazu § 9 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte) enthalten (Weichert in Kühling/Buchner a.a.O. Art. DS-GVO Rn. 139; HK-DS-GVO/BDSG/Jaspers/Schwartmann/Mühenbeck a.a.O. Art. 9 DS-GVO Rn. 206). Aber auch für die übrigen bei dem N. beteiligten Personen, die bei der Durchführung der gutachtlichen Stellungnahme beteiligt waren, sei es bei der ersten Zuordnung durch den ersten Sachbearbeiter zum geschützten Bereich, sei es durch Assistenzkräfte des geschützten Bereichs, ist die Anforderung des Art. 9 Abs. 3 DSGVO gewahrt. Diese Mitarbeiter unterliegen - wie ausgeführt - als solche des Beklagten als medizinischem Dienst der Krankenkassen dem Sozialgeheimnis, das auch innerhalb des N. Dienstes gilt. Das Sozialgeheimnis gemäß § 35 Abs. 1 SGB I ist entweder bereits Berufsgeheimnis i.S.v. Art. 9 Abs. 3 DSGVO (Weichert in Kühling/Buchner a.a.O. Art. 9 DS-GVO Rn. 142; HK-DS-GVO/BDSG/Jaspers/Schwartmann/Mühenbeck a.a.O. Art. 9 DS-GVO Rn. 206) oder eine sonstige Geheimhaltungspflicht i.S.v. Art. 9 Abs. 3 DSGVO.

(4.3.4.) Damit ist der Prüfungsauftrag, den Art. 9 Abs. 2 DSGVO dem Rechtsanwender aufgibt, nicht erschöpft. Wie ausgeführt, müssen die mitgliedstaatlichen Regelungen geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen (Art. 9 Abs. 2 Buchstabe b DSGVO). Außerdem kann der nationale

Gesetzgeber gemäß Art. 9 Abs. 4 DSGVO weitere Anforderungen aufstellen. Der deutsche Gesetzgeber hat dabei für den Bereich der Sozialdaten nicht nur spezifische Schutzregelungen erlassen, wie sie sich z.B. in § 276 Abs. 2 Satz 7 SGB V finden. Einstiegsnorm für die Erhebung von Sozialdaten ist § 67a Abs. 1 SGB X. Ganz allgemein ist danach die Datenerhebung zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem Sozialgesetzbuch - wie hier - erforderlich ist (§ 67a Abs. 1 Satz 1 SGB X). Als weitere Anforderung i.S. der von Art. 9 Abs. 2 Buchstabe b DSGVO verlangten Garantien bestimmt § 67 a Abs. 1 Satz 3 SGB X für die Erhebung von besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DSGVO die entsprechende Anwendung von § 22 Abs. 2 BDSG, der an Art. 32 Abs. 1 DSGVO anknüpft. Nach dieser Vorschrift sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, gehören dazu insbesondere die nachfolgend nicht abschließend aufgeführten Maßnahmen, wie z.B. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der DSGVO erfolgt (§ 22 Abs. 2 Satz 2 Nr. 1 BDSG), Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind (§ 22 Abs. 2 Satz 2 Nr. 2 BDSG), Sensibilisierung der an Verarbeitungsvorgängen Beteiligten (§ 22 Abs. 2 Satz 2 Nr. 3 BDSG), Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern (§ 22 Abs. 2 Satz 2 Nr. 5 BDSG), Pseudonymisierung personenbezogener Daten (§ 22 Abs. 2 Satz 2 Nr. 6 BDSG) und Verschlüsselung personenbezogener Daten (§ 22 Abs. 2 Satz 2 Nr. 7 BDSG). § 22 Abs. 2 BDSG ist flexibel ausgestaltet und gibt den Verantwortlichen einen (nicht abschließenden) Rahmen zur Orientierung (Albers/Veit in BeckOK Datenschutzrecht a.a.O. Art. 9 DSGVO Rn. 96; s.a. BAG 09.04.2019 - 1 ABR 51/17, juris Rn. 48), soweit nicht hier spezielle Anforderungen zu erfüllen sind. Die erkennende Kammer hat den Beklagten darauf mit Beschluss vom 25.09.2019 hingewiesen und ihm Gelegenheit zum Sachvortrag gegeben. Soweit - wie hier - die Erhebung der Sozialdaten nicht bei der betroffenen Person erfolgt, ist außerdem § 67a Abs. 2 Satz 2 SGB X zu beachten. Diese Anforderungen sind gewahrt.

(4.3.4.1.) Entgegen der Ansicht des Klägers ist es auch unter Würdigung dieser spezifischen Anforderungen nicht unzulässig, dass der Beklagte als Arbeitgeber des Klägers die Begutachtung durchführt. Ebenso wenig ist es unzulässig, dass dies durch Frau Dr. I. erfolgt, welche der Kläger als IT-Mitarbeiter auch zeitweise betreut. Ein solches Verbot lässt sich auch für Gesundheitsdaten, um die es hier geht, aus Art. 9 DSGV nicht ableiten. Der Kläger ist insgesamt der Ansicht, dass ein betriebliches Miteinander der Erhebung seiner Gesundheitsdaten entgegensteht. Dem folgt die erkennende Kammer nicht. Aus Art. 9 DSGVO lässt sich ein solch genereller Ansatz, wie der Kläger ihn vertritt, nicht herleiten. So ist in Art. 9 Abs. 2 Buchstabe h DSGVO z.B.

auch die Arbeitsmedizin genannt. Sie betrifft das Dreiecksverhältnis zwischen Arbeitgeber, Beschäftigtem und medizinischem Personal, d.h. insbesondere dem Betriebsarzt (Weichert in Kühling/Buchner a.a.O. Art. 9 DS-GVO Rn. 111; HK-DS-GVO/BDSG/Jaspers/Schwartmann/Mühenbeck a.a.O. Art. 9 DS-GVO Rn. 177). Ein Betriebsarzt muss kein betriebsfremder Dritter sein, sondern kann auch bei dem Arbeitgeber als Arbeitnehmer beschäftigt sein (vgl. § 2 Abs. 3 Satz 2 ASiG und BAG 24.03.1988 - 2 AZR 369/87, juris). Er kann mithin die im Betrieb beschäftigten Arbeitnehmer ebenso als „Kollegen“ kennen, ohne dass es ihm zugleich verboten ist, deren Gesundheitsdaten zu Erheben oder zur Kenntnis zu nehmen. Und auch der Betriebsrat, der ja aus „Kollegen“ besteht, kann Kenntnis von Gesundheitsdaten haben, vorausgesetzt, dass er zur Wahrung der Interessen der von der Datenverarbeitung betroffenen Arbeitnehmer angemessene und spezifische Schutzmaßnahmen i.S.v. § 22 Abs. 2 BDSG trifft (vgl. BAG 09.04.2019 - 1 ABR 51/17, juris Rn. 40). Diese sind hier zur Überzeugung der Kammer insgesamt ausreichend getroffen.

(4.3.4.2.) Dies betrifft zunächst den Aspekt, dass Kollegen Kenntnis von den Gesundheitsdaten erlangen können. Der Beklagte als medizinischer Dienst, bei dem - wie im Fall des Klägers - aufgrund der Anfrage durch dessen Krankenkasse Sozialdaten in Form von Gesundheitsdaten verarbeitet werden können, hat dieses Problem gesehen und durch die DA Sozialdaten darauf reagiert und eine innerbetriebliche organisatorische Maßnahme geschaffen, welche den Personenkreis einschränkt, der mit den Sozialdaten der eigenen Beschäftigten zu tun hat. Diese werden ganz generell nicht wie alle anderen Sozialdaten innerhalb des Beklagten bearbeitet, sondern dem geschützten Bereich, der Organisationseinheit „Spezialfall“ zugewiesen. Damit ist bereits eine organisatorische Angrenzung gegeben. Die Problematik dieses Falles zeichnet sich nun dadurch aus, dass der Kläger selbst einer der 36 Mitarbeiter des geschützten Bereichs ist. Auch dies ist in Ziffer 4 der DA Sozialdaten geregelt. Danach dürfen Beschäftigte grundsätzlich nicht an ihrem Beschäftigungsort begutachtet werden. Die Unterlagen dürfen dort nicht aufbewahrt werden und außerdem dürfen die Daten dort nicht gespeichert werden. Es erfolgt dann eine besondere Regelung für die Anwendung von Ismed3, die hier einschlägig ist. Für alle Mitarbeiter, die am Standort E. tätig sind, sind die benannten Mitarbeiter der Organisationseinheit „Spezialfall“ in E. zuständig. Für Mitarbeiter der übrigen Standorte sind die benannten Mitarbeiter der Organisationseinheit „Spezialfall“ in E. zuständig. Dies ist eine geografische Trennung, die eine gewisse „Distanz“ zwischen den Personen, die mit den Gesundheitsdaten befasst sind, schafft. Die Kammer verkennt nicht, dass der Kläger als IT-Mitarbeiter auch für den Standort E. zuständig ist und er als solcher auch einmal mit Frau Dr. I. zu tun hat. Dies ändert aber nichts daran, dass eine räumliche Distanz geschaffen ist, denn Frau Dr. I. hat ihren Beschäftigungsort räumlich in E. und der Kläger hat ihn in E.. Entgegen der Ansicht des Klägers war es nicht geboten, jede Begutachtung extern durch den Sozialmedizinischen Dienst der Knappschaft durchführen zu lassen. Richtig ist, dass dann, wenn eine körperliche Untersuchung erforderlich ist, die Begutachtung eines eigenen Beschäftigten des Beklagten gemäß Ziffer 5.5 DA Sozialdaten durch den Sozialmedizinischen Dienst der Knappschaft erfolgt. Diese Abstufung ist zur Überzeugung der Kammer vertretbar. Die körperliche Untersuchung eines Beschäftigten stellt

einen deutlich schwerwiegenderen Eingriff in die Persönlichkeitssphäre des Beschäftigten dar als eine Begutachtung nach Aktenlage. Diese Differenzierung ist nachvollziehbar und genügt den Anforderungen aus § 22 Abs. 2 BDSG.

(4.3.4.3.) Damit ist allerdings das grundlegende Problem, dass der Kläger IT-Mitarbeiter ist und auch die Kolleginnen und Kollegen der IT-Abteilung aus dem geschützten Bereich in das Gutachten Einsicht nehmen konnten, noch nicht gelöst. Im Rahmen von Art. 9 Abs. 2 DSGVO i.V.m. § 22 Abs. 2 BDSG gelten im Grundsatz vergleichbare Ausführungen wie zu Art. 6 DSGVO. Es liegen angemessene und spezifische Maßnahmen i.S.v. § 22 Abs. 2 BDSG vor. Ein Beispiel für eine solche Maßnahme ist - wie ausgeführt - das aus Art. 9 Abs. 3 DSGVO abgeleitete Gebot, dass nur dem Berufsgeheimnis unterliegendes Fachpersonal die Gesundheitsdaten verarbeiten darf. Dies ist hier aufgrund des Arzt- und Sozialgeheimnisses der Fall. Dies ist nicht ausreichend i.S.v. § 22 Abs. 2 BDSG, aber ein erster Einstieg, der innerhalb der Bewertung, ob der Beklagte angemessene und spezifische Maßnahmen getroffen hat, zu berücksichtigen ist. Die genannten Maßnahmen sind zur Überzeugung der Kammer ausreichend getroffen. Zunächst ist der Zugang innerhalb des Beklagten beschränkt (§ 22 Abs. 2 Satz 2 Nr. 5 BDSG). Dies erfolgt durch technische und organisatorische Maßnahmen (§ 22 Abs. 2 Satz 2 Nr. 1 BDSG). Die personenbezogenen Daten waren nur Personen zugänglich, die sie zur Erfüllung ihrer Aufgaben benötigten, was auch für den zuerst bearbeitenden Sachbearbeiter gilt, der den postalischen Auftrag der Krankenkasse händisch dem geschützten Bereich zugeordnet hat. Innerhalb des dann zur Bearbeitung benutzten Systems Ismed 3 konnte nicht beliebig zugegriffen werden, sondern erforderlich war ein entsprechendes Zugriffsrecht, das durch den Einsatz eines Softwarezertifikats erfolgte (Ziffern 6 und 7 DV Ismed 3). Die Zugriffsrechte wurden dabei über die Vergabe von Rechten und Rollen festgelegt. Ausweislich des Rollenkonzepts zu Ismed 3 spiegelte sich die Summe verschiedener Einzelrechte dabei in den Rollen wieder. Es gab zunächst die berufsgruppenbezogenen Rollen. Dadurch wird sichergestellt, dass jede Berufsgruppe nur auf die Daten zugreifen kann, welche sie für ihre berufungsgruppenspezifischen Aufgaben benötigt. So kann z.B. eine Verwaltungskraft für Assistenzkräfte Aufträge anlegen, Unterlagen erfassen, Gutachten bearbeiten und weiterleiten. Ein Gutachter erstellt zugewiesene Gutachten. Er verfügt zusätzlich über die Gutachterfunktion, welche die Freigabeberechtigung für Gutachten erteilt. Daneben gibt es eine standortbezogene Berechtigung. Hierbei gab es für die Bearbeitung von Gutachten von Mitarbeitern und ihren Angehörigen den virtuellen Standort „Spezialfall“. Auf die personenbezogenen Daten im Zusammenhang mit der Erstellung und Speicherung des Gutachtens des Klägers konnten nur die 36 Mitarbeiter des geschützten Bereichs, d.h. derjenigen Arbeitsorganisation, welche für die Bearbeitung der Gutachten von Mitarbeitern und ihren Angehörigen zuständig war, zugreifen. Richtig ist, dass es keine weitere interne örtliche Aufspaltung der Berechtigung bei den 36 Mitarbeitern des geschützten Bereichs gab, denn es gab nur einen virtuellen Bereich „Spezialfall“. Dies bedeutet aber nicht, dass innerhalb des Bereichs „Spezialfall“ alle 36 Mitarbeiter auf alle Daten Zugriff hatten. Dies erfolgte durch die berufsgruppenspezifische Rolle. Jeder Mitarbeiter des geschützten Bereichs hatte nur im Rahmen der jeweiligen Aufgabe, die er als Berufsgruppe ausführen musste, Zugriff. Richtig ist, dass

das Rollenkonzept selbst darüber hinaus keine weitere Unterteilung innerhalb des geschützten Bereichs vorsieht. Allerdings war die Zugriffsberechtigung noch einmal entsprechend von Ziffer 3.2 DA Sozialdaten i.V.m. dem Zugriffskonzept aufgeteilt. Dies genügt zur Überzeugung der Kammer. Es ist allerdings richtig, dass der Bereich der IT Abteilung im geschützten Bereich ein einheitlicher ist und unstreitig für den gesamten geschützten Bereich zuständig ist. Aufgrund der Aufgabenstellung der IT-Mitarbeiter konnten diese - wie der Zugriff durch Frau T. belegt - auf die gesamten Daten des geschützten Bereichs und damit auch auf das Gutachten des Klägers zugreifen. Diese grundsätzliche Zugriffsmöglichkeit auf den gesamten Datenbestand des geschützten Bereichs ist aber für die Aufgabenerfüllung als IT-Abteilung erforderlich. Der Beklagte hat insoweit zur Überzeugung der Kammer ausreichende organisatorische Maßnahmen nicht nur i.S.v. § 276 Abs. 2 Satz 7 SGB V, sondern auch i.S.v. § 22 Abs. 2 Satz 2 Nr. 1 BDSG ergriffen. Insoweit gilt nichts anderes als bereits oben ausgeführt. Die entsprechende Sensibilisierung gemäß § 22 Abs. 2 Satz 2 Nr. 3 BDSG erfolgte, weil die Beschäftigten des Beklagten auf das Sozialgeheimnis verpflichtet und entsprechend belehrt und geschult wurden. Die Wahrung des Sozialgeheimnisses bedeutet auch innerhalb des Beklagten, dass die Sozialdaten nur Befugten zugänglich sind (§ 35 Abs. 1 Satz 2 i.V.m. Satz 4 SGB I). Außerdem hat der Beklagte die DA Sozialdaten erlassen, die in Ziffer 3.2 vorsieht, dass zugriffsberechtigt nur die Mitarbeiter sind, die aufgrund ihrer arbeitsvertraglichen Tätigkeit von den Sozialdaten Kenntnis erlangen. Gemäß Ziffer 4 Abs. 2 DV Sozialdaten dürfen die Sozialdaten von den Zugriffsberechtigten nur zu den überlassenen Verarbeitungszwecken verwendet werden. Damit ist für jeden IT-Mitarbeiter klar, dass er auf die Sozialdaten innerhalb des geschützten Bereichs zwar zugreifen kann, er dies aber nur dann tun darf, wenn dies zur arbeitsvertraglichen Tätigkeit erforderlich ist. Ein bloßer Zugriff aus reiner Neugier oder einem anderen nicht aufgabenbezogenen Grund ist nicht erlaubt und durch das Sozialgeheimnis verboten. Auch insoweit gilt nichts anderes als bereits ausgeführt. Damit ist auch für jeden IT-Kollegen des Klägers klar, dass er nicht einfach außerhalb des Aufgabenbezugs auf die Gesundheitsdaten des Klägers zugreifen soll. Hinzu kommt weiter, dass im System Ismed 3 in Attributhistorie und in der Prozesshistorie protokolliert wird, wer welche Aktion an den personenbezogenen Daten durchführt (Ziffer 8 DV Ismed 3). Dies ist eine Maßnahme i.S.v. § 22 Abs. 2 Satz 2 Nr. 2 BDSG. Dies erklärt auch, warum der Beklagte über die Zugriffe auf die Datei mittels einer Auswertung nach Beteiligung des Innenrevisors und des Personalrats ermitteln konnte, wer auf das Gutachten des Klägers zugegriffen hat. Insgesamt genügt dies zur Überzeugung der Kammer, um einen ausreichenden Schutz i.S.v. § 22 Abs. 2 BDSG sicherzustellen, auch wenn berücksichtigt wird, dass gerade die IT-Kollegen technisch in das Gutachten Einsicht nehmen konnten. Es besteht kein Anhaltspunkt dafür, dass dies erfolgt wäre, wenn nicht der Kläger Frau T. darum gebeten hätte, in sein Gutachten zu schauen. Dass diese dies entgegen der klaren Regeln und unter Verstoß gegen das Sozialgeheimnis außerhalb ihres Aufgabenbezugs getan hätte, ist nicht ersichtlich. Andernfalls ist auch nicht zu erklären, warum der Kläger aus Sicht der Kammer zur Frage der Einsicht durch Frau T. zumindest irreführend vorgetragen hat. Die Verwendung des Passiv, nämlich dass er in einem Telefonat von einer im EDV-Bereich tätigen Person darauf hingewiesen worden sei, dass seine Gesundheitsdaten zumindest für ca.

10 Mitarbeiter einsehbar seien, hat bei der Kammer im Zusammenhang mit der Verwendung des Begriffs „whistleblower“ den Eindruck entstehen lassen, dass diese Person den Kläger von sich aus darauf hingewiesen hat. Die Kammer verkennt dabei nicht, dass der Vortrag so positiv nicht gehalten worden ist. Allerdings waren, wie ausgeführt, die Ausführungen des Klägers in den konkreten Formulierungen darauf angelegt, diesen falschen Eindruck entstehen zu lassen. Die Kammer hat in der letzten mündlichen Verhandlung offen gegenüber dem Kläger kommuniziert, dass sie von einem zumindest irreführenden Vortrag ausgeht. Dem ist der Kläger in der Sache nicht entgegengetreten, sondern hat sich - wie schon schriftsätzlich - darauf zurückgezogen, dass eine Einsichtnahme nie als haftungsbegründender Tatbestand vorgetragen wurde. Das ist richtig, ändert aber an dem irreführenden Vortrag nichts. Es ändert auch nichts daran, dass der dadurch entstandene Eindruck in der Gesamtwürdigung zu berücksichtigen ist. Der Vortrag des Klägers belegt, dass er selbst nicht davon ausgeht, dass eine Person ohne aufgabenbezogenen Anlass in seine Gesundheitsdaten sieht. Andernfalls hätte ohne weiteres der vollständige Sachverhalt vorgetragen werden können, nämlich dass er die Kollegin angerufen und sie ihm seine Vermutung auf seine Bitte hin bestätigt habe. Eine Namensnennung hätte genauso unterbleiben können wie bei dem im Prozess zunächst gehaltenen Vortrag. Richtig ist, dass es weiterhin möglich bleibt, dass auch ein IT-Kollege oder eine IT-Kollegin in die Datei mit dem Gutachten des Klägers Einsicht nimmt, weil ein entsprechender Aufgabenbezug gegeben ist, z.B. weil die Datei beschädigt ist und repariert werden muss. Dies muss zur Überzeugung der Kammer unter Würdigung des Sozialgeheimnisses aufgrund der Spezifika einer IT-Abteilung, die wie hier grundsätzlich Zugriff auf das gesamte IT-System haben muss, hingenommen werden. Im Übrigen ist auch unter Würdigung des Umstandes, dass Frau Dr. I. mal mit dem Kläger zu tun hatte, in keiner Weise ersichtlich oder auch nur zu befürchten, dass sie als Ärztin telefonisch unzulässige und weitergehende Fragen bei dem den Kläger behandelnden Arzt gestellt hat.

(4.3.5.) Die Gesundheitsdaten durften außerdem auch ohne Mitwirkung des Klägers bei seinem behandelnden Arzt als Leistungsträger i.S.v. § 35 Abs. 1 SGB I erhoben werden. Die Voraussetzungen des § 67a Abs. 2 Satz 2 Nr. 1 SGB X sind erfüllt. Der behandelnde Arzt war gemäß § 276 Abs. 2 Satz 2 SGB V zur Übermittlung befugt (§ 67 Abs. 2 Satz 2 Nr. 1 Buchstabe a SGB X). Die Erhebung der Daten bei dem Kläger wäre gemäß § 67 Abs. 2 Satz 2 Nr. 1 Buchstabe b SGB X mit einem unverhältnismäßigen Aufwand verbunden. Dies belegt der konkrete Fall. Die Daten zum Gesundheitszustand des Klägers waren bei dem behandelnden Arzt ohne weiteres vorhanden. Es bedurfte nur einer kurzen verfizierenden telefonischen Nachfrage, um die Arbeitsunfähigkeit - wie im Ergebnis geschehen - zu bestätigen. Die eigenständige neuerliche Untersuchung dann durch den Sozialmedizinischen Dienst der Knappschaft steht dazu außer Verhältnis. Es bestehen auch keine überwiegenden schutzwürdigen Interessen des Kläger, die beeinträchtigt werden (§ 67 Abs. 2 Satz 2 Nr. 1 Buchstabe c SGB X). Diese Regelung ist Teil der geeigneten Garantien für die Grundrechte und Interessen der betroffenen Personen i.S.v. Art. 9 Abs. 2 Buchstabe b DSGVO (BAG 09.04.2019 - 1 ABR 51/17, juris Rn. 28). Den Interessen des Klägers ist auch in diesem besonderen Fall durch die bereits beschrieben Maßnahmen gemäß § 22 Abs. 2 BDSG Rechnung

getragen, was bedeutet, dass überwiegende schutzwürdige Interessen des Klägers der konkreten Datenverarbeitung nicht entgegenstehen (vgl. dazu BAG 09.04.2019 a.a.O. Rn. 40 a.E.). Insgesamt ist im Übrigen auch der Aspekt der Datenminimierung (Art. 5 Abs. 1 Buchstabe c DSGVO) gewahrt. Es wurden nur die für die gutachtliche Stellungnahme erforderlichen Daten erhoben und verarbeitet. Mangels Datenschutzverstoß kam es auch nicht in Betracht, eine etwaige unwirksame Kündigung gegenüber dem Kläger oder die Androhung der Kündigung gegenüber Frau T. anspruchserhöhend zu berücksichtigen.

b) Dem Kläger steht weder ein Entschädigungsanspruch aus § 823 Abs. 1 BGB wegen der Verletzung seiner Gesundheit noch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG i.V.m. wegen Verletzung seines allgemeinen Persönlichkeitsrechts zu, weil es auch insoweit an einer dem Beklagten vorwerfbaren datenschutzrechtlichen Pflichtverletzung fehlt. Insoweit kann offen bleiben, ob die genannten Anspruchsgrundlagen überhaupt neben Art. 82 Abs. 1 DSGVO zur Anwendung kommen.

II. Der Kläger kann von dem Beklagten keinen Ersatz für den von ihm geltend gemachten materiellen Schaden verlangen. Die diesbezüglichen Klageanträge zu 2. und 4. sind zulässig aber unbegründet. Der Hilfsfeststellungsantrag zu 2. für die Zeit bis Oktober 2019 ist der Kammer nicht zur Entscheidung angefallen.

1. Die Klageanträge zu 2. und 4. sind zulässig.

a) Der Kläger als Berufungsführer konnte diese Anträge im Wege der Klageerweiterung im Rahmen seiner Berufung geltend machen. Die Voraussetzungen des § 533 ZPO sind gegeben. Der Beklagte hat sich in die zuletzt gestellten Anträge zu 2. und 4. in der mündlichen Verhandlung rügelos eingelassen. Unabhängig davon sind die Klageanträge zu 2. und 4. auch sachdienlich i.S.v. § 533 Nr. 1 ZPO. Sie betreffen mit dem materiellen Schadensersatz zwar einen anderen Streitgegenstand. Der Anspruch baut aber zumindest zum Teil auf dem gleichen Lebenssachverhalt auf, wie der Anspruch auf Entschädigung. Es geht in beiden Fällen um die angebliche vom Kläger geltend gemachte Datenschutzverletzung durch den Beklagten. Insoweit ist die Entscheidung auch über den materiellen Schadensersatzanspruch noch innerhalb dieses Verfahrens prozessökonomisch, weil ein Großteil des bisherigen Sach- und Streitstoffs verwertet werden kann. Unerheblich ist, dass der Streitstoff durch die Frage der Kausalität und damit ggfs. weiterer erforderlicher Feststellungen zur Frage des Zeitpunkts der Wiedergenesung des Klägers ohne den angeblichen Datenschutzverstoß erweitert wird. Dies steht der prozessökonomischen Verwertung des bisherigen Streitstoffs nicht entgegen. Die Voraussetzung des § 533 Nr. 2 ZPO ist gegeben, weil der Kläger die weiteren Tatsachen bereits in der Berufungsbegründung vorgetragen hat und diese dem Berufungsverfahren zu Grunde zu legen sind.

b) Der Klageantrag zu 2. ist als Zahlungsantrag ohne weiteres zulässig. Der Feststellungsantrag zu 4. für die Zeit ab November 2019 ist zulässig. Da die Schadensent-

wicklung noch nicht abgeschlossen ist, kann der Kläger in vollem Umfang die Feststellung der Ersatzpflicht gemäß § 256 Abs. 1 ZPO begehren (BGH 19.04.2016 - VI ZR 506/14, juris Rn. 6 m.w.N.). Insbesondere ist das Arbeitsverhältnis nicht bereits beendet. Der Kläger hat auf Nachfrage im Termin am 11.03.2020 mitgeteilt, dass er noch keinen Rentenantrag gestellt habe. Eine fortlaufende Anpassung des Feststellungsantrags an den Zahlungsantrag ist nicht erforderlich. Der Streitgegenstand, der dem Gericht zur Entscheidung gestellt ist, betrifft auch insoweit bei wertender Betrachtung einen einheitlichen Tatsachenkomplex, nämlich diejenigen Umstände, die bei „normaler“ Bearbeitungsweise des Gutachtenauftrags anfallen, d.h. von der Verteilung des Gutachtens an Frau Dr. I., der Durchführung des Gutachtens durch diese und die abschließende Speicherung des Gutachtens. Es handelt sich dabei um eine einheitliche Tätigkeit der Verarbeitung der personenbezogenen Daten des Klägers i.S.v. Art. 4 Nr. 2 DSGVO. Dieser einheitliche Lebenssachverhalt kann auch betreffend den materiellen Schaden nicht aufgespalten werden. Eine andere Frage ist, ob der Kläger den von ihm geltend gemachten Schaden haftungsbegründend auf alle Teilaspekte des Verarbeitungsvorgangs stützt.

2. Die Klageanträge zu 2. und 4. sind unbegründet. Der vom Kläger geltend gemachte materielle Schaden steht ihm weder aus Art. 82 Abs. 1 DSGVO noch aus § 823 Abs. 1 BGB wegen der Verletzung seiner Gesundheit noch aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG i.V.m. wegen Verletzung seines allgemeinen Persönlichkeitsrechts zu, weil es - wie zum Entschädigungsanspruch ausgeführt - an einer Pflichtverletzung des Beklagten in Form eines Datenschutzverstoßes fehlt. Unabhängig davon kommt ein materieller Schadensersatzanspruch, der sich auf die Speicherung des Gutachtens stützt, bereits deshalb nicht in Betracht, weil der Kläger insoweit nicht behauptet, dass diese haftungsbegründend für den materiellen Schaden ist. Daran ist die erkennende Kammer gebunden. Da es nach den Ausführungen zum Entschädigungsanspruch zur Überzeugung der Kammer an einem Datenschutzverstoß führt und außerdem der Kläger sich haftungsbegründenden für den materiellen Schaden nicht mehr auf die Speicherung des Gutachtens stützt, war eine Beweisaufnahme nicht mehr erforderlich. Einer förmlichen Aufhebung des Beweisbeschlusses vom 13.11.2019 bedurfte es nicht (BAG 25.10.2012 - 2 AZR 495/11, juris Rn. 36).

3. Der Hilfsfeststellungsantrag zu 2. für die Zeit bis Oktober 2019 einschließlich ist der Kammer nicht zur Entscheidung angefallen, weil er als Hilfsantrag nur für den nicht eingetretenen Fall der Unzulässigkeit des Leistungsantrags aufrechterhalten wurde. Als Hilfsantrag kam auch eine Auslegung als Zwischenfeststellungsantrag nicht in Betracht.

B. Die Kostenentscheidung beruht auf § 97 Abs. 1 ZPO. Gründe, dem Kläger über die Kostenentscheidung erster Instanz hinaus, bei der es bleibt, auch die erstinstanzlichen außergerichtlichen Kosten des Beklagten abweichend von § 12a Abs. 1 ArbGG aufzuerlegen, bestanden nicht.

C. Das Gericht hat die Revision gemäß § 72 Abs. 2 Nr. 1 ArbGG zugelassen.

…

RECHTSMITTELBELEHRUNG

Gegen dieses Urteil kann von der klagenden Partei

R E V I S I O N

eingelegt werden.

Für die beklagte Partei ist gegen dieses Urteil ein Rechtsmittel nicht gegeben.

Die Revision muss **innerhalb einer Notfrist* von einem Monat** schriftlich oder in elektronischer Form beim

Bundesarbeitsgericht
Hugo-Preuß-Platz 1
99084 Erfurt
Fax: 0361 2636-2000

eingelegt werden.

Die Notfrist beginnt mit der Zustellung des in vollständiger Form abgefassten Urteils, spätestens mit Ablauf von fünf Monaten nach der Verkündung.
Die Revisionsschrift **muss** von einem **Bevollmächtigten** unterzeichnet sein. Als **Bevollmächtigte** sind nur zugelassen:

1. Rechtsanwälte,
2. Gewerkschaften und Vereinigungen von Arbeitgebern sowie Zusammenschlüsse solcher Verbände für ihre Mitglieder oder für andere Verbände oder Zusammenschlüsse mit vergleichbarer Ausrichtung und deren Mitglieder,
3. Juristische Personen, deren Anteile sämtlich im wirtschaftlichen Eigentum einer der in Nummer 2 bezeichneten Organisationen stehen, wenn die juristische Person ausschließlich die Rechtsberatung und Prozessvertretung dieser Organisation und ihrer Mitglieder oder anderer Verbände oder Zusammenschlüsse mit vergleichbarer Ausrichtung und deren Mitglieder entsprechend deren Satzung durchführt, und wenn die Organisation für die Tätigkeit der Bevollmächtigten haftet.

In den Fällen der Ziffern 2 und 3 müssen die Personen, die die Revisionsschrift unterzeichnen, die Befähigung zum Richteramt haben.
Eine Partei, die als Bevollmächtigter zugelassen ist, kann sich selbst vertreten.

Die elektronische Form wird durch ein elektronisches Dokument gewahrt. Das elektronische Dokument muss für die Bearbeitung durch das Gericht geeignet und mit einer qualifizierten elektronischen Signatur der verantwortenden Person versehen sein oder von der verantwortenden Person signiert und auf einem sicheren Übermittlungsweg

…

gemäß § 46c ArbGG nach näherer Maßgabe der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (ERVV) v. 24. November 2017 in der jeweils geltenden Fassung eingereicht werden. Nähere Hinweise zum elektronischen Rechtsverkehr finden Sie auf der Internetseite des Bundesarbeitsgerichts www.bundesarbeitsgericht.de.

*** eine Notfrist ist unabänderlich und kann nicht verlängert werden.**

Dr. Gotthardt vom Brocke Bickhove-Swiderski

Beglaubigt
Urkundsbeamtin der Geschäftsstelle
Landesarbeitsgericht Düsseldorf

- maschinell erstellt, ohne Unterschrift gültig, § 169 Abs. 3 ZPO -