MEMO

Noerr LLP
Charlottenstraße 57
10117 Berlin
Deutschland

T +49 30 20942000
F +49 30 20942094
www.noerr.com

Alicante
Berlin
Bratislava
Brüssel
Budapest
Bukarest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moskau
München
New York
Prag
Warschau

Datum 04.07.2018

Von Dr. Torsten Kraul, LL.M.
Pascal Schumacher
Dr. Steffi Kindler

Betreff Rechtliche Prüfung der Nutzbarkeit der Cloud Speicher Lösung „Bdrive“ für Berufsgeheimnisträger gemessen an den Anforderungen des § 203 StGB sowie an denen des Datenschutzrechtes

A. Ergebnis

1. Einer Verwendung der Cloud Speicher Lösung „Bdrive“ durch Berufsgeheimnisträger stehen weder § 203 StGB noch datenschutzrechtliche Aspekte entgegen.

2. Die Nutzung des Tools „Bdrive“ durch Berufsgeheimnisträger unterfällt nicht dem Anwendungsbereich des Straftatbestandes des § 203 StGB. Dies ergibt sich unabhängig von der aufgrund der Neufassung der Vorschrift über § 203 Abs. 3 S. 2 StGB n.F. eröffneten Nutzungsmöglichkeit externer IT-Dienstleister und Cloud-Systeme auch für Berufsgeheimnisträger. Denn bei Nutzung des Tools „Bdrive“ werden den involvierten externen IT-Dienstleistern schon keine Daten der schweigepflichtigen Person offenbart. Des Abschlusses einer Verschwiegenheitsvereinbarung nach berufsrechtlichen Vorschriften wie § 43e BRAO bedarf es vor diesem Hintergrund ebenfalls nicht.

3. Das „BDrive“ sieht durch die immanente Verschlüsselung und Fragmentierung geeignete technische Maßnahmen vor, um ein angemessenes Schutzniveau auch für hochsensible Daten zu gewährleisten. Zudem werden die Datenschutz-

grundsätze wie etwa Datenminimierung vorbildlich umgesetzt. Aus der Perspektive der Bundesdruckerei und der weiteren am Cloud Storage Beteiligten sind die in „Bdrive“ gespeicherten Daten quasi anonym. Eine Einwilligung seiner Endkunden zur Speicherung von Personendaten in „Bdrive“ benötigt der Berufsgeheimnisträger nach richtiger Ansicht nicht - auch nicht im Fall sensibler Daten (bspw. Gesundheitsdaten). Soweit der Berufsgeheimnisträger in „Bdrive“ personenbezogene Daten über seine Endkunden (bspw. Mandanten, Patienten etc.) speichert, ist lediglich der Abschluss einer Standard-Vereinbarung über die Verarbeitung der Daten im Auftrag nach Art. 28 DS-GVO („**ADV**“) zwischen dem Berufsgeheimnisträger und der Bundesdruckerei erforderlich.

B. Sachverhalt

Die neXenio GmbH („**neXenio**“) entwickelt und vertreibt Software-Tools, die den Nutzern am digitalen Arbeitsplatz ein einfaches und sicheres Arbeiten ermöglichen. Im Auftrag der Bundesdruckerei hat neXenio das Softwaresystem „Bdrive“ entwickelt. Hierbei handelt es sich um eine Cloud Speicher-Lösung, die einen mobilen Datenzugriff und Datenaustausch auf höchstem Sicherheitsniveau zeitgleich zwischen mehreren Benutzern und Endgeräten ermöglicht. Betreiberin von „Bdrive“ ist die Bundesdruckerei.

Im Einzelnen funktioniert das Software Tool „Bdrive“ wie folgt:

Die zu speichernden Daten werden vor der Übertragung am Arbeitsplatz des Eigentümers verschlüsselt. Hierfür nutzt „Bdrive“ ein vom Bundesamt für Sicherheit und Informationstechnik empfohlenes asymmetrisches Verschlüsselungsverfahren. Die verschlüsselten Daten werden sodann mittels eines Erasure-Coding Verfahrens in mehrere Fragmente zerteilt, so dass nur eine Teilmenge der Fragmente für eine Wiederherstellung ausreichend ist. Die erzeugten Fragmente („Datenpäckchen“) werden anschließend auf mehrere unabhängige Cloud-Speicherdienste in Deutschland hochgeladen. Hierdurch wird sichergestellt, dass die Verfügbarkeit der verschlüsselten Daten unabhängig von der Verfügbarkeit der Cloud-Speicher-Anbieter ist und dass kein Cloud-Speicher-Anbieter in Besitz der vollständigen verschlüsselten Daten ist. Die Speicherung der verschlüsselten Datenfragmente erfolgt ausschließlich auf Servern in Deutschland.

Für die Wiederherstellung der Ursprungsform der Daten sowie den Datenaustausch zwischen Geräten und Nutzern werden in „Bdrive“ sog. Baupläne erstellt, zentral gespeichert und nur asymmetrisch mit Nutzerschlüssel verschlüsselt an die Bundesdruckerei übertragen. Alle hierfür benötigten IT-Komponenten (Server, Datenbanken) sind in speziell abgesicherten Bereichen innerhalb der D-Trust untergebracht. Zugang zu den Räumlichkeiten haben nur die Administratoren von „Bdrive“ nach dem Vier-Augen-Prinzip. Die von der Bundesdruckerei verwalteten Baupläne enthalten Informationen über die Fragmente der Dateien, die Verteilung der verschlüsselte Datenfragmente sowie kryptographische In-

formation zu deren Entschlüsselung. Die Baupläne enthalten hingegen keinerlei Informationen über den Inhalt der Daten und auch weder den Namen der Datei noch der Ordner und Unterordner, aus denen sich etwaige Rückschlüsse auf den Dateninhalt ableiten ließen. Überdies können die Baupläne von Dritten inklusive der Bundesdruckerei nicht gelesen werden. Der Eigentümer verschlüsselt die Baupläne explizit für die von ihm autorisierten Nutzer. So werden die Baupläne zum Teilen individuell für die autorisierten Nutzer mittels öffentlicher Schlüssel gesichert und können einzig mit den privaten Nutzerschlüsseln, welche zu keinem Zeitpunkt die Geräte verlassen, entschlüsselt werden. Einzig die vom Eigentümer autorisierten Nutzer sind in der Lage, den für sie bereit gestellten Bauplan mit ihrem privaten Schlüssel zu entschlüsseln, sich die einzelnen Datenfragmente abzurufen und wieder in die Ursprungsform zusammenzusetzen. Die über das „Bdrive"-Tool geteilten Dokumente sind mit einer digitalen Signatur versehen und ermöglichen dadurch die eindeutige Authentifizierung des Senders.

Die Verarbeitung der Daten findet bei Verwendung des „Bdrive"-Tools individuell auf dem Gerät eines jeden Nutzers statt. Ausgelagert in die Cloud ist nur die Datenspeicherung, wobei die Speicherung auf die zuvor beschriebene Weise in verschlüsselter und fragmentierter Form verteilt auf mehrere unabhängige Cloud-Speicherdienste erfolgt. Weder die Cloud-Speicher-Anbieter, auf deren Server die verschlüsselten Datenfragmente hochgeladen werden, noch die Bundesdruckerei oder neXenio können die Inhalte der gespeicherten Dateien und Datenfragmente lesen.

C. Prüfungsauftrag

Nexenio hat uns beauftragt, auf der Grundlage des vorstehenden Sachverhaltes zu prüfen, ob das Software Tool „Bdrive" auch von Berufsgeheimnisträgern (z.B. Ärzte, Steuerberater, Wirtschaftsprüfer, Rechtsanwälte) verwendet werden kann oder ob einer Verwendung durch diese Berufsgruppen § 203 StGB und/oder spezifische aus dem Datenschutzrecht folgende rechtliche Anforderungen entgegenstehen.

D. Rechtliche Würdigung

I. Verletzung von Privatgeheimnissen (§ 203 StGB)

Gemäß § 203 Abs. 1 StGB machen sich Träger solcher Berufe, denen der Einzelne Geheimnisse regelmäßig anvertrauen muss (sog. Berufsgeheimnisträger) strafbar, wenn sie unbefugt ein fremdes Geheimnis offenbaren, dass ihnen kraft ihrer Berufsausübung anvertraut oder sonst bekannt geworden ist. Zu den Berufsgeheimnisträgern gehören die in § 203 Abs. 1 Nr. 1 bis 7 StGB aufgeführten Berufsgruppen, u.a. Ärzte, Berufspsychologen, Rechtsanwälte, Steuerberater und Wirtschaftsprüfer.

1. Anwendungsbereich der Norm

Eine Nutzung des Tools „Bdrive“ käme für Berufsgeheimnisträgern folglich dann nicht in Betracht, wenn sie bei Anwendung von „Bdrive“ den für die Nutzung des Tools benötigten IT-Dienstleistern, namentlich den Cloud-Speicher-Anbietern, der Bundesdruckerei oder neXenio, berufsrechtlich zu wahrende fremde Geheimnisse „unbefugt offenbaren“ würden.

Das ist nicht der Fall:

a) Tatbestandsausschluss bei an der beruflichen oder dienstlichen Tätigkeit mitwirkenden Personen, § 203 Abs. 3 S. 2 StGB

Ein „unbefugtes Offenbaren“ scheidet im vorliegenden Fall bereits deshalb aus, weil die Vorschrift des § 203 StGB seit ihrer am 09.11.2017 in Kraft getretenen Neufassung einen ausdrücklichen Tatbestandsausschluss für die Offenbarung von Geheimnissen gegenüber den an der beruflichen oder dienstlichen Tätigkeit der schweigepflichtigen Person mitwirkenden Personen enthält, wobei – anders als bisher – interne Mitarbeiter und externe Dienstleister gleichgestellt sind.

Während § 203 Abs. 3 S.2 StGB a.F. den Tatbestandsausschluss lediglich in Bezug auf eine Geheimnisoffenbarung gegenüber den berufsmäßig tätigen Gehilfen des Berufsgeheimnisträgers (z.B. Sekretariatsmitarbeiter oder sonstiges Büropersonal) vorsah, dürfen Berufsgeheimnisträger gemäß § 203 Abs. 3 S. 2 StGB n.F. fremde Geheimnisse nunmehr auch

> *„(…) gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Person erforderlich ist; (…)“*

Zu den „sonstigen Personen“ zählen ausweislich der Gesetzesbegründung auch die Mitarbeiter von externen IT-Dienstleistern, die nach alter Rechtslage mit Berufsgeheimnissen nicht in Berührung kommen durften. Voraussetzung für die Offenbarungsbefugnis – und damit den Tatbestandsausschluss – ist nur noch, dass die betreffende Person an der beruflichen oder dienstlichen Tätigkeit der schweigepflichtigen Person mitwirkt, ohne dass sie in die Sphäre des Berufsgeheimnisträgers eingebunden sein muss (vgl. BT-Drs. 18/11936, S. 22). Hierbei sind gemäß § 203 Abs. 3 S. 2 Hs. 2 StGB n.F. auch mehrstufige Auftragsverhältnisse möglich.

Eine Mitwirkung in diesem Sinne liegt vor, wenn die betreffende Person unmittelbar mit der beruflichen Tätigkeit des Schweigepflichtigen, ihrer Vorbereitung, Durchführung, Auswertung und Verwaltung befasst ist. Als Beispiel nennt die Gesetzesbegründung u.a. die Bereitstellung von Systemen zur externen Speicherung von Daten und spricht damit explizit die Speicherung von Daten schweigepflichtiger Personen wie etwa Ärzte und Rechtsanwälte in sog. Cloud-Systemen an (vgl. BT-Drs. 18/11936, S. 22, s. auch *Kargl*, StV 2017, 482, 486).

Soweit § 203 Abs. 3 S.2 StGB n.F. fordert, dass die Offenbarung fremder Geheimnisse für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Person „erforderlich" sein muss, folgt hieraus allgemeiner Ansicht nach keine Begrenzung für die Inanspruchnahme externer Dienstleister. Dem Merkmal der Erforderlichkeit wird vielmehr eine rein symbolische Bedeutung beigemessen, mit der das Gesetz lediglich zum Ausdruck bringt, dass keine unnötige Offenbarung erfolgen darf (vgl. *Cierniak/Niehaus* in MünchKomm StGB, 3. Auflage, 2017, § 203 Rn. 138).

Bereits vor dem Hintergrund der Neureglung des § 203 StGB kann das Tool „Bdrive" ohne Weiteres auch von Berufsgeheimnisträgern genutzt werden.

b) Kein Offenbaren fremder Geheimnisse bei Nutzung von „Bdrive"

Ungeachtet der Neuregelung des § 203 StGB ist eine Nutzung des Tools „Bdrive" für Berufsgeheimnisträger aber auch deshalb unbedenklich, weil aufgrund des besonderen Funktionsmechanismus des Tools den involvierten IT-Dienstleistern fremde Geheimnisse schon nicht offenbart werden.

Offenbaren im Sinne des § 203 StGB ist jedes Mitteilen eines bestehenden Geheimnisses an einen Dritten. Die Offenbarung kann allgemeiner Ansicht nach auch in der Einräumung einer Zugangsmöglichkeit zu gespeicherten Daten bestehen. Ob eine inhaltliche Kenntnisnahme tatsächlich erfolgt, ist nicht relevant. Es muss jedoch die Möglichkeit einer inhaltlichen Kenntnisnahme der Daten gegeben sein; eine verschlüsselte oder anonymisierte Mitteilung reicht nicht aus (vgl. *Fischer*, StGB, 65. Auflage, § 203 Rn. 33 f. m.w.N.).

Bei Verwendung von „Bdrive" findet die Verarbeitung der Daten ausschließlich individuell auf dem Gerät des jeweiligen Nutzers statt. In die Cloud ausgelagert ist nur die Datenspeicherung. Anders als bei herkömmlichen Could-Speichersystemen wird durch den Speichervorgang den Cloud-Speicher-Anbietern aber gerade keine inhaltliche Zugriffsmöglichkeit auf die in der Cloud gespeicherten Daten verschafft. Denn vor dem Hochladen der Daten in die Cloud erfolgt auf dem Gerät des Eigentümers eine Verschlüsselung und

Fragmentierung der Daten. Die verschlüsselten Datenfragmente werden zudem auf verschiedene unabhängige Cloud-Speicherdienste verteilt. Infolge der Fragmentierung ist kein Cloud-Speicher-Anbieter im Besitz der vollständigen Ursprungsdatei. Aufgrund der zusätzlichen Verschlüsselung besteht auch in Bezug auf die in der Cloud gespeicherten Datenfragmente keine inhaltliche Zugriffsmöglichkeit durch die Mitarbeiter des Cloud-Speicher-Anbieters.

Ein inhaltlicher Datenzugriff ist allein über die von der Bundesdruckerei verwalteten Baupläne und die Verwendung eines vom Eigentümer der Datei autorisierten Nutzerschlüssel möglich. Die Baupläne enthalten selbst aber keine Informationen über den Inhalt der Ursprungsdatei und Datenfragmente oder sonstige Informationen, die Rückschlüsse auf den Inhalt der Ausgangsdaten ermöglichten. Der zur Wiederherstellung der Ursprungsform überdies notwendige Schlüssel liegt auf dem Gerät des autorisierten Nutzers. Aufgrund des besonderen Funktionsmechanismus von „Bdrive" können daher während des gesamten Vorgangs der Datenspeicherung und Datenübertragung die Inhalte der gespeicherten Dateien weder von den Cloud-Speicher-Anbietern, auf deren Server die verschlüsselten Datenfragmente hochgeladen werden, noch von der Bundesdruckerei oder von neXenio eingesehen und gelesen werden.

Die Nutzung von „Bdrive" führt daher nicht zu einer Offenbarung der Daten schweigepflichtiger Person gegenüber den für die Nutzung des Tools benötigten IT-Dienstleistern, so dass der Straftatbestand des § 203 StGB hier schon ungeachtet dessen entfällt, dass ein solches Offenbaren nach neuer Rechtslage gemäß § 203 Abs. 3 S. 2 StGB n.F. befugt wäre.

2. Ergebnis

Die Nutzung des Tools „Bdrive" durch Berufsgeheimnisträger unterfällt nicht dem Anwendungsbereich des Straftatbestandes des § 203 StGB. Dies ergibt sich unabhängig von der durch die Neufassung der Vorschrift über § 203 Abs. 3 S. 2 StGB eröffneten Nutzungsmöglichkeit externer IT-Dienstleister und Cloud-Systeme auch für Berufsgeheimnisträger, da den involvierten externen IT-Dienstleistern bei Verwendung des Tools fremde Geheimnisse schon nicht offenbart werden. Des Abschlusses einer Verschwiegenheitsvereinbarung nach berufsrechtlichen Vorschriften wie § 43e BRAO bedarf es vor diesem Hintergrund ebenfalls nicht.

II. Datenschutzrecht

Soweit der Berufsgeheimnisträger in „Bdrive" personenbezogene Daten über seine Endkunden (bspw. Mandanten, Patienten etc.) speichert (im Folgenden „Kundendaten"), findet die EU Datenschutz-Grundverordnung (DS-GVO) auf diesen Vorgang und die Beziehungen zur Bundesdruckerei grundsätzlich Anwendung.

1. Personenbeziehbarkeit der Daten

Die aus Sicht des Datenschutzrechts zentrale Frage ist, ob die Kundendaten einen direkten oder indirekten „Personenbezug“ aufweisen (Art. 4 Nr. 1 DS-GVO). Die Daten in „Bdrive“ so verschlüsselt und fragmentiert, dass weder die Bundesdruckerei noch andere Unterauftragnehmer noch andere Dritte ohne explizite Autorisierung durch den Berufsgeheimnisträger technisch in der Lage sind, Rückschlüsse auf den Inhalt der Daten zu ziehen. Das „BDrive“ sieht dadurch geeignete technische Maßnahmen vor, um ein angemessenes Schutzniveau zu gewährleisten auch für hochsensible Daten und Anwendungen zu gewährleisten. Zudem werden die Datenschutzgrundsätze wie etwa Datenminimierung vorbildlich umgesetzt. Aus der Perspektive der Bundesdruckerei und der weiteren am Cloud Storage Beteiligten sind die in „Bdrive“ gespeicherten Daten daher quasi anonym.

Für die Beurteilung der Frage, ob eine Personenbeziehbarkeit von Daten vorliegt, wählt das Europäische Datenschutzrecht allerdings eine andere Perspektive. Danach kommt es ausschlaggebend auf den Berufsgeheimnisträger und seine Möglichkeit an, die Daten in personalisierter Form wieder aus der Cloud abzurufen. Die Eigentümer und von ihnen autorisierte Nutzer sollen in „Bdrive“ in der Lage sein, den für sie bereitgestellten Bauplan mit ihrem privaten Schlüssel zu entschlüsseln, sich die einzelnen Datenfragmente abzurufen und wieder in die Ursprungsform zusammenzusetzen. In einem solchen Zusammenhang sind die Datenfragmente aus Sicht der Datenschutzbehörden weiterhin personenbeziehbar. Nur wenn selbst der Berufsgeheimnisträger nicht mehr in der Lage wäre, die Daten(-fragmente) wieder zu entschlüsseln und so wieder einer Person zuzuordnen, wäre von einem vollständig fehlenden Personenbezug auszugehen (vgl. nur BayLDA, TB 2002, Ziff. 4.6; LDA MV, Datenschutz im Krankenhaus, 2011, S. 33). Die einschlägigen Vorschriften der DS-GVO bringen insoweit gegenüber der bisherigen Rechtslage keine materiellen Änderungen mit sich. Die Erwägungsgründe bestätigen dies sogar (ErwG 26 ff.).

Damit ist zwar keine Aussage darüber verbunden, ob die Kundendaten auch für die Bundesdruckerei personenbeziehbar sind. Dies kann aber aus Sicht des Berufsgeheimnisträgers letztlich nicht maßgeblich sein. Für ihn kommt es allein darauf an, dass die Kundendaten für ihn selbst personenbezogen sind und damit jede Form der Verarbeitung dieser Daten (einschließlich ihrer Speicherung in „Bdrive“) einer datenschutzrechtlichen Rechtsgrundlage bedürfen.

2. Rechtsfolgen

Da die Bundesdruckerei die Datenspeicherung nicht aus eigenem Zweck sondern als Dienstleistung und für Zwecke des Berufsgeheimnisträgers durchführt, ist der Abschluss einer Standard-Vereinbarung über die Verarbeitung der Daten im Auftrag

nach Art. 28 DS-GVO zwischen dem Berufsgeheimnisträger und der Bundesdruckerei erforderlich. Die Pflicht hierzu trifft sowohl den Kunden als auch die Bundesdruckerei.

Bei einem Verstoß gegen die Pflicht zum Abschluss einer ADV kann sowohl gegen den Berufsgeheimnisträger als auch gegen die Bundesdruckerei ein Bußgeld in Höhe von EUR 10 Mio. oder (falls höher) 2% des gesamten weltweit erzielten Umsatzes verhängt werden.

Streitig, ob darüber hinaus – jedenfalls für sensible Daten wir Patientendaten – auch eine eigenständige Rechtsgrundlage im Sinne von Art. 6/9 DS-GVO notwendig ist (vgl. dazu Schmidt/Freund, ZD 2017, 14 ff.). Als solche käme regelmäßig nur eine Einwilligung der Endkunden in Betracht. Die besseren Argumente sprechen aber aus unserer Sicht dafür, dass keine separate Rechtsfertigungsbedürftigkeit für die Übermittlung an einen Auftragsverarbeiter besteht. Insbesondere gelten Auftragsverarbeiter nach Art. 4 Nr. 10 DS-GVO (wie bereits unter der alten Rechtslage) weiterhin nicht als Dritte im Verhältnis zum Verantwortlichen.

3. Ergebnis

Aus datenschutzrechtlicher Sicht ist die Nutzung des Tools „Bdrive“ durch Berufsgeheimnisträger grundsätzlich datenschutzkonform. Eine Einwilligung seiner Endkunden zur Speicherung von Personendaten in „Bdrive“ benötigt der Berufsgeheimnisträger daneben aber nach richtiger Ansicht nicht. Es ist lediglich der Abschluss einer Standard-Vereinbarung über die Verarbeitung der Daten im Auftrag nach Art. 28 DS-GVO zwischen dem Berufsgeheimnisträger und der Bundesdruckerei erforderlich.

* * * *