# MEMORANDUM

Noerr LLP
Charlottenstrasse 57
10117 Berlin
Germany

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

Alicante
Berlin
Bratislava
Brussels
Bucharest
Budapest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moscow
Munich
New York
Prague
Warsaw

Date 4 July 2018

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

Subject Legal review of usability of the Bdrive cloud storage solution for persons with a duty of professional secrecy measured against the requirements of section 203 German Criminal Code (*StGB*) and of data privacy law

## A. Result

1. The use of the Bdrive cloud storage solution by persons with a duty of professional secrecy is not prevented by section 203 German Criminal Code or by aspects of data privacy law.

2. The use of the Bdrive tool by persons with a duty of professional secrecy does not fall within the scope of the criminal offence of section 203 German Criminal Code. This results independently of the option of using external IT service providers and cloud systems based on the revised version of the regulation via section 203(3) second sentence German Criminal Code as amended for persons with a duty of professional secrecy. This is because when using the Bdrive tool, no confidential data is disclosed to the external IT service providers involved. No nondisclosure agreement under professional regulations such as section 43e of the Federal Regulations for Lawyers (*BRAO*) is required in this context either.

3. With its inherent encryption and fragmentation, Bdrive provides appropriate technical measures to guarantee an appropriate level of protection for highly sensitive data. In addition, the data protection principles such as data minimisation are perfectly implemented. From the perspective of Bundesdruckerei and the other parties involved in the cloud

storage, the data stored in Bdrive is virtually anonymous. Persons with a duty of professional secrecy do not require consent from their end customers for the storage of personal data in Bdrive, according to the correct opinion – not even in the case of sensitive data (e.g. health data). Insofar as persons with a duty of professional secrecy store personal data of their end customers (such as clients, patients, etc.) in Bdrive, only the conclusion of a standard data processing agreement is necessary under Article 28 GDPR between the person with a duty of professional secrecy and Bundesdruckerei.

## B. Facts

neXenio GmbH ("**neXenio**") develops and sells software tools which allow users to work simply and securely in the digital workplace. neXenio developed the Bdrive software system on behalf of Bundesdruckerei. It is a cloud storage solution which enables mobile data access and data exchange with the highest level of security between several users and terminals simultaneously. Bundesdruckerei is the operator of Bdrive.

In detail, the software tool Bdrive works as follows:

The data to be saved is encrypted before the transfer to the owner's workplace. To do so, Bdrive uses an asymmetrical encryption procedure recommended by the German Federal Office for Information Security. The encrypted data is then split into several fragments using an erasure coding procedure so that only a partial quantity of fragments is sufficient for restoration. The fragments generated ('data packets') are then uploaded to several independent cloud storage services in Germany. It is thus guaranteed that the availability of the encrypted data is independent of the availability of the cloud storage providers and that no cloud storage provider is in possession of the complete encrypted data. The encrypted data fragments are stored exclusively on servers in Germany.

In Bdrive, to restore the original form of the data as well as for data exchange between devices and users, blueprints are produced, stored centrally and only transferred to Bundesdruckerei asymmetrically with a user key. All IT components needed for this (server, databases) are accommodated in specially secured areas within the D-Trust. Only the administrators of Bdrive have access to the premises according to the principle of dual control. The blueprints administered by Bundesdruckerei contain information about the fragments of the files, the distribution of the encrypted data fragments as well as cryptographic information on their decoding. However, the blueprints contain no information whatsoever about the contents of the data and neither the name of the file nor the folder and subfolder from which any inferences could be made as to the data contents. In addition, the blueprints cannot be read by third parties including Bundesdruckerei. The owner encrypts the blueprints expressly for the users authorised by it. The blueprints are thus secured individually for the authorised users by means of public keys and can only be de-

crypted with the private user keys which at no time leave the devices. Only the users authorised by the owner are able to decrypt the blueprint provided for them with their private key, to call up the individual data fragments, and to reconstruct them into the original form. The documents shared via Bdrive tools are provided with a digital signature and thereby enable the clear authentication of the sender.

The processing of the data takes place individually on each user's device when using the Bdrive tool. Only the data storage is outsourced to the cloud, whereby storage takes place in the manner described above in an encrypted and fragmented form distributed to several independent cloud storage services. Neither the cloud storage providers to whose servers the encrypted data fragments are uploaded nor Bundesdruckerei or neXenio can read the contents of the stored files and data fragments.

## C. Our review

neXenio engaged us to review, on the basis of the aforementioned facts, whether the Bdrive software tool can also be used by persons with a duty of professional secrecy (e.g. doctors, tax accountants, auditors, lawyers) or whether use by these occupational groups is prevented by section 203 German Criminal Code and/or specific legal requirements arising from data privacy law.

## D. Legal assessment

### I. Violation of private secrets (section 203 German Criminal Code)

Pursuant to section 203(1) German Criminal Code, professionals to whom individuals often have to entrust secrets (known as persons with a duty of professional secrecy) shall be criminally liable if they unlawfully disclose a secret of another which was confided to or otherwise made known to them by virtue of their professional capacity. Persons with a duty of professional secrecy include the professions listed in section 203(1) no. 1 to no. 7 German Criminal Code, such as physicians, professional psychologists, lawyers, tax accountants and auditors.

#### 1. Scope of the regulation

Use of the Bdrive tool would therefore not come into consideration for persons with a duty of professional secrecy if, when using Bdrive, they were to 'unlawfully disclose' secrets of others which ought to be kept confidential under professional law to the IT service providers, namely the cloud storage providers, Bundesdruckerei or neXenio, as required for the use of the tool.

That is not the case:

a) **Persons participating in a professional or service activity are excluded from the offence, section 203(3)** second sentence **German Criminal Code**

'Unlawful disclosure' is already ruled out in this case because the provision of section 203 German Criminal Code, since its revised version which entered into force on 9 November 2017, contains an express exclusion from the offence for the disclosure of secrets to people participating in the professional or service activity of the person subject to confidentiality, whereby – unlike previously – internal employees and external service providers are treated as equivalent.

While the superseded version of section 203(3) second sentence German Criminal Code only referred to disclosure of secrets to the professionally active assistants of the persons with a duty of professional secrecy (e.g. secretarial staff or other office staff), persons with a duty of professional secrecy may now, pursuant to the new version of section 203(3) second sentence German Criminal Code, also disclose secrets of others

> '(...) *to other persons who participate in their professional or service activity insofar as this is necessary for the utilisation of the activity of the other participating person;* (...)'

The 'other persons' according to the explanatory memorandum also include the employees of external IT service providers who, according to the previous legal situation, were not allowed to come into contact with professional secrets. The condition for the authorisation to disclose – and thus the exclusion from fulfilling the elements of the offence – is now only that the relevant person participates in the professional or service activity of the person bound by confidentiality, without having to be integrated into the sphere of the person with a duty of professional secrecy (see Bundestag document 18/11936, p22). Pursuant to section 203(3) second half of second sentence German Criminal Code as amended, multi-level contract relationships are also possible in these cases.

Participation in this sense exists when the person in question deals directly with the professional activity of the person bound by confidentiality, being involved in preparing, carrying out, analysing and administering it. As an example, the explanatory memorandum mentions the provision of systems for external storage of data and thus expressly addresses the storage of data of persons bound by confidentiality such as physicians and lawyers in cloud systems (see Bundestag document 18/11936, p22; see also *Kargl*, StV 2017, 482, 486).

Insofar as section 203(3) second sentence German Criminal Code as amended requires that the disclosure of others' secrets be 'necessary' for the utilisation of the activity of the other participating person, according to the prevailing opinion no re-

striction on the utilisation of external service providers can be derived from this. The characteristic of necessity is instead attributed a purely symbolic meaning with which the law expresses only that no unnecessary disclosure may take place (see *Cierniak/Niehaus* in MünchKomm StGB, 3rd ed. 2017, § 203 para. 138).

Against the backdrop of the new provision of section 203 German Criminal Code, the Bdrive tool can easily be used by persons with a duty of professional secrecy too.

**b) Others' secrets are not disclosed when using Bdrive**

Notwithstanding the new provision of section 203 German Criminal Code, persons with a duty of professional secrecy can use the Bdrive tool without any concerns because due to the special functioning mechanism of the tool, others' secrets are not disclosed to the IT service providers involved anyway.

Disclosure within the meaning of section 203 German Criminal Code means any communication of an existing secret to a third party. In the prevailing opinion, disclosure can also consist of granting the opportunity for access to stored data. Whether note is actually taken of the content is not relevant. However, there must be a possibility of taking note of the content of the data; an encrypted or anonymised notification is not sufficient (see *Fischer*, StGB, 65th ed., § 203 para. 33 onwards with other evidence).

When Bdrive is used, the processing of the data takes place only individually on the device of each user. Only data storage is outsourced to the cloud. Unlike in conventional cloud storage systems, the storage procedure does not provide the cloud storage providers with any opportunity to access the content of the data stored in the cloud. Because before uploading the data into the cloud, encryption and fragmentation of the data take place on the owner's device. The encrypted data fragments are also distributed to different independent cloud storage services. As a result of the fragmentation, no cloud storage provider is in possession of the complete original file. Due to the additional encryption, the employees of the cloud storage provider have no access to the content of the data fragments stored in the cloud either.

Access to the content of data is solely possible via the blueprints administered by Bundesdruckerei and the use of an authorised user key from the owner of the file. However, the blueprints themselves contain no information about the content of the original file and data fragments or other information which would enable inferences to be made about the content of the output data. The additionally necessary key for restoring the original form is located on the authorised user's device. Due to the special functioning mechanism of Bdrive, during the entire process of data stor-

age and data transfer the contents of the stored files cannot be viewed or read by the cloud storage providers to whose servers the encrypted data fragments are uploaded, nor by Bundesdruckerei or neXenio.

Using Bdrive thus does not lead to a disclosure of the data of persons bound by confidentiality to the IT service providers required for the use of the tool, and therefore the criminal offence of section 203 German Criminal Code does not apply regardless of the fact that such disclosure would be lawful according to the new legal position under section 203(3) second sentence German Criminal Code as amended.

### 2. Result

The use of the Bdrive tool by persons with a duty of professional secrecy does not fall within the scope of the criminal offence of section 203 German Criminal Code. This results independently of the opportunity for persons with a duty of professional secrecy to use external IT service providers and cloud systems opened up by the revised version of the provision via section 203(3) second sentence German Criminal Code, since in any case no secrets of others are disclosed to the IT service providers involved in the use of the tool. No nondisclosure agreement under professional regulations such as section 43e of the Federal Regulations for Lawyers (BRAO) is required in this context either.

## II. Privacy law

If the persons with a duty of professional secrecy store personal data about their end customers (e.g. clients, patients, etc.) (hereinafter 'Customer Data') in Bdrive, the EU General Data Protection Regulation (GDPR) generally applies to this process and to the relations to Bundesdruckerei.

### 1. Personal identifier in data

The central question from the perspective of data privacy law is whether the Customer Data shows a direct or indirect identifier to an identifiable person (Article 4 no. 1 GDPR). The data in Bdrive is encrypted and fragmented such that neither Bundesdruckerei nor other subcontractors nor other third parties are technically able to make inferences about the content of the data without the express authorisation of the person with a duty of professional secrecy. Bdrive thus provides appropriate technical measures to guarantee an appropriate level of protection for highly sensitive data and applications too. In addition, the data privacy principles such as data minimisation are perfectly implemented. From the perspective of Bundesdruckerei and the other parties involved in the cloud storage, the data stored in Bdrive are thus virtually anonymous.

To judge whether data contains personal identifiers, European privacy law chooses a different perspective, however. According to it, it depends crucially on the person with a duty of professional secrecy and his or her opportunity to retrieve the data in a personalised form from the cloud. The owners and the users authorised by them should be able in Bdrive to decrypt the blueprint provided for them with their private key, to call up the individual data fragments, and to reconstruct them into the original form. In such a context the data fragments still contain personal references, from the perspective of the data privacy authorities. Only if the person with a duty of professional secrecy him or herself were no longer able to decrypt the data (fragments) and thus assign them to a person again would a complete lack of personal reference be assumed (see BayLDA, TB 2002, no. 4.6; LDA MV, *Datenschutz im Krankenhaus*, 2011, p33). The relevant provisions of the GDPR do not bring about any material changes compared to the legal position to date. The recitals even confirm this (recital 26 onwards).

This says nothing about whether the Customer Data contains personal identifiers accessible by the Bundesdruckerei as well. But from the perspective of the person with a duty of professional secrecy, this ultimately cannot be decisive. For that person, the only important thing is that the Customer Data has personal references accessible to him or her and thus any form of processing of this data (including its storage in Bdrive) requires a basis in data privacy law.

## 2. Legal consequences

Since Bundesdruckerei carries out the data storage not for its own purpose but as a service and for the purposes of the person with a duty of professional secrecy, the conclusion of a standard data processing agreement is necessary under Art. 28 GDPR between the person with a duty of professional secrecy and Bundesdruckerei. This obligation is incumbent on both the customer and Bundesdruckerei.

In the case of a breach of the obligation to enter into a data processing agreement, a fine of EUR 10 million or (if higher) 2% of total worldwide revenues can be imposed on both the person with a duty of professional secrecy and Bundesdruckerei.

It is debatable whether in addition – in any case for sensitive data such as patient data – a separate legal basis within the meaning of Art. 6/9 GDPR is necessary (see *Schmidt/Freund*, ZD 2017, 14 et seq.). Usually only the consent of the end customers would come into question as such. But from our perspective there are better arguments for saying that no separate justification is needed for transfer to a data processor. In particular, under Article 4 no. 10 GDPR (as in the old legal situation), processors still do not count as third parties in relation to the data controller.

## 3. Result

From a privacy law perspective, the use of the Bdrive tool by persons with a duty of professional secrecy generally complies with data privacy law. Persons with a duty of professional secrecy do not, however, additionally require consent from their end customers for the storage of personal data in Bdrive, according to the correct view. Only the conclusion of a standard data processing agreement is necessary under Article 28 GDPR between the person with a duty of professional secrecy and Bundesdruckerei.

* * * *