

## Rechtliche Begutachtung des Dienstes Notary's Desc

### Inhaltsverzeichnis

Inhaltsverzeichnis	1
<b>A. Beschreibung des Dienstes</b>	<b>1</b>
I. Verschlüsselter Dokumentenaustausch	2
a) Inhaltsverschlüsselung	2
b) Dokumentenaustausch mittels Client/Server-Struktur	3
II. Serverstandort	3
<b>B. Prüfungsauftrag</b>	<b>3</b>
<b>C. Zusammenfassung des Prüfungsergebnisses</b>	<b>4</b>
<b>D. Rechtliche Würdigung</b>	<b>4</b>
I. Strafrechtliche Bewertung	4
a) Strafbarkeit wegen § 203 StGB	4
b) Zwischenergebnis	5
II. Berufsrechtliche Bewertung	6
a) Anforderungen des Berufsrechts der Berufsträger	6
b) Zwischenergebnis	6
III. Datenschutzrechtliche Bewertung	6
a) Personenbezogene Daten	6
b) Auftragsverarbeitung	7
c) Kein eigenes Legitimationserfordernis für den Einsatz von Notary's Desc	8
d) Zwischenergebnis	8

### A. Beschreibung des Dienstes

Die Literacy GmbH (nachfolgend "Literacy") hat das Softwaresystem "Notary's Desc " entwickelt. Bei Notary's Desc handelt es sich um eine Software-as-a-Service-Anwendung, die Notare, Rechtsanwälte, Wirtschaftsprüfer und Steuerberater (nachfolgend: „Berufsträger“) bei

der Abwicklung des Beurkundungsprozesses unterstützt, indem Notary's Desc den elektronischen Austausch von vertraulichen Dokumenten zwischen den im M&A Prozess beteiligten Parteien ermöglicht.

## **I. Verschlüsselter Dokumentenaustausch**

Das System basiert auf dem Ende-zu-Ende verschlüsselten Austausch von Dokumenten zwischen den einzelnen autorisierten Nutzern. Die Dokumente können nur an zuvor autorisierte Nutzer versendet werden. Sämtliche zu versendenden Dokumente werden auf dem Gerät des sendenden Nutzers über eine Inhaltsverschlüsselung gesichert und erst wieder auf dem Gerät des empfangenden Nutzers entschlüsselt. Ein Zugriff von Literacy oder Dritten auf den Inhalt der Dokumente ist somit – im Gegensatz zum Versand per E-Mail – praktisch ausgeschlossen.

Nachfolgend wird das Prinzip der Inhaltsverschlüsselung der Dokumente (unter **a**) sowie die Funktionsweise des Dokumentenaustauschs (unter **b**) detailliert dargestellt. Die unter **a**) und **b**) dargestellten Maßnahmen werden nachfolgend zusammenfassend als „Datensicherheitsmaßnahmen“ bezeichnet.

### **a) Inhaltsverschlüsselung**

Die Inhaltsverschlüsselung der Dokumente wird mittels eines „asymmetrischen Verschlüsselungsverfahrens“ auf der Basis des X509-Standards unter Verwendung einer RSA-PSS-Verschlüsselung (Rivest-Shamir-Adleman-Probabilistic Signature Scheme) durchgeführt.

Bei einem solchen Verfahren besitzt jeder Nutzer zwei Schlüssel, also ein Schlüsselpaar: Einerseits hat jeder Nutzer einen „öffentliche Schlüssel“, der ausschließlich zur Verschlüsselung der für ihn bestimmten Dokumente dient, nicht aber zur Entschlüsselung verwendet werden kann. Daneben hat jeder Nutzer einen „privaten Schlüssel“, der zur Entschlüsselung an ihn versendeten Dokumenten dient. Wenn ein Dokument verschlüsselt werden soll, erhält der Versender den öffentlichen Schlüssel des Empfängers über eine von Literacy bereitgestellte Schnittstelle. Mit diesem Schlüssel sichert der Versender das Dokument. Erst auf dem Endgerät des Empfängers findet die Entschlüsselung der Dokumente mit Hilfe des privaten Schlüssels des Empfängers statt. Der private Schlüssel des Empfängers ist nur diesem bekannt. Ein auf diese Weise verschlüsseltes Dokument kann damit ausschließlich vom jeweiligen Empfänger, der den privaten Schlüssel des Dokuments kennt, entschlüsselt werden. Weder der Versender, der das Dokument verschlüsselt hat, noch Dritte können das Dokument selbst entschlüsseln. Damit ist die Kenntnisnahme Dritter vom Inhalt der versendeten Dokumente nach aktuellem technischen Stand praktisch ausgeschlossen.

## **b) Dokumentenaustausch mittels Client/Server-Struktur**

Für den Austausch der inhaltsverschlüsselten Dokumente ist von Notary's Desc der Austausch mittels einer Client/Server-Struktur vorgesehen:

Der Dokumentenaustausch mittels Notary's Desc erfolgt über einen Server auf den die einzelnen Arbeitsplätze (nachfolgend: „Clients“) zugreifen können. Clients können dabei über eine Schnittstelle Dokumente sowie Dokumentendaten auf den Server hoch- bzw. von diesem herunterladen. Sämtliche Dokumenten- und Adressinformationen (z.B. Titel oder Metadaten der Dokumente) werden hierbei bereits von dem Client des jeweiligen Nutzers in Zufallswerte ohne Bezug zum Inhalt des Dokuments oder zum Mandanten übersetzt. Hierdurch wird eine Pseudonymisierung dieser Daten erreicht. Danach werden inhaltsverschlüsselten Dokumente samt inhaltsverschlüsselter Dokumentdaten sowie die pseudonymisierten Informationen transportverschlüsselt an eine Schnittstelle von Literacy übertragen und dort auf dem Server gespeichert. Andere authentifizierte Clients können die verschlüsselten Informationen dann über diese Schnittstelle vom Server herunterladen.

Über diese Schnittstelle werden auch die öffentlichen Schlüssel, die zum Verschlüsseln der auszutauschenden Dokumente verwendet werden, verteilt.

Die Kommunikation mit der Schnittstelle erfolgt dabei ihrerseits transportverschlüsselt mithilfe des Secure-Sockets-Layer-Protokolls (nachfolgend: „SSL-Protokoll“). Die Authentifizierung an der Schnittstelle erfolgt mittels des OAuth2-Verfahrens. Die von der Schnittstelle abrufbaren pseudonymen bzw. verschlüsselten Informationen werden auf einer Datenbank seitens Literacy vorgehalten. Der Transport der Dokumente erfolgt mithin zweifach verschlüsselt.

## **II. Serverstandort**

Die Server, auf denen das System betrieben wird, werden von der Deutschen Telekom als Auftragsverarbeiter von Literacy betrieben. Der Serverstandort ist ausschließlich Deutschland.

### **B. Prüfungsauftrag**

Im Auftrag von Literacy war zu prüfen, ob – unter Zugrundelegung der von Literacy mitgeteilten Datensicherheitsmaßnahmen – der Einsatz von Notary's Desc durch Berufsträger ein strafbares Offenbaren von Privatgeheimnissen gegenüber Literacy im Sinne des § 203 Strafgesetzbuches (StGB) darstellt.

Daneben sollte untersucht werden, ob der Einsatz von Notary's Desc den jeweils einschlägigen besonderen berufsrechtlichen Voraussetzungen von § 43e der Bundesrechtsanwaltsordnung (BRAO) bzw. § 26a Bundesnotarordnung (BNotO), § 62a des Steuerberatergesetzes (StBerG) oder § 50a der Wirtschaftsprüferordnung (WPO) unterliegt.

Schließlich sollte zusammenfassend dargestellt werden, welche Anforderungen die Datenschutzgrundverordnung (DSGVO) an den Einsatz von Notary's Desc stellt.

### **C. Zusammenfassung des Prüfungsergebnisses**

Die Inanspruchnahme des Dienstes Notary's Desc durch Berufsträger stellt keine strafbare Verletzung von Privatgeheimnissen gemäß § 203 StGB dar. Aufgrund der Datensicherheitsmaßnahmen von Notary's Desc ist es weder Literacy noch Dritten möglich, Kenntnis von Privatgeheimnissen im Sinne von § 203 StGB zu nehmen. Ein strafbares Offenbaren gegenüber Literacy oder Dritten liegt damit nicht vor.

Daneben müssen Berufsträger bei Nutzung von Notary's Desc auch nicht die besonderen Anforderungen gemäß § 43e BRAO, § 26a BNotO, § 62a StBerG oder § 50a WPO erfüllen. Da bei Nutzung von Notary's Desc weder Literacy noch Dritten „Zugang zu Tatsachen, auf die sich die Verschwiegenheitsverpflichtung der Berufsträger bezieht“ eröffnet wird, stellt die Nutzung von Notary's Desc keine nach § 43e BRAO bzw. § 26a BNotO, § 62a StBerG oder § 50a WPO geregelte „Inanspruchnahme von Dienstleistungen“ dar.

Da die Inanspruchnahme von Notary's Desc eine weisungsgebundene Verarbeitung (pseudonymer) personenbezogener Daten durch Literacy darstellt, muss zwischen Literacy und dem Nutzer ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO geschlossen werden. Eine datenschutzrechtlichen Einwilligung der Mandanten in die Nutzung von Notary's Desc bedarf es hingegen nicht.

### **D. Rechtliche Würdigung**

#### **I. Strafrechtliche Bewertung**

##### **a) Strafbarkeit wegen § 203 StGB**

Ein Berufsträger macht sich gemäß § 203 StGB strafbar, wenn er ein *fremdes Geheimnis*, das ihm anvertraut worden ist, *unbefugt offenbart*.

Neben mandatsbezogenen Informationen stellt auch die Mandanteneigenschaft selbst für den Berufsträger *fremde Geheimnisse* (nachfolgend: „Berufsgeheimnisse“) dar. Als solche sind

nämlich sämtliche Tatsachen zu verstehen, die sich auf den Mandanten beziehen und nur einem begrenzten Personenkreis bekannt sind (vgl. *Weidemann* in: BeckOK StGB, § 203, Rn. 4.). Auch juristische Personen können Geheimnisträger sein, so dass auch Informationen, die beispielsweise Partnerschaftsgesellschaften anvertraut sind, von dem Tatbestand umfasst (vgl. *Eisele* in: Schönke/Schröder StGB, § 203, Rn. 8.).

*Offenbaren* bedeutet in diesem Zusammenhang, das Berufsgeheimnis einem Dritten mitzuteilen (vgl. *Weidemann* in: BeckOK StGB, § 203, Rn. 32). Für ein Offenbaren genügt es nach der Begründung des Gesetzgebers bereits, wenn einem Dritten die *Möglichkeit verschafft wird ein Berufsgeheimnis zur Kenntnis zu nehmen* (vgl. BT-Drs. 18/11936, S. 28.).

Durch die Datensicherheitsmaßnahmen wird die Möglichkeit der Kenntnisnahme Dritter unter Zugrundelegung des aktuellen Stands der Technik effektiv verhindert. Einerseits werden alle Dokumente, die mittels Notary's Desc ausgetauscht werden, mittels eines asymmetrischen Verschlüsselungsverfahrens Ende-zu-Ende verschlüsselt. Aufgrund des Funktionsmechanismus des asymmetrischen Verschlüsselungsverfahrens ist es auch Literacy als Anbieter nicht möglich, etwaige Berufsgeheimnisse zur Kenntnis zu nehmen. Da außer dem Empfänger des versendeten Dokuments niemand, insbesondere nicht Literacy zur Entschlüsselung der zu versendenden Dokumente in der Lage ist, bleiben Literacy sämtliche Informationen aus diesen Dokumenten vollständig verborgen.

Da aufgrund der Datensicherheitsmaßnahmen auch alle weiteren Informationen, die sich auf diese Dokumente beziehen (wie Titel oder Metadaten der Dokumente) auf dem Client des jeweiligen Nutzers softwareseitig durch pseudonyme Zufallswerte ersetzt wurden, bevor sie transportverschlüsselt an Literacy übertragen werden, kann Literacy auch von diesen Berufsgeheimnissen keine Kenntnis nehmen.

Selbst in dem (theoretischen) Fall, wenn ein Dritter unter Überwindung der Datensicherheitsmaßnahmen über den Dienst Kenntnis von dem Berufsgeheimnis unterliegende Informationen erlangen würde, käme eine Strafbarkeit des betroffenen Berufsträgers nicht in Betracht. Aufgrund der bestehenden Datensicherheitsmaßnahmen würde die Kenntnisnahme von diesen Informationen durch einen Dritten für diesen Dritten ein strafbares Ausspähen von Daten gemäß § 202a StGB darstellen. Wenn aber die Kenntnisnahme Dritter lediglich auf strafbarem Weg erfolgen kann, schließt dies eine Strafbarkeit des Berufsträgers gemäß § 203 StGB aus (vgl. hierzu nur *Cornelius* in: StV, 2016, S. 380, 387f.).

## **b) Zwischenergebnis**

Wegen der Nutzung von Notary's Desc kommt für den Berufsgeheimnisträger keine Strafbarkeit gemäß § 203 StGB in Betracht.

## **II. Berufsrechtliche Bewertung**

### **a) Anforderungen des Berufsrechts der Berufsträger**

Gemäß § 43a BRAO, § 18 BNotO, sowie § 57 Abs. 1 StBerG in Verbindung mit § 5 der Berufsordnung der Steuerberaterkammer (BOSTB) und § 43 WPO in Verbindung mit § 10 der Berufssatzung für Wirtschaftsprüfer/vereidigte Buchprüfer (BS WP/vBP) werden Berufsgeheimnisse von der Verschwiegenheitspflicht der Berufsträger erfasst.

Sofern einem Dienstleister *Zugang* zu solchen Berufsgeheimnissen *eröffnet* wird, hat der Berufsträger die besonderen Anforderungen von § 43e BRAO bzw. § 26a BNotO, § 62a StBerG oder § 50a WPO zu beachten. Beispielsweise ist dann eine vorherige Einwilligung von Mandanten bei einzelmandatsbezogener Inanspruchnahme einer Dienstleistung oder der Abschluss einer Verschwiegenheitsvereinbarung mit dem Dienstleister erforderlich.

Die Zugangseröffnung liegt, ebenso wie beim strafrechtlich relevanten *Offenbaren*, dann vor, wenn dem Dienstleister die *Möglichkeit zur Kenntnisnahme* eröffnet wird.

Aufgrund der bereits oben dargestellten Datensicherheitsmaßnahmen wird Literacy keine Möglichkeit gegeben, vom Inhalt des Berufsgeheimnisses Kenntnis zu nehmen. Der Berufsträger eröffnet Literacy damit keinen Zugang zu Berufsgeheimnissen.

### **b) Zwischenergebnis**

Die Nutzung von Notary's Desc stellt keine berufsrechtlich relevante Zugangseröffnung zu Berufsgeheimnissen dar. Besondere Anforderungen, wie beispielsweise eine vorherige Einwilligung von Mandanten bei einzelmandatsbezogener Inanspruchnahme von Dienstleistungen oder der Abschluss einer Verschwiegenheitsvereinbarung müssen daher vom Berufsträger bei der Nutzung von Notary's Desc nicht beachtet werden.

## **III. Datenschutzrechtliche Bewertung**

### **a) Personenbezogene Daten**

Die mittels Notary's Desc versendeten Dokumente werden regelmäßig personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO beinhalten. Hierbei handelt es sich um alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. In

Frage kommen hier also insbesondere Namen von Mandanten oder Mitarbeitern sowie alle mit diesen Personen verknüpften Informationen.

Der Personenbezug der Daten entfällt dann, wenn die Daten „anonym“, also nicht mehr auf eine natürliche Person beziehbar, sind. In diesem Fall wäre diese Verarbeitung nicht dem Regelungsregime der DSGVO unterworfen.

Anonymität im Sinne des Datenschutzrechts bestimmt sich nicht aus der „relativen“ Sicht eines einzelnen Beteiligten am Datenverarbeitungsvorgang, sondern immer „absolut“ aus der Sicht aller am Datenverarbeitungsvorgang Beteiligten. Anonymität liegt demgemäß nur dann vor, wenn niemand der am Datenverarbeitungsvorgang Beteiligten in der Lage ist, anhand eines gewissen Datums eine natürliche Person zu identifizieren (vergleichbar: *Helfrich/Forgó/Schneider* .in: Betrieblicher Datenschutz, Kap. 5, Rn. 22 m.w.N.). Zwar ist Literacy aufgrund der zuvor beschriebenen Datensicherheitsmaßnahmen nicht in der Lage, anhand der Daten natürliche Personen zu identifizieren. Denn Literacy ist nicht einmal in der Lage, vom Inhalt der verschlüsselten Daten überhaupt Kenntnis zu erlangen. Jedoch ist der rechtmäßige Empfänger der jeweiligen Dokumente technisch zur Entschlüsselung und damit zur Kenntnisnahme des Inhalts in der Lage. Aus datenschutzrechtlicher Sicht liegt damit eine bloße Pseudonymisierung gemäß Art. 4 Nr. 5 DSGVO vor, jedoch keine Anonymisierung der Daten. Bei bloß pseudonymen Daten liegt der Personenbezug im Sinne von Art. 4 Nr. 1 DSGVO vor, sodass die Anforderungen der DSGVO beachtet werden müssen.

## **b) Auftragsverarbeitung**

Literacy verarbeitet diese personenbezogenen Daten im Sinne von Art. 4 Nr. 2 DSGVO ausschließlich nach Weisung der jeweiligen Berufsträger, indem es die Daten über Server weitergibt und die hierzu erforderlichen Informationen bereitstellt. Literacy entscheidet aber selbst weder über Zwecke noch über Mittel der Verarbeitung. Dies geschieht einzig durch die Nutzer von Notary's Desc. Literacy wird gegenüber den Berufsträgern daher als Auftragsverarbeiter gemäß Art. 28 DSGVO tätig.

In diesem Zusammenhang ist zwischen Literacy und den Nutzern von Notary's Desc ein Auftragsverarbeitungsvertrag zu schließen. Hierin hat sich Literacy gegenüber den Nutzern zu verpflichten, sämtliche personenbezogenen Daten ausschließlich weisungsgemäß zu verarbeiten, insbesondere die Daten nicht zu eigenen Zwecken zu verarbeiten. Daneben muss sich Literacy gegenüber den Nutzern verpflichten, dass entsprechende technische und organisatorische Maßnahmen getroffen werden, um die Anforderungen der DSGVO betreffend den Schutz der Rechte betroffener Personen zu gewährleisten.

**c) Kein eigenes Legitimationserfordernis für den Einsatz von Notary's Desc**

Da Literacy die personenbezogenen Daten ausschließlich nach Weisung der Nutzer verarbeitet, handelt es sich bei Literacy nicht um einen Verantwortlichen im Sinne von Art. 4 Nr. 7 DSGVO. Daher besteht für den Einsatz von Notary's Desc kein Bedürfnis einer eigenständigen Legitimation der Datenverarbeitung. Es bedarf somit insbesondere keine Einwilligung der Mandanten wegen des Einsatzes von Notary's Desc.

**d) Zwischenergebnis**

Der Einsatz von Notary's Desc stellt eine Verarbeitung personenbezogener Daten durch Literacy im Auftrag des jeweiligen Berufsträgers dar. Bei Abschluss eines Auftragsvertrages zwischen dem Berufsträger und Literacy bedarf es für diese Datenverarbeitung keiner eigenständigen Legitimation mehr.

Stuttgart, den 21. April 2021



Dr. Carsten Ulbricht, M.C.L.  
- Rechtsanwalt -



Carlo Kunz  
- Rechtsanwalt -