

## MEMORANDUM

Datum 22.07.2020

Von Tobias Kugler  
Lars Powierski

Betreff **Datenschutz und Berufsrecht beim Einsatz von LEXolution.FLOW**

### 1 Sachverhalt

Die STP Informationstechnologie AG mit Sitz in Karlsruhe, Deutschland (im folgenden „STP“) entwickelt derzeit mit „LEXolution.FLOW“ eine cloudbasierte Workflow-Engine zu Unterstützung von rechtlichen Prüf-, Beratungs- und Entscheidungsprozessen in Rechtsanwaltskanzleien (im Folgenden die „Kunden“).

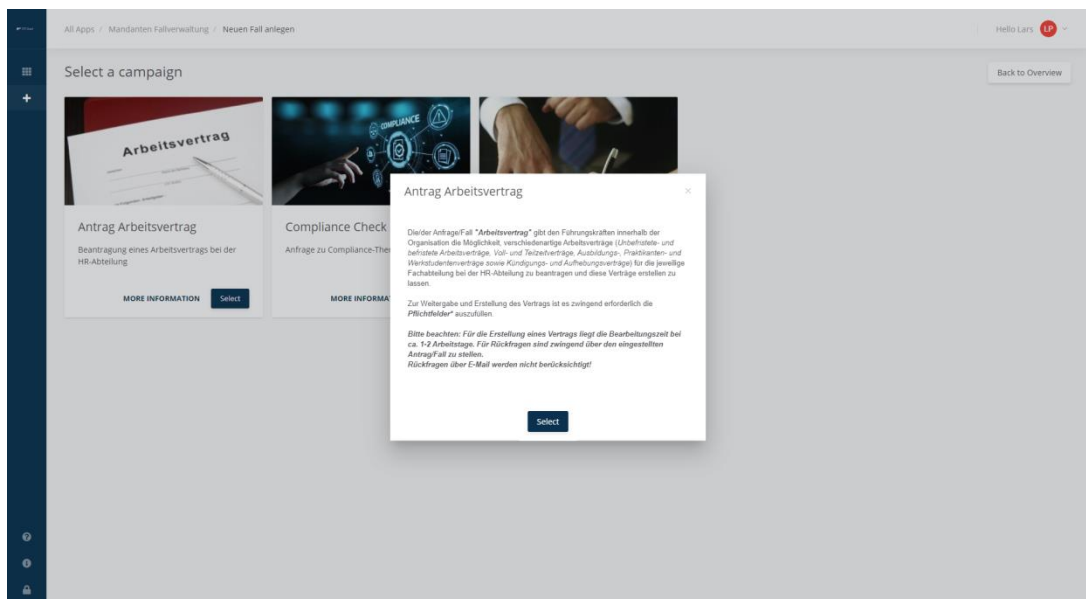
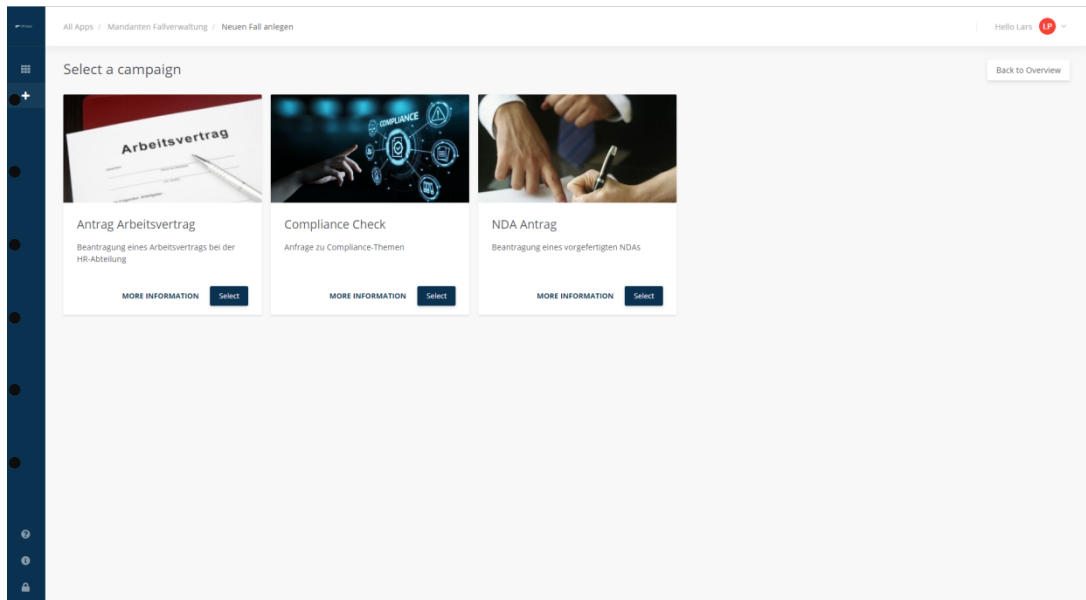
#### 1.1 Systemarchitektur

LEXolution.FLOW unterteilt sich funktional in das Mandantenportal und das Back-End:

##### 1.1.1 Mandantenportal

Im Mandantenportal kann der Kunde seinen Mandanten rechtsberatungsbezogene Services anbieten und die zur Erbringung dieser Services ggf. erforderliche Informationen mit den Mandanten austauschen. Die Mandanten können über das Mandantenportal die dort angebotenen Services auch direkt beauftragen und/oder Dateien hochladen, wenn der Kunde dies zulässt.

Die nachfolgenden Abbildungen zeigen exemplarisch einen Service zur Erstellung eines Arbeitsvertrages im Mandantenportal:



All Apps / Mandanten Fallverwaltung / Fall

Hello Lars LP

### Case LVD-UFU-6X7

**Familienstand\***

ledig  
 verheiratet  
 verwitwet  
 alleinerziehend  
 getrennt lebend  
 Nebenjobber

**Steuerklasse\***

Steuerklasse 1

**Steuer-ID\***

1,234,567

**Krankenkasse\***

test

**Sozialversicherungsnummer\***

87,986,754

**Bewerbungsunterlagen**

Drop files here to upload

Erlaubte Dateierweiterungen: Bilder, Audiodateien, Textdokumente

Back Save

GESELLSCHAFT  
VERTRAG  
ARBEITSVERHÄLTNIS  
▶ ARBEITNEHMER

All Apps / Mandanten Fallverwaltung / Ihre Fälle

Hello Lars LP

+ Create new case

### Your cases

**Antrag Arbeitsvertrag**

Client: Not specified  
 Created on: 19.02.2020  
 Case number: LVD-UFU-6X7  
 Status: Dokument

Show

Go to document area

**Next step:**

We will contact you as soon as possible!

## 1.1.2 Back-End

In dem Back-End von LEXolution.FLOW kann der Kunde mit unterschiedlichen Funktionalitäten, wie zum Beispiel einer Vorgangsverwaltung und einem Dokumentengenerator, die für die im Mandantenportal angebotenen Services erforderlichen Workflows modellieren, verwalten und automatisieren.

Die nachfolgenden Abbildungen zeigen exemplarisch einige der im Back-End zur Verfügung stehenden Funktionen:

STP Cloud All Apps Hello Lars

Welcome back, Lars!  
Today is Wednesday, 19 February 2020

- Customization
- Identity Admin
- Identity Provider
- Kampagnen Management
- Kanzlei Fallverwaltung
- Mandanten Fallverwaltung
- Tenant Admin
- User Management

Legal Notice  
Privacy Policy

STP Cloud Campaign overview + New campaign

Search  
Please enter a search term. Campaigns per page: 5

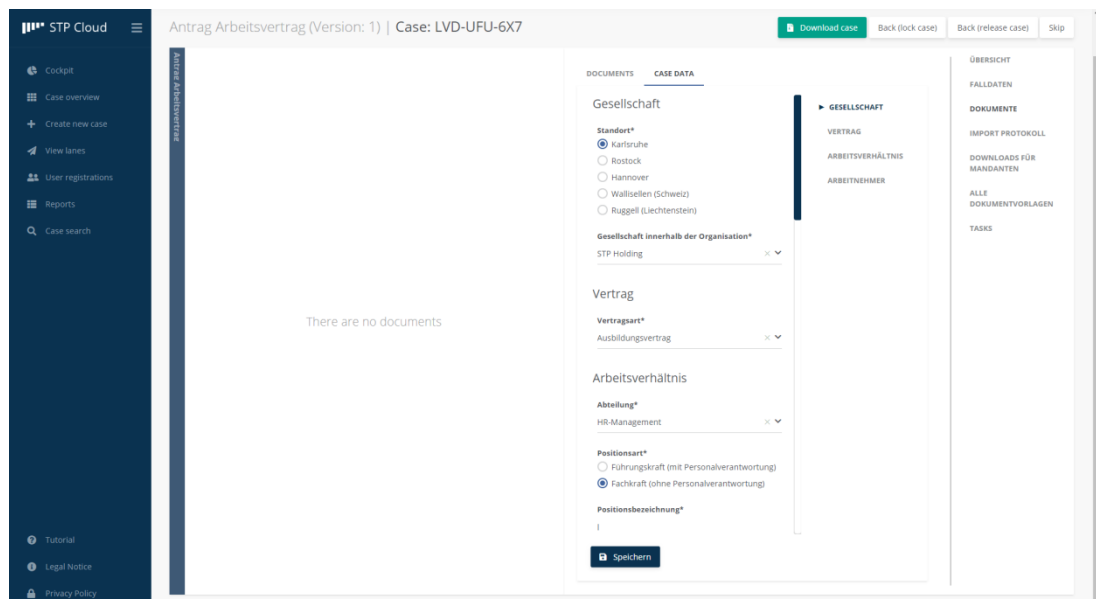
4 campaigns were found

- Aktenanlage
- Antrag Arbeitsvertrag
 

Campaign details Released: 06.08.2019 EDIT	Workflow <b>Draft</b> Released: 06.08.2019 EDIT	Definition for dossiers Released: - EDIT	Document types Released: 06.08.2019 EDIT
Document Generation SHOW			
- Compliance Check
- NDA Antrag

Legal Notice  
Privacy Policy

- 1 -



### 1.1.3 Technische Basis

LEXolution.FLOW soll als SaaS-Applikation mit einer Multi-Tenant Architektur, bestehend aus verschiedenen Micro-Services und Datenbanken auf der Basis eines Kubernetes Clusters in einem Rechenzentrum in Deutschland betrieben werden (im Folgenden die „**Produktiv-Instanz**“). Die Nutzer greifen mittels des Browsers ihrer Endgeräte (im Folgenden „**Client**“) auf LEXolution.FLOW zu. Dabei werden diverse Cookies zur Abwehr von Anti-Forgery-Angriffen sowie Session-Cookies zur Speicherung der Anmeldeinformationen und Cookies zur Speicherung der Benutzerprofil- und etwaiger Filtereinstellungen auf den von den Nutzern genutzten Endgeräten gesetzt.

Mit LEXolution.FLOW verarbeitete, Daten werden in verschiedenen Datenbanken<sup>1</sup> auf dem Kubernetes Cluster gespeichert (nachfolgend „**Cloudspeicher**“).

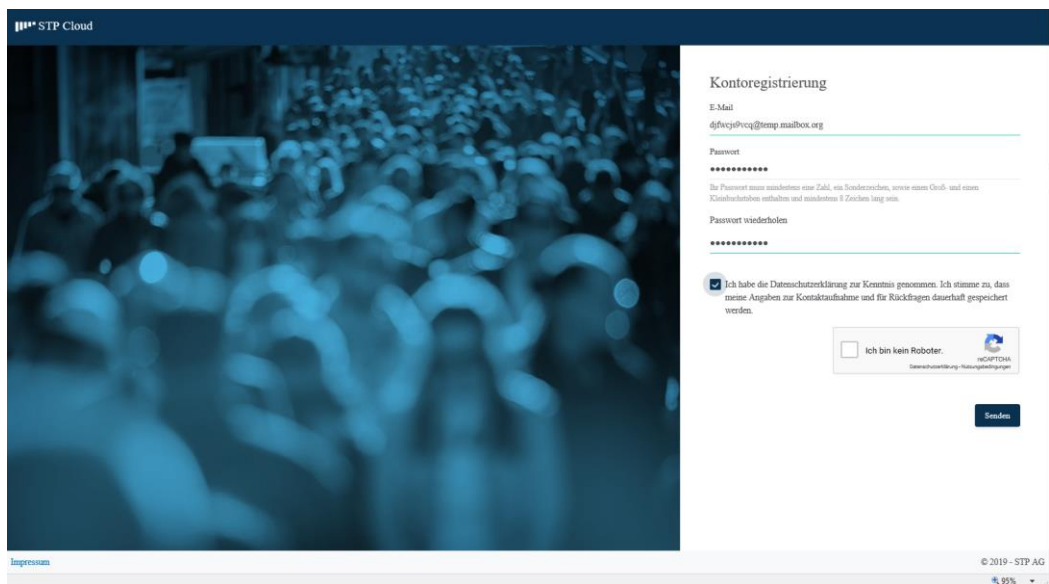
Die im Cloudspeicher gespeicherten ruhenden Daten sollen dabei verschlüsselt werden. LEXolution.FLOW

Jeder Kunde wird als separater Tenant in LEXolution.FLOW geführt, das heißt es gibt innerhalb der Applikation eine logische Trennung zwischen den einzelnen den Kunden zugeordneten Daten (jeweils ein „**Kundenbereich**“).

<sup>1</sup> Microsoft SQL Server (RDBMS), MongoDB (NoSQL Database), Elasticsearch (Searchindex) und S3 Storage (Data Storage).

Ein Nutzer kann entweder durch den Kunden oder – wenn und soweit der Kunde dies zulässt – durch eine Selbstregistrierung des Nutzers angelegt werden. Für die Registrierung ist das Double-Opt-In-Verfahren mit einer Registrierungsbestätigung per E-Mail implementiert.

Die nachfolgende Abbildung zeigt die Selbstregistrierung eines Nutzers.



Nach Eingabe der Daten und einen Klick auf die Schaltfläche „Senden“ erhält der Nutzer die Bestätigung einer Registrierung.

## Kontoregistrierung

### Vielen Dank für Ihre Registrierung

Eine Bestätigung der Registrierung wird in Kürze an die E-Mail-Adresse [djfwcjs9vcq@temp.mailbox.org](mailto:djfwcjs9vcq@temp.mailbox.org) gesendet.

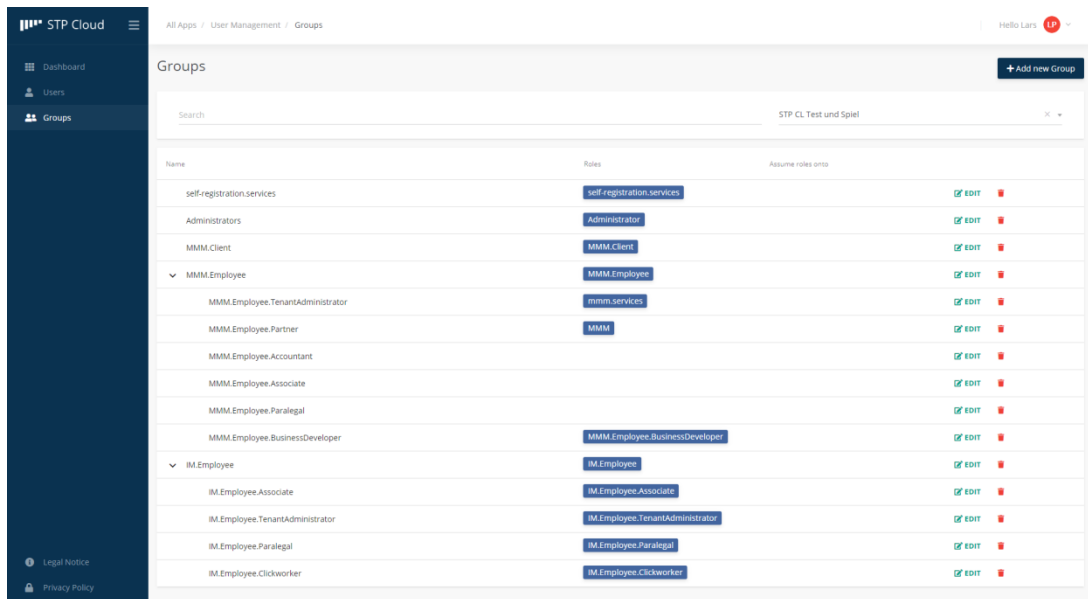
Bitte schließen Sie Ihre Registrierung durch einen Klick auf den darin enthaltenen Aktivierungslink ab.

Danach ist Ihre Registrierung abgeschlossen und Sie können sich mit Ihrer E-Mail-Adresse und Ihrem Passwort einloggen.

Standardmäßig erfolgt die Anmeldung eines Nutzers mit E-Mail und Benutzerpasswort. Optional kann der Kunde eine Zwei-Faktor-Authentifizierung aktivieren. Für die Realisierung dieser Funktion werden die Lösungen *DUO Multi-Factor Authentication (MFA)* (vgl. <https://duo.com/product/multi-factor-authentication-mfa>, Abruf: 19.02.2020) und *FIDO2* (<https://fidoalliance.org/fido2/>, Abruf: 19.02.2020) eingesetzt.

Auf jeden Kundenbereich kann rollengebunden über eine „**Kundensicht**“ oder eine „**Mandantensicht**“ zugegriffen werden. Zusätzlich besteht für den Kunden im Rahmen des Berechtigungsmanagements die Möglichkeit, die den Nutzern zugeordneten Zugriffs-, Lese- und Schreibrechte gruppenbasiert einzustellen.

Die nachfolgende Abbildung zeigt eine beispielhafte Gruppenkonfiguration in einem Kundenbereich:



In der Kundensicht wird neben dem Mandantenportal auch das Back-End der Workflow-Engine von LEXolution.FLOW angezeigt. Dieses erlaubt neben der Einrichtung und Verwaltung existierender Workflows den Zugriff auf und die Bearbeitung (inklusive Löschung und Export) aller dem Kundenbereich zugeordneten Daten. Hierzu gehören

- die „**Stammdaten**“ aller im Kundenbereich angelegten Nutzer,
- Informationen über das Nutzungsverhalten dieser Nutzer, wie zum Beispiel eine Nutzungshistorie („**Nutzungsdaten**“), sowie
- Informationen, die Mandanten selbst in LEXolution.FLOW im Rahmen der Inanspruchnahme eines Services hochladen oder die Kunden zu einem bestimmten in LEXolution.FLOW angelegten Vorgang speichern („**Falldaten**“).

Nutzer mit höheren Rechten können in Lexolution.Flow gespeicherte Daten selektiv für die weitere Verarbeitung durch rangniedere Nutzer sperren. Der Export von Daten aus LEXolution.FLOW ist für entsprechend berechnigte Nutzer im PDF- und/oder im CSV-Format möglich.

In der Mandantensicht kann der Nutzer mit dem Mandantenportal ausschließlich auf den ihn zugeordneten Mandantenbereich Zugriff nehmen und dort seine eigenen Stamm- und Falldaten einsehen.



Alle Aufrufe von LEXolution.FLOW durch Nutzer werden protokolliert. Die protokollierten Daten umfassen einen Zeitstempel, die IP-Adresse des zum Abruf verwendeten Endgeräts, die Bezeichnung des Tenants, eine Vorgangs-ID, den Umstand der erfolgreichen Anmeldung, den Username, ein Anwendungsname, sowie den genutzten Browsertyp („**Protokolldaten**“). Die Protokolldaten werden nicht für jeden Kunden separat, sondern kundenbereichsübergreifend durch STP erhoben und sind für die Kunden nicht zugänglich. Die Protokolldaten werden in temporären Log-Dateien für einen Zeitraum von 10 Tagen gespeichert. Diese Protokolldaten werden von STP ausschließlich zur Gewährleistung der Sicherheit der für die Bereitstellung von LEXolution.FLOW genutzten IT-Infrastruktur, insbesondere zur Feststellung, Beseitigung und beweissichernden Dokumentation von Störungen (z. B. DDoS-Angriffen) sowie zur Aktivierung einer temporären Anmelde Sperre bei mehreren fehlgeschlagenen Anmeldeversuchen eingesetzt. Darüber hinaus werden in LEXolution.FLOW Fehler des Programmablaufs protokolliert. Diese Fehlerprotokolle werden nach einer Aufbewahrungsdauer von 6 Monaten gelöscht.

LEXolution.FLOW bietet zudem eine Benachrichtigungsfunktion, mit der den Nutzern manuell oder automatisch generierte Benachrichtigungen an ihre in der Plattform hinterlegte E-Mail-Adresse zugeschickt werden können. Für die Realisierung dieser Funktion wird die SaaS-Lösung *Mailjet* genutzt, die über eine API an LEXolution.FLOW angebunden wird.

## 1.2 **Betrieb von LEXolution.FLOW**

LEXolution.FLOW wird von STP als „**Managed-Service**“ betrieben, sodass STP ohne spezifische Beauftragung durch die Kunden die Administration und kontinuierliche Weiterentwicklung von LEXolution.FLOW übernimmt. Zu diesen Zwecken muss STP auch auf die Produktiv-Instanz und den Cloudspeicher zugreifen. Es kann nicht ausgeschlossen werden, dass die hiermit beauftragten Mitarbeiter von STP hierbei von den in den Kundenbereichen verarbeiteten beziehungsweise gespeicherten Daten Kenntnis nehmen oder Kenntnis nehmen könnten.

Die grafische Benutzeroberfläche des Mandantenportals kann von jedem Kunden, zum Beispiel mit Freitextfeldern und grafischen Elementen, individuell gestaltet werden. Zudem bietet das Mandantenportal die Möglichkeit, in der Menüleiste ein Impressum und eine Datenschutzerklärung – jeweils als Freitextfelder – dauerhaft zu verlinken.

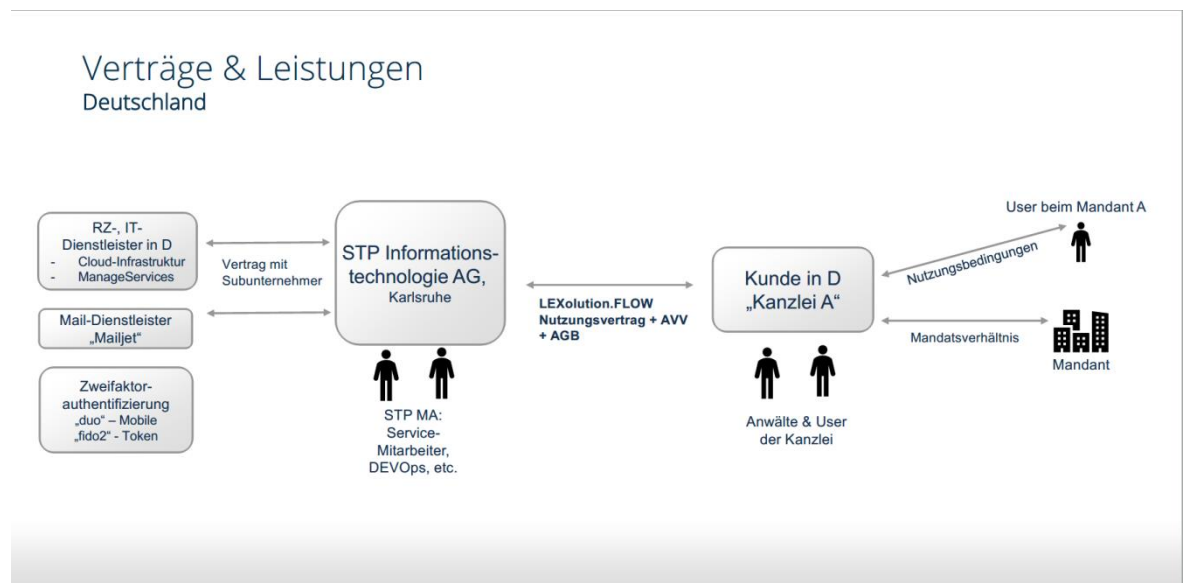
Zudem bietet STP den Kunden einen „**Customizing-Service**“ an, der im Einzelfall gesondert durch die Kunden beauftragt werden muss. Im Rahmen des Customi-

zung Service unterstützt STP den Kunden bei der Einrichtung und Nutzung von LEXolution.FLOW.

### 1.3 Vertragliche Beziehungen

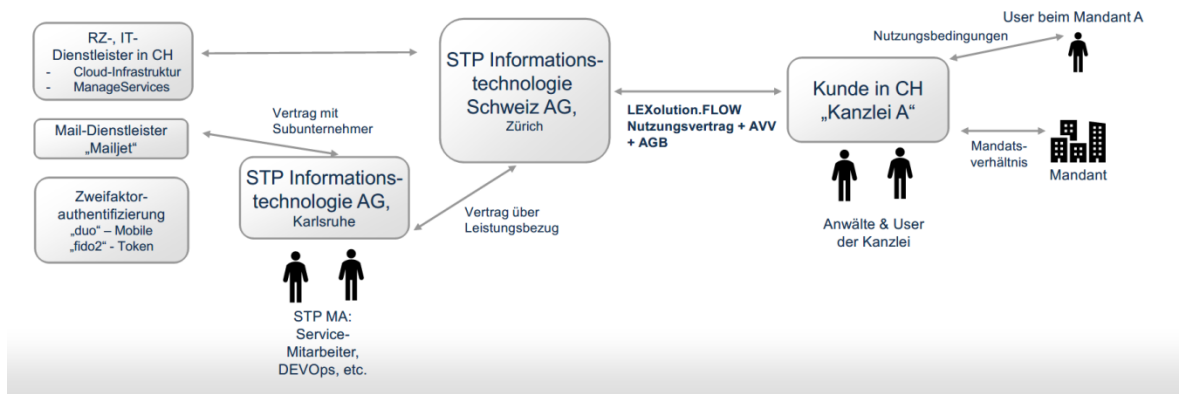
Mit in Deutschland ansässigen Kunden soll der Nutzungsvertrag für LEXolution.FLOW durch STP selbst abgeschlossen werden. In der Schweiz soll die STP Informationstechnologie Schweiz AG mit Sitz in Zürich, Schweiz, Vertragspartnerin der Kunden werden.

Die vertragliche Zielstruktur für Kunden in Deutschland und in der Schweiz ist in den nachfolgenden Abbildungen dargestellt:



Quelle: STP, Präsentation vom 12. Februar 2020.

## Verträge & Leistungen Schweiz



Quelle: STP, Präsentation vom 12. Februar 2020.

## 2 Zu prüfende Fragen

Wir sind von STP gebeten worden zu prüfen, ob und unter welchen Voraussetzungen die Nutzung von LEXolution.FLOW grundsätzlich mit dem Berufsrecht der Rechtsanwälte vereinbar und datenschutzrechtskonform möglich ist.

Bei der berufsrechtlichen Prüfung soll ein besonderes Augenmerk auf den Umstand gelegt werden, dass es sich bei LEXolution.FLOW um einen cloudbasierten Managed Service handelt.

Gegenstand der datenschutzrechtlichen Prüfung soll sein, ob die nachfolgend genannten Pflichten des Verantwortlichen unter der DS-GVO im Hinblick auf die Verarbeitung personenbezogener Daten in LEXolution.FLOW erfüllt und so dokumentiert werden können, dass der Verantwortliche seinen Rechenschaftspflichten gemäß Art. 5 Abs. 2 DS-GVO nachkommen kann:

1. Informationspflicht nach Art. 13/14 DS-GVO
2. Auskunftsrecht nach Art. 15 Abs. 1 DS-GVO sowie in Form der Bereitstellung einer Kopie der personenbezogenen Daten nach Art. 15, Abs. 3 DS-GVO.
3. Recht auf Berichtigung nach Art. 16 DS-GVO
4. Recht auf Löschung nach Art. 17 DS-GVO

5. Recht auf Einschränkung der Bearbeitung nach Art. 18 DS-GVO
6. Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO
7. Widerspruchsrecht nach Art. 20 DS-GVO
8. Die Grundsätze des Datenschutzes durch Technikgestaltung (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) nach Art. 25 DS-GVO.

Da die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, d. h. das Eingreifen eines gesetzlichen Erlaubnistatbestandes im Sinne des Art. 6 Abs. 1 bzw. Art. 9 Abs. 2 DS-GVO maßgeblich von dem konkreten Einsatz von LEXolution.FLOW durch den Kunden, d. h. dem mit der Datenverarbeitung verfolgten Zwecke sowie der gegebenenfalls bestehenden Mandatsbeziehung zu den Nutzern abhängt, soll die Frage der Rechtmäßigkeit der Datenverarbeitung im Sinne von Art. 5 Abs. 1 lit. a) i. V. m. Art. 6 bzw. 9 DS-GVO unberücksichtigt bleiben, soweit nicht aufgrund der Funktion des LEXolution.FLOW Zweifel daran bestehen, ob die Datenverarbeitung überhaupt auf einen Erlaubnistatbestand gestützt werden kann.

Nicht geprüft werden soll ferner, ob die Kunden bei Einsatz von LEXolution.FLOW ihren Pflichten nach Art. 32 DS-GVO, technische und organisatorische Maßnahmen zu treffen, genügen, da die Antwort hierauf maßgeblich von der technischen Ausgestaltung des Produkts, insbesondere der konkreten Form der Verschlüsselung von Daten und des Datenverkehrs abhängt und insoweit eine technische Fragestellung ist.

Im Rahmen der Prüfung der Funktionalitäten von LEXolution.FLOW werden im Rahmen dieses Memorandums die grundlegenden Funktionalitäten zur Erfüllung der Betroffenenrechte gemäß Art. 12 ff. DS-GVO geprüft. Da der Umfang der erfassten personenbezogenen Daten und die Verarbeitungsmodalitäten von dem konkreten Einsatz von LEXolution.FLOW durch den Kunden abhängen, kann die Vollständigkeit von Datenexporten zur Beantwortung von Betroffenenanfragen gemäß Art. 15 und Art. 20 DS-GVO nur einzelfallbezogen beurteilt werden. Die Prüfung der Datenexportfunktionen von LEXolution.FLOW im Rahmen dieses Memorandums beschränkt sich deshalb auf die Frage, ob diese grundsätzlich geeignet sind, entsprechende Anfragen von Betroffenen zu erfüllen.

Ferner hat STP uns gebeten, neben den berufsrechtlichen und datenschutzrechtlichen Themen auch zu erörtern,

- ob die allgemeine Impressumspflicht gemäß § 5 TMG grundsätzlich erfüllt werden kann und wer hierfür verantwortlich ist,
- ob die Informationspflichten gemäß der Dienstleistungs-Informationspflichten-Verordnung (DL-InfoV) und ggf. nach dem Verbraucherstreitbeilegungsgesetz (VSBG) und der Verordnung über Online-Streitbeilegung in Verbraucherangelegenheiten (ODR-VO) grundsätzlich erfüllt werden können und
- ob die zivilrechtlichen Anforderungen für den elektronischen Geschäftsverkehr und für Fernabsatzgeschäfte bei über LEXolution.FLOW angebotenen Services grundsätzlich erfüllt werden können.

Die Prüfung weiterer Rechtsfragen, die sich im Zusammenhang mit LEXolution.FLOW stellen könnten, einschließlich Fragen der Erfüllung berufsrechtlicher Pflichten bei der Speicherung von mittels LEXolution.FLOW erzeugter Daten in an LEXolution.FLOW angebundenen IT-Systemen sind nicht Gegenstand dieses Memorandums.

### **3 Executive Summary**

- Die Nutzung von LEXolution.FLOW hat eine Offenlegung der Daten an STP und deren Subunternehmer zur Folge, die vom Kunden in LEXolution.FLOW erfasst oder damit verarbeitet werden. Eine rechtskonforme Nutzung von LEXolution.FLOW durch Anwälte setzt daher voraus, dass sich STP vertraglich
  - gegenüber den Kunden zur Verschwiegenheit und dazu verpflichten
    - sämtliche Beschäftigte von STP, die in den Betrieb von LEXolution.FLOW eingebunden werden, zur Verschwiegenheit zu verpflichten sowie
    - sämtlichen Subunternehmern, die möglicherweise Zugriff auf die in LEXolution.FLOW gespeicherten Daten nehmen könnten die gleichen vertraglichen Pflichten aufzuerlegen.
- Organisatorisch muss STP dafür Sorge tragen, dass alle mit dem Betrieb von LEXolution.FLOW betrauten Beschäftigten dokumentiert zur Verschwiegenheit verpflichtet werden und dass die Einhaltung der entsprechenden Pflichten durch die Subunternehmer von STP, sowohl im Hinblick auf deren eigene Beschäftigte wie auch im Hinblick auf gegebenen-

falls eingesetzte weitere Subunternehmer, nachweisbar kontrolliert wird.

- Die als Rechtsanwalt tätigen Kunden sind berufsrechtlich verpflichtet, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Anwaltsberuf zumutbar sind. Die Nutzung der Funktion zum Versand unverschlüsselter automatischer E-Mails von LEXolution.FLOW ist jedenfalls dann erlaubt, wenn der Mandant dieser Kommunikation zugestimmt hat oder diese Zustimmung fingiert wird. Es wird empfohlen, den Kunden auch die Möglichkeit zur Verschlüsselung der von LEXolution.FLOW versandten E-Mails zu ermöglichen.
- Die als Rechtsanwalt tätigen Kunden können ihre berufsrechtlichen Pflichten zum Führen einer Handakte bei Nutzung von LEXolution.FLOW nur dann erfüllen, wenn die mittels LEXolution.FLOW generierten Daten und Protokolle zur Darstellung der Tätigkeit des Anwalts in dem Dokumentenmanagement System des Anwalts gespeichert werden. Dies ist nach der uns vorliegenden Beschreibung durch die Anbindung an das jeweilige Kanzleisystem gewährleistet.
- Der rechtskonforme Einsatz von LEXolution.FLOW setzt den Abschluss eines Vertrages zur Auftragsverarbeitung zwischen dem Kunden und STP sowie den Abschluss deckungsgleicher Verträge in der gesamten Vertragskette, also zwischen STP und deren Unterauftragnehmern sowie diesen und ggf. eingeschalteten Unter-Unterauftragnehmern, voraus.
- Die Kunden können mittels der Funktionen von LEXolution.FLOW ihre datenschutzrechtlichen Informations- und Auskunftspflichten nach Art. 13/14 und Art. 15 DS-GVO, sowie ihre Pflicht zur Berichtigung unrichtiger personenbezogener Daten nach Art. 16 DS-GVO einhalten.
- Um den Kunden die Erfüllung ihrer Pflicht zur Löschung personenbezogener Daten nach Art. 17 DS-GVO auch dann mit angemessenem Aufwand zu ermöglichen, wenn der Kunde LEXolution.FLOW in nennenswertem Umfang nutzt, müsste LEXolution.FLOW weitere Funktionen zur automatisierten Löschung von Fall-, Stamm- und sonstigen personenbezogenen Daten bei Eintritt bestimmter Ereignisse und nach einem definierten Zeitablauf, der wiederum an ein Ereignis anknüpft, vorsehen.
- Der Kunde kann Nutzer berechtigen, in Lexolution.Flow gespeicherte Daten für die Verarbeitung durch rangniedere Nutzer zu sperren. Mit ei-

ner entsprechenden Rechtevergabe und Ausgestaltung seines Prozesses zur Bearbeitung von Anträgen betroffener Personen auf Einschränkung der Verarbeitung ihrer personenbezogenen Daten können die Kunden ihren sich aus Art. 18 Abs. 1 DS-GVO ergebenden Pflichten nachkommen.

- Die Kunden können die im Sachverhalt beschriebene Exportfunktion nutzen, um in Lexolution.Flow gespeicherte Daten im PDF- und/oder im CSV-Format zu exportieren und damit Datenübertragungverlangen gemäß Art. 20 DS-GVO nachkommen.
- Aufgrund der vorliegenden Informationen kann nicht beurteilt werden, ob die bei Nutzung von LEXolution.FLOW gesetzten Cookies zwingend für die Nutzung erforderlich sind und daher keiner Einwilligung bedürfen. Es wird daher empfohlen, einen Cookie-Banner zur Einholung der Einwilligung des Nutzers in die Speicherung nicht zwingend notwendiger Cookies zu implementieren.
- Die Einhaltung der Datenschutzgrundsätze in Art. 5 DS-GVO hängt – von den vorstehend genannten Punkten abgesehen - maßgeblich vom konkreten Einsatz von LEXolution.FLOW durch den Kunden ab. Es bestehen insoweit keine Anhaltspunkte dafür, dass diese bei Nutzung von LEXolution.FLOW nicht eingehalten werden könnten.

## **4 Rechtliche Würdigung im Einzelnen**

### **4.1 Grundsätzliche Rechtskonformität des Betriebsmodells von LEXolution.FLOW unter Einsatz von Hilfspersonen bzw. Dienstleistern**

#### **4.1.1 Zu berücksichtigende strafrechtliche und berufsrechtliche Regelungen**

Der rechtliche Rahmen für den Betrieb von LEXolution.FLOW wird nicht nur durch das Datenschutzrecht bestimmt, sondern insbesondere auch durch die Vorschriften zum Schutz des Mandatsgeheimnisses, die sich im Strafrecht und im Berufsrecht der Rechtsanwälte finden, soweit es sich bei den Kunden um Rechtsanwälte handelt.<sup>2</sup>

---

<sup>2</sup> Die nachfolgenden strafrechtlichen Vorschriften gelten auch für weitere zur besonderen Verschwiegenheit verpflichteten Berufsträger, wie zum Beispiel Steuerberater oder Wirtschaftsprüfer. Das Berufsrecht dieser Berufe kann jedoch andere Anforderungen als das anwaltliche Berufsrecht an die Nutzung von LEXolution.FLOW stellen.

Die Verletzung des Mandatsgeheimnisses ist durch § 203 StGB unter Strafe gestellt.

Gemäß § 203 Abs. 1 Nr. 3 StGB macht sich ein Rechtsanwalt strafbar, wenn er unbefugt ein fremdes Geheimnis offenbart, das ihm im Rahmen seiner Tätigkeit als Rechtsanwalt bekannt geworden ist.

Gemäß § 203 Abs. 4 S. 1 StGB machen sich zudem auch die Hilfspersonen von STP strafbar, wenn sie unbefugt ein fremdes Geheimnis offenbaren, das ihnen im Zusammenhang mit der Nutzung von LEXolution.FLOW durch den Rechtsanwalt bekannt geworden ist.

Diese beiden zentralen Straftatbestände, die jeweils die unbefugte Offenbarung von Privatgeheimnissen zum Gegenstand haben, werden noch durch weitere Straftatbestände, die eine unterlassene Verpflichtung von mitwirkenden Personen auf die Verschwiegenheit zum Gegenstand haben, ergänzt (§ 203 Abs. 4 Nr. 1 und 2 StGB).

Zusätzlich wird dieser strafrechtliche Schutz des Mandatsgeheimnisses durch berufsrechtliche Regelungen in §§ 43a Abs. 2, 43e BRAO sowie § 2 BORA flankiert. Diese berufsrechtlichen Regelungen stellen zum Teil weitergehende Anforderungen an die Einbindung von Dienstleistern in die rechtsanwaltliche Tätigkeit als § 203 StGB. Ein Verstoß ausschließlich gegen berufsrechtliche Regelungen wäre strafrechtlich nicht relevant. Gleichwohl wäre ein Verstoß gegen das Berufsrecht im Zusammenhang mit LEXolution.FLOW eine Berufspflichtverletzung, die berufsrechtlich gegenüber den Kunden – nicht aber gegenüber STP – geahndet werden könnte.

#### **4.1.2 Strafrechtskonformität von LEXolution.FLOW**

##### **4.1.2.1 Strafrechtlich relevante Offenbarung von Geheimnissen im Rahmen von LEXolution.FLOW**

Voraussetzung für den strafrechtskonformen Betrieb von LEXolution.FLOW ist, dass hierbei sowohl durch den Kunden gegenüber STP, wie auch durch STP gegenüber seinen zur Leistungserbringung eingesetzten Beschäftigten und Subunternehmern, nicht unbefugt Geheimnisse offenbart werden, die dem Mandatsgeheimnis unterliegen.

Geheimnisse im Sinne des § 203 StGB sind Tatsachen, die nur einem begrenzten Personenkreis bekannt sind und an denen der Geheimnisbetroffene, im Fall eines



Rechtsanwalts also der Mandant, ein sachlich begründetes Geheimhaltungsinteresse sowie einen Geheimhaltungswillen besitzt.<sup>3</sup> Hiervon ausgehend sind grundsätzlich sämtliche auf einen Mandanten bezogene oder beziehbare Tatsachen von denen der Rechtsanwalt im Rahmen seiner Beratungstätigkeit Kenntnis erlangt strafrechtlich geschützte Geheimnisse. Folglich sind sowohl die Falldaten, wie auch alle Umstände des Kontaktes eines Mandanten mit einem Rechtsanwalt Geheimnisse im Sinne des § 203 StGB. Demgemäß ist bereits die Tatsache, dass ein Mandant von einem Rechtsanwalt mittels LEXolution.FLOW beraten wird/wurde oder eine Beratung angefragt hat, geheimhaltungspflichtig. Es sind damit auch die Stammdaten der Nutzer, soweit es sich hierbei um Mandanten handelt, strafrechtlich geschützte Geheimnisse.

Die Offenbarung von Geheimnissen ist nach § 203 Abs. 1 StGB jedoch nur dann strafbar, wenn sie unbefugt ist, also weder eine Einwilligung des Geheimnisberechtigten, hier des Mandanten, vorliegt, noch ein gesetzlicher Erlaubnistatbestand zur Offenbarung einschlägig ist.

Offenbaren im Sinne des § 203 Abs. 1 StGB ist jede Mitteilung eines geschützten Geheimnisses. Nach dem Willen des Gesetzgebers genügt für ein Offenbaren bereits das Verschaffen der Möglichkeit der Kenntnisnahme durch Dritte,<sup>4</sup> auf eine tatsächliche Kenntnisnahme kommt es hiernach nicht an. Bei digital gespeicherten Geheimnissen genügt für ein Offenbaren mithin die Einräumung der Verfügungsgewalt über die Daten, wenn diese nicht wirksam gegenüber der speichernden Stelle verschlüsselt werden.<sup>5</sup>

Da im Rahmen von LEXolution.FLOW eine nicht gegenüber STP wirksame Verschlüsselung verwendet wird, und LEXolution.FLOW den Kunden als Managed-Service angeboten werden soll, ist mit der Nutzung von LEXolution.FLOW durch die Kunden eine Offenbarung ihrer in LEXolution.FLOW verarbeiteten, mandatsbezogenen Informationen gegenüber STP zur Leistungserbringung eingesetzten Beschäftigten verbunden.

Des Weiteren muss davon ausgegangen werden, dass auch die von STP eingesetzten Subunternehmer die Möglichkeit haben, von dem Inhalt mandatsbezogener Informationen Kenntnis zu nehmen, es sei denn, es ist technisch sicher ausgeschlossen, dass der Subunternehmer die Möglichkeit hat, von mandatsbezogenen Informationen Kenntnis zu erlangen.

---

<sup>3</sup> Vgl. *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 30. Auflage 2019, § 203 StGB Rn. 5 mwN.

<sup>4</sup> BT-Drs. 18/11936, S. 28.

<sup>5</sup> *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 30. Auflage 2019, § 203 StGB Rn. 20.

Speziell im Hinblick auf den Cloud-Infrastrukturprovider kann nicht sicher ausgeschlossen werden, dass im Rahmen der Administration und/oder des Supports für die Cloud-Plattform möglicherweise mandatsbezogene Informationen von dem hiermit betrauten Personal oder weiteren Subunternehmern des Cloud-Infrastrukturproviders zur Kenntnis genommen werden könnten. Auch der E-Mailprovider wird im Rahmen der Übermittlung der E-Mails Kenntnis von deren Inhalt und damit von einzelnen mandatsbezogenen Umständen erlangen können. Folglich ist mit der Nutzung von LEXolution.FLOW durch die Kunden eine Offenbarung der in LEXolution.FLOW verarbeiteten, mandatsbezogenen Informationen jedenfalls gegenüber

- den Personen, die bei STP auf das Back-End von LEXolution.FLOW zugreifen können,
- dem Cloud-Infrastrukturprovider und dessen Personal/dessen weiteren Subunternehmern sowie
- gegebenenfalls gegenüber anderen Subunternehmern von STP, wie bspw. dem E-Mailprovider) die die Möglichkeit haben, mandatsbezogene Informationen zur Kenntnis zu nehmen,

verbunden.

#### **4.1.2.2 Gesetzliche Rechtfertigung der Offenbarung gemäß § 203 Abs. 3 Satz 2 StGB**

Der durch das „Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“<sup>6</sup> neu geschaffene Erlaubnistatbestand in § 203 Abs. 3 Satz 2 Hs. 1 StGB erlaubt Rechtsanwälten die Offenbarung von Geheimnissen gegenüber Dritten, ohne dass vom Geheimnisberechtigten, also dem Mandanten, eine vorherige Einwilligung eingeholt werden muss. Voraussetzung hierfür ist, dass die Dritten als „sonstige mitwirkende Person“ an der Tätigkeit des Rechtsanwalts mitwirken, und die Offenbarung auf das Erforderliche beschränkt ist.

Unter den gleichen Voraussetzungen ist es auch sonstigen mitwirkenden Personen gestattet, weitere – sonstige mitwirkende – Personen hinzuzuziehen, die an der beruflichen Tätigkeit des Rechtsanwalts mitwirken (§ 203 Abs. 3 Satz 2 HS. 2 StGB).

---

<sup>6</sup> BGBl. I. 2017 Nr. 71 vom 08.11.2017.

Eine Mitwirkung an der beruflichen Tätigkeit im Sinne des § 203 Abs. 3 Satz 2 Hs. 1 StGB liegt dann vor, wenn die betreffende Person unmittelbar mit der beruflichen Tätigkeit der schweigepflichtigen Person, ihrer Vorbereitung, Durchführung, Auswertung und Verwaltung befasst ist.<sup>7</sup> Dies ist im Hinblick auf den Nutzungszweck von LEXolution.FLOW, nämlich die Unterstützung von rechtlichen Prüf-, Beratungs- und Entscheidungsprozessen in Rechtsanwaltskanzleien zu bejahen. Demgemäß sind STP und ihre im Rahmen der Bereitstellung von LEXolution.FLOW mit der Leistungserbringung betrauten Beschäftigten sonstige mitwirkende Personen im Sinne des § 203 Abs. 3 Satz 2 Hs. 1 StGB. Entsprechendes gilt für alle Subunternehmer, weiteren Subunternehmer und deren Beschäftigte, soweit sie Leistungen im Zusammenhang mit LEXolution.FLOW erbringen.

Entscheidend für die Rechtfertigung der mit der Nutzung von LEXolution.FLOW verbundenen Offenbarung von Mandatsgeheimnissen auf der Grundlage von § 203 Abs. 3 Satz 2 Hs. 1 StGB ist, ob sich diese im Rahmen des Erforderlichen hält. In der Gesetzesbegründung wird hierzu lediglich pauschal ausgeführt, dass der Berufsgeheimnisträger nicht mehr geschützte Geheimnisse preisgeben dürfe als notwendig.<sup>8</sup>

Ausweislich des eindeutigen Wortlautes des § 203 Abs. 3 Satz 2 Hs. 1 StGB kommt es im Rahmen der Erforderlichkeit jedoch nicht darauf an, ob der Rechtsanwalt LEXolution.FLOW zwingend für seine rechtsanwaltliche Tätigkeit benötigt. Denn die Erforderlichkeit bezieht sich, wie die Konjunktion „soweit“ anzeigt, ausschließlich auf den Umfang der Offenbarung von Berufsgeheimnissen an die sonstige mitwirkende Person zur Erbringung ihrer Tätigkeit, nicht aber auf die Inanspruchnahme der Tätigkeit als solche.

Es wäre folglich mit dem strafrechtlichen Bestimmtheitsgrundsatz (Art. 103 Abs. 2 GG), der eine wortlautüberschreitende Auslegung zu Lasten des Rechtsanwalts bzw. der sonstigen mitwirkenden Person verbietet, nicht vereinbar, wenn man auch die Inanspruchnahme der Tätigkeit als solche dem Erforderlichkeitsgebot unterstellte. Die Frage, ob ein Rechtsanwalt LEXolution.FLOW für seine rechtsanwaltliche Tätigkeit (zwingend) benötigt, ist demgemäß für die Frage der Erforderlichkeit nicht von Relevanz.<sup>9</sup> Hierfür spricht auch, dass der Gesetz-

---

<sup>7</sup> BT-Drs. 18/11936, S. 22; *Ciernak/Niehaus*, in Münchener Kommentar StGB, 3. Aufl. 2017, § 203 Rn. 137; *Eisele*, JR 2018, 79, 83.

<sup>8</sup> BT-Drs. 18/11936, S. 23, 28.

<sup>9</sup> Vgl. nur *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 30. Auflage 2019, § 203 StGB Rn. 51; *Ciernak/Niehaus*, in Münchener Kommentar, StGB, 3. Aufl. 2017, § 203 Rn. 138; *Cornelius*, NJW 2017, 3751, 3752; *Klugmann/Leenen/Salz*, AnwBl Online 2018, 283, 285; *Basar*, jurisPR-StrafR 4/2018 Anm. 1; *Nolte/Thelen*, jurisPR-Compl 6/2017 Anm. 4; *Pohle/Ghaffari*, CR 2017, 489, 493.

geber für die berufsrechtliche Parallelvorschrift in § 43e Abs. 1 Satz 1 BRAO explizit davon ausgeht, dass die Erforderlichkeit einer Auslagerung nicht deshalb zu verneinen sei, weil auch die Möglichkeit bestünde, Dienstleister in der Kanzlei anzustellen.<sup>10</sup>

Folglich kann der Rechtsanwalt im Rahmen des § 203 Abs. 3 Satz 2 Hs. 1 StGB grundsätzlich frei darüber entscheiden, welche Dienstleistungen er für die Unterstützung seiner rechtsanwaltlichen Tätigkeit beziehen möchte. Er wird durch das Erforderlichkeitsgebot bei der Auswahl der Dienstleistung nur insoweit beschränkt, als dass er nur Dienstleistungen in Anspruch nehmen darf, bei denen die Offenbarung von Berufsgeheimnissen auf das zur Erbringung der konkreten Dienstleistung Erforderliche beschränkt ist.<sup>11</sup>

Nicht eindeutig in § 203 Abs. 3 Satz 2 Hs. 1 StGB geregelt ist jedoch, ob ein strenger Erforderlichkeitsmaßstab im Sinne einer absolut zwingenden Notwendigkeit, wonach nur solche Offenbarungen von Mandatsgeheimnissen zulässig wären ohne die die Erbringung der Dienstleistung nicht möglich wäre, anzulegen ist, oder ob es ausreichend ist, wenn sich die Offenbarung bei vernünftiger Würdigung als objektiv sinnvoll im Kontext der konkreten Dienstleistung erweist.

Wörtlich heißt es hierzu in der Gesetzesbegründung lediglich:

*„Notwendige Einschränkung des § 203 Absatz 3 StGB-E ist das Erfordernis, dass eine Offenbarung von Geheimnissen an eine sonstige mitwirkende Person insoweit nicht der Strafbarkeit unterfällt, als sie erforderlich für die Inanspruchnahme von deren Tätigkeit ist – der Berufsgeheimnisträger darf nicht mehr geschützte Geheimnisse preisgeben als notwendig ist, damit er die Tätigkeit der sonstigen mitwirkenden Person übertragen kann.“<sup>12</sup>*

Soweit ersichtlich gibt es zu dieser Frage bislang keine publizierten Gerichtsentscheidungen. Die bislang hierzu veröffentlichte Literatur geht vor dem Hintergrund der Gesetzesbegründung grundsätzlich davon aus, dass ein strenger Maßstab anzulegen ist, und die Offenbarung von Geheimnissen nur insoweit erforderlich sei, wie die konkrete Dienstleistung nicht ohne Kenntnis der Geheimnisse durchgeführt werden könne.<sup>13</sup>

---

<sup>10</sup> BT-Drs. 18/11936, S. 34.

<sup>11</sup> Eisele, in: Schönke/Schröder, Strafgesetzbuch, 30. Auflage 2019, § 203 StGB Rn. 51; Pohle/Ghaffari, CR 17, 492.

<sup>12</sup> BT-Drs. 18/11936, S. 23.

<sup>13</sup> So zum Beispiel Klugmann/Leenen/Salz, AnwBl Online 2018, 283, 285; Grosskopf/Momsen, CCZ 2018, 98, 102; Härting, NJW 2019, 1423.

Gleichwohl wird mit unterschiedlichen Formulierungen nicht auf eine zwingende Notwendigkeit abgestellt, sondern auf eine wertende Betrachtung; so geht zum Beispiel *Cornelius* davon aus, dass die sachgemäße Erbringung der Tätigkeit der Bezugspunkt der Erforderlichkeit sei.<sup>14</sup> *Härting* bejaht die Erforderlichkeit einer Offenbarung dann, wenn die Ausführung der Dienstleistung ohne den Zugang zum Geheimnis erschwert wäre,<sup>15</sup> und auch *Grosskopf/ Momsen* gehen davon aus, dass die Erforderlichkeit der Offenbarung dann bejaht werden könne, wenn die Dienstleistung ansonsten nur unter unverhältnismäßig großen Schwierigkeiten, mit einem unvermeidbar höheren Aufwand oder verspätet erfüllt werden könne.<sup>16</sup> Speziell die mit der Nutzung von ASP/SaaS-Diensten verbundene Offenbarung halten *Nolte/ Thelen* und *Klugmann/ Leenen/ Salz* grundsätzlich für mit dem Erforderlichkeitsgrundsatz für vereinbar:

*„Jedes Offenbaren über die Erforderlichkeit hinaus ist mit einem Strafbarkeitsrisiko verbunden. Mietet beispielsweise ein Berufsgeheimnisträger Speicherplatz auf einem externen Server an, wird es regelmäßig nicht erforderlich sein, dem Vertragspartner Zugang zu Tatsachen zu verschaffen, die der Verschwiegenheit unterliegen. In einem solchen Fall dürfen die Daten nur verschlüsselt auf dem externen Server gespeichert werden. Anders kann es aber bereits sein, wenn nicht nur Speicherplatz angemietet, sondern auch Service-Leistungen in Anspruch genommen werden“ (Hervorhebung nicht im Original).<sup>17</sup>*

*„Wenn die Daten in der Cloud hingegen (auch) verarbeitet werden müssen (zum Beispiel bei SaaS-Diensten), ist es derzeit nicht möglich, eine Kenntnisnahme durch den Dienstleister effektiv auszuschließen. Eine auch gegen den Dienstleister wirksame Verschlüsselung scheidet insoweit aus, da die Verarbeitung verschlüsselter Daten ohne zumindest vorübergehende Entschlüsselung derzeit technisch noch nicht realisierbar ist.“<sup>18</sup>*

Vor diesem Hintergrund sprechen gute Argumente dafür, dass die mit dem Betrieb von LEXolution.FLOW als Managed-Service verbundene Offenbarung von Mandatsgeheimnissen mit dem Erforderlichkeitskriterium vereinbar ist, wenn sich der Zugriff auf das für die Administration von LEXolution.FLOW notwendige Maß beschränkt. Entsprechendes gilt auch für die Inanspruchnahme von Cloud-Infrastruktur- und E-Maildiensten durch STP für den Betrieb von LEXolution.FLOW, wenn der jeweilige Provider nur in dem für die Administration seiner

---

<sup>14</sup> *Cornelius*, NJW 2017, 3751, 3752.

<sup>15</sup> *Härting*, NJW 2019, 1423.

<sup>16</sup> *Grosskopf/Momsen*, CCZ 2018, 98, 102.

<sup>17</sup> *Nolte/Thelen*, jurisPR-Compl 6/2017 Anm. 4.

<sup>18</sup> *Klugmann/Leenen/Salz*, AnwBl Online 2018, 283, 285.

Dienste notwendigen Umfang auf die in LEXolution.FLOW verarbeiteten Daten zugreifen kann.

Dies vorausgesetzt ist die mit der Nutzung von LEXolution.FLOW verbundene Offenbarung von Mandatsgeheimnissen durch den Rechtsanwalt gegenüber STP auf der Grundlage von § 203 Abs. 3 Satz 2 Hs. 1 StGB gerechtfertigt. Entsprechendes gilt gemäß § 203 Abs. 3 Satz 2 Hs. 2 StGB auch für die mit der Nutzung von LEXolution.FLOW verbundene Offenbarung von Mandatsgeheimnissen durch STP gegenüber ihren Subunternehmern wie bspw. dem Cloud-Infrastrukturprovider und dem E-Mailprovider.

Nichtsdestotrotz ist die Frage, in welchem Umfang die Offenbarung von Mandatsgeheimnissen für die Inanspruchnahme einer Tätigkeit einer sonstigen mitwirkenden Person erforderlich ist, letztlich eine Wertungsfrage, die ein Gericht anders als die in der deutschen Rechtsliteratur derzeit vorherrschende Meinung beantworten könnte. Demgemäß kann es im Hinblick auf die bislang fehlende Rechtsprechung zum Erforderlichkeitskriterium und der gesetzlich nicht eindeutigen Festlegung des Maßstabes für die Erforderlichkeitsprüfung nicht sicher ausgeschlossen werden, dass ein ggf. mit der Sache befasstes Gericht zu der Auffassung gelangen könnte, dass die mit der Nutzung von LEXolution.FLOW verbundene Offenbarung von Berufsgeheimnissen nicht auf der Grundlage von § 203 Abs. 3 Satz 2 Hs. 1 StGB bzw. § 203 Abs. 3 Satz 2 Hs 2 StGB gerechtfertigt werden kann.

Dennoch halten wir das Risiko einer strafrechtlichen Ahndung eines möglichen Verstoßes gegen § 203 StGB selbst in diesem Fall für gering, denn die in der deutschen Rechtsliteratur derzeit vorherrschende Meinung legt zumindest die Annahme eines strafbarkeitsausschließenden unvermeidbaren Verbotsirrtums (§ 17 StGB) nahe.

#### **4.1.2.3 Technische und organisatorische Maßnahmen zum Geheimnisschutz**

Da der Tatbestand des § 203 Abs. 1 Nr. 3 StGB bzw. § 203 Abs. 4 Satz 1 StGB auch durch ein vorwerfbares Unterlassen der Verhinderung einer nicht erforderlichen Kenntnisnahme von Geheimnissen verwirklicht werden kann,<sup>19</sup> müssen zur Vermeidung von Strafbarkeitsrisiken für die Kunden und die Verantwortlichen bei STP wirksame technische und organisatorische Maßnahmen ergriffen werden, um eine über das Erforderliche hinausgehende Offenbarung von in LEXoluti-

---

<sup>19</sup> *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 30. Auflage 2019, § 203 StGB Rn. 23; *Fischer*, in: Fischer, Strafgesetzbuch, 64. Auflage 2017, § 203 StGB Rn. 30b.

on.FLOW verarbeiteten Fall- oder Stammdaten möglichst zu vermeiden.<sup>20</sup> Zusätzlich legt die objektive, das heißt nach außen dokumentierte, Manifestation der Absicht, eine nicht für die Leistungserbringung erforderliche Offenbarung von Geheimnissen nach Möglichkeit zu vermeiden, die Annahme eines strafbarkeitsausschließenden Erlaubnistatbestandsirrtums über das Bestehen eines Rechtfertigungsgrundes, hier § 203 Abs. 3 Satz 2 StGB, nahe:

*„Soweit sich der Berufsträger hier über die tatsächlichen Grundlagen der Erforderlichkeit und damit der Befugnisnorm irrt, wird ein vorsatz- bzw. schuldaußschließender Erlaubnistatbestandsirrtum in Betracht kommen; bei bloßem Irrtum über den rechtlich zu betreibenden Aufwand liegt hingegen ein idR nur unbeachtlicher Verbotsirrtum gemäß § 17 vor.“<sup>21</sup>*

Vor diesem Hintergrund ist es insbesondere erforderlich, dass STP die Zugriffsmöglichkeit ihrer eigenen Beschäftigten auf LEXolution.FLOW technisch beschränkt und nur den mit der Administration von LEXolution.FLOW betrauten Beschäftigten den Zugang zu LEXolution.FLOW eröffnet. Zudem sollte jeder Login durch die Administratoren protokolliert und deren Zugriff auf LEXolution.FLOW regelmäßig kontrolliert werden. Organisatorisch sollten alle im Zusammenhang mit LEXolution.FLOW tätigen Beschäftigten von STP durch eine Dienstanweisung dazu verpflichtet werden, sich nur insoweit Kenntnis von den in LEXolution.FLOW gespeicherten Daten zu verschaffen, als dies zur Erfüllung ihrer Aufgaben erforderlich ist.

Zu diesen Maßnahmen sollte STP auch den für den Betrieb von LEXolution.FLOW eingesetzten Subunternehmer mit Zugang zu den Daten vertraglich verpflichten und die Einhaltung dieser Pflichten ebenfalls regelmäßig kontrollieren. Dies setzt voraus, dass sich STP vertraglich das Recht vorbehält, die Protokolldaten der Zugriffe von Beschäftigten des Cloud-Infrastrukturproviders auf die Systemumgebung von LEXolution.FLOW zu kontrollieren bzw. auf die Protokolldaten Zugriff zu erhalten. Zusätzlich ist die Implementierung einer gegenüber dem Cloud-Infrastrukturprovider wirksamen Verschlüsselung ruhender Daten obligatorisch.

#### **4.1.2.4 Verpflichtung mitwirkender Personen zur Verschwiegenheit (§ 203 Abs. 4 Satz 2 StGB)**

Neben der nicht erforderlichen Offenbarung von Geheimnissen ist es gemäß § 203 Abs. 4 Satz 2 Nr. 1 StGB auch strafbar, wenn der Rechtsanwalt nicht dafür Sorge trägt, dass eine sonstige mitwirkende Person zur Verschwiegenheit ver-

---

<sup>20</sup> Vgl.– allerdings ohne nähere Begründung – auch *Klugmann/Leenen/Salz*, AnwBl Online 2018, 283, 285.

<sup>21</sup> *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 30. Auflage 2019, § 203 StGB Rn. 52.

pflichtet wird, und diese mitwirkende Person unbefugt Geheimnisse offenbart. Dies gilt auch für die Verantwortlichen bei STP, wenn eine durch STP beauftragte sonstige mitwirkende Person nicht zur Verschwiegenheit verpflichtet wird und unbefugt Geheimnisse offenbart (§ 203 Abs. 4 Satz 2 Nr. 3 StGB).

Diese beiden Strafvorschriften beschränken sich nicht auf eine Verpflichtung des jeweiligen Vertragspartners sondern setzen voraus, dass für eine durchgehende Verpflichtungskette Sorge getragen wird. Ausweislich der Gesetzesbegründung bezweckt die Vorschrift, dass dafür Sorge getragen wird, dass die konkret mitwirkenden Personen zur Geheimhaltung verpflichtet werden.<sup>22</sup>

Es reicht folglich nicht aus, wenn sich lediglich STP gegenüber dem Rechtsanwalt zur Verschwiegenheit verpflichtet, bzw. der Cloud-Infrastrukturprovider gegenüber STP. Vielmehr ist es erforderlich, dass sowohl der Kunde wie auch STP dafür Sorge tragen, dass sämtliche in den Betrieb von LEXolution.FLOW eingebundenen Personen, die möglicherweise Kenntnis von dort gespeicherten Geheimnissen erlangen könnten, zur Verschwiegenheit verpflichtet werden.

Vertraglich muss sich STP also selbst gegenüber den Kunden zur Verschwiegenheit verpflichten und zusätzlich die Pflicht übernehmen,

- sämtliche Beschäftigte von STP, die in den Betrieb von LEXolution.FLOW eingebunden werden, zur Verschwiegenheit zu verpflichten sowie
- sämtlichen Subunternehmern, die möglicherweise Zugriff auf die in LEXolution.FLOW gespeicherten Daten nehmen könnten, wie zum Beispiel der Cloud-Infrastrukturprovider, die gleichen vertraglichen Pflichten aufzuerlegen.

Ihre eigenen Subunternehmer, insbesondere den Cloud-Infrastrukturprovider, muss STP vertraglich zur Verschwiegenheit verpflichten und diesen ebenfalls die Pflicht auferlegen,

- sämtliche zur Leistungserbringung eingesetzte Beschäftigte des Subunternehmers, die möglicherweise Zugriff auf die in LEXolution.FLOW gespeicherten Daten nehmen könnten, zur Verschwiegenheit zu verpflichten sowie

---

<sup>22</sup> BT-Drs. 18/11936, S. 21.



- sämtlichen weiteren Subunternehmern, die möglicherweise Zugriff auf die in LEXolution.FLOW gespeicherten Daten nehmen könnten, die gleichen vertraglichen Pflichten aufzuerlegen.

Organisatorisch muss STP dafür Sorge tragen, dass sämtliche mit dem Betrieb von LEXolution.FLOW betraute Beschäftigte dokumentiert zur Verschwiegenheit verpflichtet werden. Zudem sollte die Einhaltung der entsprechenden Pflichten durch die Subunternehmer von STP, sowohl im Hinblick auf deren eigene Beschäftigte wie auch im Hinblick auf gegebenenfalls eingesetzte weitere Subunternehmer, nachweisbar kontrolliert werden.

Inhaltlich sind keine besonderen Anforderungen an die Verpflichtung zu stellen. Es reicht aus, wenn alle sonstigen mitwirkenden Personen allgemein zur Geheimhaltung bzw. Verschwiegenheit verpflichtet werden, wobei dies zum Zwecke des Nachweises dokumentiert werden sollte. Eine darüber hinausgehende Belehrung über die möglichen strafrechtlichen Folgen einer unbefugten Offenbarung von Berufsgeheimnissen, wie sie im Berufsrecht der Rechtsanwälte vorgesehen ist (vgl. hierzu noch unter Ziff. 4.1.3.3 dieses Memorandums), ist zur Erfüllung der sich aus § 203 Abs. 4 Satz 2 Nr. 1 und 3 StGB ergebenden Pflichten nicht erforderlich.<sup>23</sup> Dies ergibt sich aus der Gesetzesbegründung:

*„Dabei kommt es auf die berufsrechtlichen Besonderheiten der Geheimhaltungsverpflichtung – wie etwa in § 43e Absatz 3 Satz 1 und 2 Nummer 1 bis 3 BRAO-E – nicht an. Der Berufsgeheimnisträger kann entweder die mitwirkende Person selbst zur Geheimhaltung verpflichten oder dies auch auf andere übertragen. In mehrstufigen Auftragsverhältnissen kann dies bedeuten, dass der Berufsgeheimnisträger die von ihm beauftragte mitwirkende Person selbst verpflichtet und sie gleichzeitig – beispielsweise durch eine entsprechende vertragliche Vereinbarung – verpflichtet, ihre ausführenden Mitarbeiter oder auch weitere Unterauftragnehmer, soweit der Berufsgeheimnisträger eine Unterauftragung gestattet, auf gleiche Weise zur Geheimhaltung zu verpflichten.“(Hervorhebung nicht im Original).<sup>24</sup>*

#### **4.1.3 Berufsrechtskonformität des Einsatzes von Dienstleistern durch die Nutzung von LEXolution.FLOW**

Für einen berufsrechtskonformen Einsatz von LEXolution.FLOW müssen die sich aus § 43e BRAO und § 2 BORA ergebenden Anforderungen für die Inanspruchnahme von Dienstleistungen durch Rechtsanwälte erfüllt werden, soweit es sich

---

<sup>23</sup> So auch *Eisele*, in: Schönke/Schröder, Strafgesetzbuch, 30. Auflage 2019, § 203 StGB Rn. 102; *Ciernak/Niehaus*, in Münchener Kommentar, StGB, 3. Aufl. 2017, § 203 Rn. 157.

<sup>24</sup> BT-Drs. 18/11936, S. 29.

bei den Kunden um bei einer deutschen Rechtsanwaltskammer zugelassene Rechtsanwälte oder dort registrierte Rechtsanwaltsgesellschaften (vgl. § 59m Abs. 2 BRAO) handelt.

Ein Verstoß ausschließlich gegen berufsrechtliche Regelungen wäre strafrechtlich nicht relevant. Gleichwohl wäre ein Verstoß gegen das Berufsrecht im Zusammenhang mit LEXolution.FLOW eine Berufspflichtverletzung, die berufsrechtlich gegenüber den Kunden – nicht aber gegenüber STP – geahndet werden könnte.

#### **4.1.3.1 Erforderlichkeitsvorbehalt**

Zunächst regelt § 43 Abs. 1 Satz 1 BRAO, dass Dienstleistern nur insoweit Zugang zu Berufsgeheimnissen eröffnet werden darf, wie dies für die Inanspruchnahme der Dienstleistung erforderlich ist. Inhaltlich stellt § 43 Abs. 1 Satz 1 BRAO an die Offenbarung von Berufsgeheimnissen die gleichen Anforderungen wie die strafrechtliche Parallelvorschrift in § 203 Abs. 3 Satz 2 StGB, sodass die Ausführungen unter Ziff.4.1.2.2 dieses Memorandums entsprechend gelten.

Ergänzend hierzu verpflichtet § 2 Abs. 2 BORA den Rechtsanwalt, risikoadäquate technische und organisatorische Maßnahmen zum Schutze des Mandatsgeheimnisses zu ergreifen, sodass auch berufsrechtlich die Implementierung der unter Ziff. 4.1.2.3 beschriebenen Schutzmaßnahmen geboten ist.

#### **4.1.3.2 Inhaltliche Anforderungen an die abzuschließenden Verträge**

Zusätzlich stellt das Berufsrecht – anders als das Strafrecht – in § 43e Abs. 3 BRAO besondere Anforderungen an den zwischen den Kunden und STP abzuschließenden Vertrag.

Zunächst muss dieser gemäß § 43e Abs. 3 Satz 1 BRAO in Textform abgeschlossen werden, wobei die strengere Schriftform ebenfalls den gesetzlichen Anforderungen genügt.<sup>25</sup>

In diesem Vertrag muss der Kunde STP unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit verpflichten (§ 43e Abs. 3 Satz 2 Nr. 1 BRAO) und STP ausdrücklich die Pflicht auferlegen, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist (§ 43e Abs. 3 Satz 2 Nr. 2 BRAO).

---

<sup>25</sup> BT-Drs. 18/11936, S. 35.

Die berufsrechtlichen Pflichten des Kunden gehen also insoweit über die strafrechtlichen Anforderungen hinaus, als dass STP in dem Nutzungsvertrag für LEXolution.FLOW nicht nur allgemein zur Verschwiegenheit, sondern zusätzlich auch zur Einhaltung des Erforderlichkeitsgebots verpflichtet werden muss und über die strafrechtlichen Konsequenzen einer Pflichtverletzung belehrt werden muss. Die Belehrung über die strafrechtlichen Konsequenzen muss sich neben der Strafbarkeit der Verletzung von Privatgeheimnissen nach § 203 StGB auch auf die Strafbarkeit der Verwertung fremder Geheimnisse nach § 204 StGB sowie auf die Strafbarkeit der Verletzung der Vertraulichkeit des Wortes nach § 201 StGB beziehen.<sup>26</sup>

Des Weiteren ist es erforderlich, ausdrücklich die Befugnis von STP zum Einsatz von weiteren Personen zur Leistungserbringung in den Nutzungsvertrag für LEXolution.FLOW aufzunehmen (§ 43e Abs.3 Satz 2 Nr. 3 Var. 1 BRAO). Die entsprechende Regelung sollte sich ausdrücklich auf den Einsatz von eigenen Beschäftigten von STP wie auch auf den Einsatz von Subunternehmern, weiteren Subunternehmern und jeweils deren Beschäftigten beziehen. Berufsrechtlich nicht zwingend erforderlich ist es, die von STP zur Leistungserbringung eingesetzten Subunternehmer ausdrücklich zu benennen; wobei sich jedoch eine entsprechende Pflicht in der Regel aus den zusätzlich zu beachtenden datenschutzrechtlichen Anforderungen an eine Auftragsverarbeitung ergibt (siehe hierzu noch näher unter Ziff. 4.1.4 dieses Memorandums).

Die zur Umsetzung der Anforderung des § 43e Abs. 2 BRAO erforderlichen Regelungen müssen nicht im Hauptdokument des Nutzungsvertrages für LEXolution.FLOW enthalten sein und können auch in einem separaten Dokument zusammengefasst werden. Da § 43e Abs. 2 Satz 1 BRAO jedoch eindeutig eine vertragliche Umsetzung der in § 43e Abs. 2 Satz 2 BRAO geregelten Pflichten fordert, muss darauf geachtet werden, dass das entsprechende Dokument als Anlage in den Nutzungsvertrag für LEXolution.FLOW einbezogen wird. Eine einseitige Verpflichtungserklärung von STP wäre nicht ausreichend.

#### **4.1.3.3 Verpflichtung und Belehrung der Dienstleister sowie ihrer Hilfspersonen**

§ 43e Abs. 2 Satz 2 Nr. 3 Var. 2 BRAO sieht zudem vor, dass der Dienstleister des Rechtsanwalts, also STP, vertraglich dazu verpflichtet werden muss, alle Personen, die der Dienstleister zur Leistungserbringung hinzuzieht, ebenfalls in Textform zur Verschwiegenheit zu verpflichten.

---

<sup>26</sup> Vgl. BT-Drs. 18/11936, S. 31.

Demgemäß muss in dem Nutzungsvertrag für LEXolution.FLOW geregelt werden, dass STP seine eigenen Beschäftigten und sämtliche Subunternehmer, die im Zusammenhang mit LEXolution.FLOW tätig werden, in Textform zur Verschwiegenheit verpflichtet.

**a) Verpflichtung zur Weitergabe der Pflichten in der Kette der (Sub-)Subunternehmer**

Nicht eindeutig geregelt ist jedoch, ob sich der Dienstleister, also STP, gegenüber dem Rechtsanwalt darüberhinausgehend vertraglich dazu verpflichten muss, seinen zur Leistungserbringung eingesetzten Subunternehmern vertraglich die gleichen Pflichten aufzuerlegen (d. h. diesen aufzugeben, dass auch sie ihre (Sub-)Subunternehmer und ihre Beschäftigten entsprechend verpflichten).

Zwar spricht der Wortlaut der Vorschrift eher dafür, dass der Dienstleister des Rechtsanwalts, also STP, lediglich dazu verpflichtet ist, die eigenen Beschäftigten und die unmittelbar für STP tätigen Subunternehmer zur Verschwiegenheit zu verpflichten, allerdings würde dies dem Sinn und Zweck der Regelung, nämlich nur einem geschlossenen Kreis von zur Verschwiegenheit verpflichteten Personen Zugang zu den Mandatsgeheimnissen zu gewähren, nicht vollständig gerecht werden. Des Weiteren folgt bereits aus der strafrechtlichen Parallelvorschrift in § 203 Abs. 4 StGB die Pflicht, dafür Sorge zu tragen, dass sämtliche konkret an der Leistungserbringung mitwirkenden Personen zur Verschwiegenheit verpflichtet werden. Es spricht damit Überwiegendes dafür, dass die unter Ziff. 4.1.2.4 dieses Memorandums erläuterten vertraglichen Regelungen zur Weiterreichung der Verschwiegenheitspflichten in der Leistungskette auch gemäß § 43e Abs. 2 Satz 2 Nr. 3 BRAO obligatorisch sind. Zur Einhaltung des in § 43e Abs. 2 Satz 2 Nr. 3 Var. 2 BRAO geregelten Formerfordernisses muss in dem Nutzungsvertrag für LEXolution.FLOW und in den Verträgen, die STP mit seinen Subunternehmern abschließt, geregelt werden, dass alle Verpflichtungen zur Verschwiegenheit in Textform erfolgen.

**b) Inhalt der Verpflichtung**

Bezüglich des Inhalts der Verpflichtung der Beschäftigten bzw. der Subunternehmer von STP sieht § 43e Abs. 2 Satz 2 Nr. 3 BRAO seinem Wortlaut nach lediglich vor, dass diese zur Verschwiegenheit zu verpflichten sind. Die Pflicht, diese zusätzlich über die strafrechtlichen Folgen einer Pflichtverletzung zu belehren und/oder diese zu verpflichten, sich nur insoweit Kenntnis von den Berufsgeheimnissen zu verschaffen wie dies für die Ausübung ihrer Tätigkeiten erforderlich ist, wird hingegen in § 43e Abs. 2 Satz 2 Nr. 3 BRAO, anders als in § 43e Abs. 2 Satz 2 Nr. 1 und 2 BRAO, nicht erwähnt.

Ob diese unterschiedliche Reichweite des Pflichtenkreises des Rechtsanwaltes gegenüber dem Dienstleister (§ 43e Abs. 2 Satz 2 Nr. 1 und 2 BRAO) und des Dienstleisters gegenüber seinem Personal und seinen Subunternehmern (§ 43e Abs. 2 Satz 2 Nr. 3 BRAO) eine bewusste gesetzgeberische Entscheidung ist, kann anhand der Gesetzeshistorie nicht eindeutig ermittelt werden.

Es spricht jedoch Überwiegendes dafür, dass es sich hierbei um ein Redaktionsversehen des Gesetzgebers handelt, denn die Belehrung über die strafrechtlichen Konsequenzen von Verstößen gegen die Verschwiegenheitsverpflichtung macht vor allem gegenüber den konkret handelnden Personen, also den Beschäftigten des Dienstleisters und den zur Leistungserbringung eingesetzten Subunternehmern, Sinn. Zudem ist der Rechtsanwalt selbst verpflichtet, seine eigenen Beschäftigten nicht nur zur Verschwiegenheit zu verpflichten, sondern diese auch über die strafrechtlichen Folgen einer Pflichtverletzung zu belehren (§ 43a Abs. 2 BRAO). Im Hinblick auf die mögliche Gefährdung der Vertraulichkeit durch die Mitwirkung von Hilfspersonen an der Tätigkeit des Rechtsanwalts macht es aber keinen Unterschied, ob es sich bei den Hilfspersonen um eigene Beschäftigte des Rechtsanwalts handelt oder aber um Beschäftigte des Dienstleisters oder seiner Subunternehmer.

Zwar gibt es bislang, soweit ersichtlich, keine publizierten gerichtlichen Entscheidungen oder Stellungnahmen der Rechtsanwaltskammern zu dieser Thematik. Sollte jedoch eine Rechtsanwaltskammer zu der Auffassung gelangen, dass die allgemeine Verpflichtung zur Verschwiegenheit nicht ausreichend ist, und auch die in § 43e Abs. 2 Satz 2 Nr. 1 und 2 BRAO geregelten zusätzlichen Belehrungspflichten entlang der Leistungskette weiterzureichen sind, bestünde kein Bestandsschutz. Insbesondere die vertraglichen Vereinbarungen mit dem Cloud-Infrastrukturprovider müssten dann entsprechend angepasst und umgesetzt werden, um den berufsrechtskonformen Betrieb von LEXolution.FLOW weiter zu gewährleisten. Vor diesem Hintergrund sollte für die weitere Konzeption von LEXolution.FLOW und die Vertragsverhandlungen mit den Subunternehmern unterstellt werden, dass die sich aus § 43e Abs. 2 Satz 2 Nr. 1 und Nr. 2 BRAO ergebenden Pflichten auch an die Subunternehmer von STP und von den Subunternehmern an ihre weiteren Subunternehmer weitergereicht werden müssen.

Dies unterstellt, muss sich STP also selbst gegenüber den Kunden vertraglich zur Verschwiegenheit verpflichten und zusätzlich die Pflicht übernehmen,

- sämtliche Beschäftigte von STP, die in den Betrieb von LEXolution.FLOW eingebunden sind in Textform,
  - zur Verschwiegenheit zu verpflichten,

- zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Erfüllung ihrer Aufgaben erforderlich ist,
- über die strafrechtlichen Konsequenzen einer Pflichtverletzung zu belehren

sowie

- sämtlichen Subunternehmern, die im Zusammenhang mit LEXolution.FLOW tätig werden sollen, die gleichen vertraglichen Pflichten aufzuerlegen und
- diese zu verpflichten, die gleichen vertraglichen Pflichten jeweils ihren weiteren Subunternehmern aufzuerlegen.

Ihre eigenen Subunternehmer, insbesondere den Cloud-Infrastrukturprovider, muss STP mindestens in Textform

- unter Belehrung über die strafrechtlichen Folgen von Pflichtverstößen vertraglich zur Verschwiegenheit verpflichten,
- vertraglich verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Erfüllung ihrer Aufgaben erforderlich ist,

und diesen jeweils zusätzlich die Pflicht auferlegen,

- sämtliche Beschäftigte des Subunternehmers, die in den Betrieb von LEXolution.FLOW eingebunden sind, in Textform
  - zur Verschwiegenheit zu verpflichten,
  - zu verpflichten, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Erfüllung ihrer Aufgaben erforderlich ist,
  - über die strafrechtlichen Konsequenzen einer Pflichtverletzung zu belehren

sowie

- sämtlichen weiteren Subunternehmern, die im Zusammenhang mit LEXolution.FLOW tätig werden sollen, die gleichen vertraglichen Pflichten aufzuerlegen.

#### **4.1.4 Datenschutzkonformität von LEXolution.FLOW**

##### **4.1.4.1 Abschluss einer Auftragsverarbeitungsvereinbarung mit den Kunden**

Mit allen Kunden, die LEXolution.FLOW nutzen wollen, muss STP vor dem erstmaligen Einsatz von LEXolution.FLOW durch den jeweiligen Kunden gemäß Art. 28 Abs. 3 Satz 1 DS-GVO eine Auftragsverarbeitungsvereinbarung abschließen. Dies gilt auch für eine lediglich vorübergehende Nutzung von LEXolution.FLOW im Rahmen einer Testphase o. Ä.

Die datenschutzrechtlichen Vorschriften sind neben den berufsrechtlichen Vorschriften anwendbar, insbesondere ersetzt eine Vereinbarung gemäß § 43e Abs. 3 BRAO nicht die datenschutzrechtlich erforderliche Auftragsverarbeitungsvereinbarung (§ 43 Abs. 8 BRAO).

Die Auftragsverarbeitungsvereinbarung muss nicht zwingend als separates Dokument abgefasst sein. Es ist ausreichend, die Auftragsverarbeitungsvereinbarung als Anlage zu dem Nutzungsvertrag für LEXolution.FLOW in das Vertragsverhältnis mit dem Kunden einzubeziehen.

In der Auftragsverarbeitungsvereinbarung müssen Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen im Zusammenhang mit LEXolution.FLOW beschrieben werden (vgl. Art. 28 Abs. 3 Satz 1 DS-GVO). Zudem müssen die in Art. 28 Abs. 3 Satz 2 DS-GVO geregelten inhaltlichen Anforderungen erfüllt werden:

*„Dieser Vertrag [...] sieht insbesondere vor, dass der Auftragsverarbeiter*

*a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;*

- b) *gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;*
- c) *alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;*
- d) *die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;*
- e) *angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;*
- f) *unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;*
- g) *nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht;*
- h) *dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.“*

#### **4.1.4.2 Abschluss einer Auftragsverarbeitungsvereinbarung mit den Subunternehmern von STP**

Ferner muss STP mit allen Subunternehmern, die im Zusammenhang mit LEXolution.FLOW personenbezogene Daten verarbeiten, insbesondere mit dem Cloud-Infrastrukturprovider, Auftragsverarbeitungsvereinbarungen abschließen. Gemäß Art. 28 Abs. 4 DS-GVO müssen den Subunternehmern grundsätzlich „*dieselben Datenschutzpflichten*“ auferlegt werden, die in der Auftragsverarbeitungsvereinbarung zwischen LEXolution.FLOW und ihren Kunden geregelt sind. Dies macht es erforderlich, die mit den Kunden abzuschließende Auftragsverarbeitungsvereinbarung zu standardisieren und diese inhaltlich mit den Auftragsverarbeitungsvereinbarungen, die STP mit seinen Subunternehmern abschließt, abzustimmen.



Vor diesem Hintergrund ist es schwierig für STP, individuelle Vorschläge von Kunden für Auftragsverarbeitungsvereinbarungen zu akzeptieren. Zudem sollte berücksichtigt werden, dass die überwiegende Anzahl der Kunden aufgrund der Sensibilität der mithilfe von LEXolution.FLOW verarbeiteten Daten wohl verhältnismäßig hohe Anforderungen an den Inhalt der Auftragsverarbeitungsvereinbarung stellen wird. Es sollte deshalb bei dem Entwurf der Muster-Auftragsverarbeitungsvereinbarung für die Kunden darauf geachtet werden, dass diese möglichst ausgewogene Regelungen enthält.

## **4.2 Erfüllbarkeit einzelner rechtlicher Pflichten des Kunden im Zusammenhang mit der Nutzung von LEXolution.FLOW**

### **4.2.1 Berufsrechtliche Pflicht anwaltlicher Nutzer**

#### **4.2.1.1 Führung einer Handakte**

Der als Rechtsanwalt tätige Kunde ist nach Maßgabe von § 50 BRAO dazu verpflichtet, Handakten zu führen, die ein geordnetes und zutreffendes Bild über die Bearbeitung seiner Aufträge geben. Gemäß § 50 Abs. 4 BRAO ist es dem Rechtsanwalt gestattet, seine Handakten digital zu führen.

Hierbei ist allerdings zu beachten, dass auch bei der Führung einer digitalen Handakte eine geordnete Aktenführung in Form eines zusammenhängenden, und revisions sicheren Vorgangs für jedes Mandat, zu dem alle mandatsrelevanten Dokumente und Dateien genommen werden, gewährleistet sein muss. Dies setzt grundsätzlich die Verwendung eines Dokumentenmanagementsystems (DMS) voraus. LEXolution.FLOW ist eine Workflow-Engine, die nicht über die Funktionalitäten eines DMS verfügt und ist deshalb nicht für die Führung von Handakten geeignet.

Vor diesem Hintergrund ist es erforderlich, für die Mandate, die mithilfe von LEXolution.FLOW bearbeitet werden, separate Handakten in einer anderen Applikation zu führen. Die hierfür benötigten Daten aus dem Kundenbereich des Kunden in LEXolution.FLOW können mit der dort zur Verfügung stehenden Exportfunktion in die Handakte kopiert werden, sodass LEXolution.FLOW in Konformität mit § 50 BRAO genutzt werden kann.

Zusätzlich wäre es sinnvoll in LEXolution.FLOW durch Vorkehrungen, wie zum Beispiel die doppelte Bestätigung einer Löschung, abzusichern, dass keine für die Handakte relevanten Daten versehentlich gelöscht werden.

#### **4.2.1.2 Verschwiegenheit anwaltlicher Nutzer**

Der als Rechtsanwalt tätige Kunde unterliegt – wie dargestellt – berufsrechtlichen Verschwiegenheitspflichten.

Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt nach § 2 Abs. 2 BORA,

„Die Verschwiegenheitspflicht gebietet es dem Rechtsanwalt, die zum Schutze des Mandatsgeheimnisses erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen, die risikoadäquat und für den Anwaltsberuf zumutbar sind.<sup>2</sup> Technische Maßnahmen sind hierzu ausreichend, soweit sie im Falle der Anwendbarkeit der Vorschriften zum Schutz personenbezogener Daten deren Anforderungen entsprechen.<sup>3</sup> Sonstige technische Maßnahmen müssen ebenfalls dem Stand der Technik entsprechen.<sup>4</sup> Abs. 4 lit. c) bleibt hiervon unberührt.<sup>5</sup> Zwischen Rechtsanwalt und Mandant ist die Nutzung eines elektronischen oder sonstigen Kommunikationsweges, der mit Risiken für die Vertraulichkeit dieser Kommunikation verbunden ist, jedenfalls dann erlaubt, wenn der Mandant ihr zustimmt.<sup>6</sup> Von einer Zustimmung ist auszugehen, wenn der Mandant diesen Kommunikationsweg vorschlägt oder beginnt und ihn, nachdem der Rechtsanwalt zumindest pauschal und ohne technische Details auf die Risiken hingewiesen hat, fortsetzt.“

Welche technischen Maßnahmen als erforderlich, risikoadäquat und für den Anwaltsberuf zumutbar sind, ist im Wesentlichen eine technische Frage und nicht Gegenstand dieses Memorandums.

Für einen erfolgreichen Vertrieb von LEXolution.FLOW empfehlen wir jedoch, den als Rechtsanwalt tätigen Kunden die Möglichkeit zur Verschlüsselung von mittels LEXolution.FLOW versandten E-Mails zu bieten, so dass diese auch dann ihrer oben genannten Pflicht aus § 2 Abs. 2 BORA genügen können, wenn ihr Mandant nicht gemäß § 2 Abs. 5 BORA der unverschlüsselten Übermittlung zugestimmt oder die Zustimmung nach § 2 Abs. 6 BORA unterstellt wird.

#### **4.2.2 Datenschutzrechtliche Pflichten**

##### **4.2.2.1 Erfüllbarkeit der Informationspflicht gegenüber den Nutzern**

###### **a) Nutzung von LEXolution.FLOW durch den Kunden**

Ob, in welchem Umfang und zu welchen Zwecken personenbezogene Daten in seinem Kundenbereich in LEXolution.FLOW verarbeitet werden, bestimmt der Kunde, sodass er als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO die Nutzer seines Kundenbereichs über die Verarbeitung sie betreffender personenbe-

zogener Daten gemäß Art. 13, 14 DS-GVO informieren muss (nachfolgend auch **“Datenschutzerklärung“**). Diese Informationspflicht besteht sowohl gegenüber den Nutzern, die als Mandanten auf das Mandantenportal zugreifen, wie auch gegenüber sonstigen Nutzern, die das Back-End von LEXolution.FLOW nutzen, wie zum Beispiel die Mitarbeiter des Kunden.

Die gemäß Art. 13, 14 DS-GVO zu erteilenden Informationen beziehen sich nicht auf die Applikationen LEXolution.FLOW als solche, sondern auf die Datenverarbeitung, die der Kunde mithilfe von LEXolution.FLOW durchführt. Beispielsweise muss darüber informiert werden, für welche Zwecke der Kunde personenbezogene Daten in seinem Kundenbereich in LEXolution.FLOW verarbeitet, welche Kategorien personenbezogener Daten von ihm verarbeitet werden und auf welcher Rechtsgrundlage dies geschieht.

Da es sich bei LEXolution.FLOW um eine Workflow-Engine handelt, mit der ganz unterschiedliche Prüf-, Beratungs- und Entscheidungsprozesse in Rechtsanwaltskanzleien modelliert werden können, ist es für STP nicht möglich, eine Muster-Datenschutzerklärung für LEXolution.FLOW bereitzustellen: Der Kunde bestimmt frei darüber, wofür er LEXolution.FLOW nutzt und welche personenbezogenen Daten er in diesem Zusammenhang verarbeitet, sodass nur der Kunde die gemäß Art. 13, 14 DS-GVO speziell für seinen Anwendungsfall erforderlichen Informationen zusammenstellen kann.

Bei der Bereitstellung der Datenschutzerklärung sind die sich aus Art. 12 DS-GVO ergebenden Anforderungen an die Modalitäten der Kommunikation mit den Nutzern zu berücksichtigen. Insbesondere muss die Datenschutzerklärung den Nutzern in *„einer präzisen, verständlichen und leicht zugänglicher Form“* sowie in *„klarer und einfacher Sprache“* übermittelt werden (Art. 12 Abs. 1 S. 1 DS-GVO).

Hierfür stehen in LEXolution.FLOW hinreichende Funktionen zur Verfügung: Zum einen bietet die grafische Oberfläche des Mandantenportals und des Back-Ends die Möglichkeit, dort in der Menüleiste dauerhaft eine Datenschutzerklärung zu verlinken. Diese Verlinkung führt zu einem Freitextfeld, das dem Kunden eine seinen eigenen Standards entsprechende, adressatengerechte Information der Nutzer ermöglicht. Ferner kann die Datenschutzerklärung den Nutzern zusätzlich auch mithilfe der in LEXolution.FLOW integrierten Benachrichtigungsfunktion per E-Mail übersandt werden.

In zeitlicher Hinsicht ist zu beachten, dass die Datenschutzerklärung den Nutzern spätestens zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten bereitgestellt werden muss (Art. 13 Abs. 1 DS-GVO). Da die Verarbeitung bereits mit dem erstmaligen Aufruf des Kundenbereichs durch den Nutzer beginnt, muss der

Kunde die Möglichkeit haben, bereits vor seiner Registrierung auf die Datenschutzerklärung zugreifen zu können. Dies kann durch die Nutzung der im Menü der Benutzeroberfläche bereitgestellten Verlinkungsfunktion gewährleistet werden.

Nicht erforderlich ist es, dass die Nutzer ihr Einverständnis mit der Datenschutzerklärung, insbesondere im Rahmen des Registrierungsprozesses durch das Anklicken einer Checkbox o. Ä., ausdrücklich erklären oder deren Kenntnisnahme bestätigen (siehe zum Beispiel die Abbildung der Muster-Selbstregistrierung eines Nutzers unter Ziffer 1.1.3). Insofern sollte zur Vermeidung einer Fehlvorstellung der Nutzer über die rechtliche Bedeutung der Datenschutzerklärung, die lediglich eine einseitige Mitteilung des Verantwortlichen an den Nutzer ist, darauf verzichtet werden, eine Erklärung der Nutzer einzuholen und stattdessen nur mit einer einfachen Verlinkung auf die Datenschutzerklärung im Rahmen des Registrierungsprozesses auf diese hingewiesen werden.

Zudem sollte keinesfalls pauschal eine „Zustimmung“ des Nutzers zur Verarbeitung seiner personenbezogenen Daten im Rahmen der Registrierung eingeholt werden (siehe zum Beispiel die Abbildung der Muster-Selbstregistrierung eines Nutzers unter Ziffer 1.1.3), wenn zur Rechtfertigung der Datenverarbeitung gemäß Art. 6/ Art. 9 DS-GVO nicht tatsächlich auf die Einwilligung zurückgegriffen werden muss (siehe hierzu noch näher unter Ziffer 4.2.2.9a)). Eine solche Formulierung würde nämlich dem Transparenzgebot widersprechen, da der Nutzer aufgrund eines Widerspruchs zwischen der Angabe auf der Registrierungsseite und zur Rechtsgrundlage in der vom Kunden genutzten Datenschutzerklärung nicht zweifelsfrei feststellen könnte, auf welcher Rechtsgrundlage die Verarbeitung seiner personenbezogenen Daten bei Nutzung von LEXolution.FLOW tatsächlich basiert.

Zudem sind bei einer solchen Gestaltung auch nicht die datenschutzrechtlichen Anforderungen an eine wirksame Einwilligung erfüllt. Die „Zustimmung“ des Nutzers würde damit nicht die datenschutzrechtlichen Wirkungen einer Einwilligung entfalten.

**b) Ausnahme: Protokolldaten**

Anders als die Verarbeitung personenbezogener Daten im Kundenbereich, wird die Protokollierung von Aufrufen von LEXolution.FLOW nicht vom Kunden, sondern von STP gesteuert. Demgemäß bestimmt STP insoweit über Zweck und Mittel der Verarbeitung und ist insoweit als Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO zu qualifizieren. Es ist damit die Pflicht von STP, die Nutzer über die mit

der Protokollierung verbundene Verarbeitung personenbezogener Daten gemäß Art. 13, 14 DS-GVO zu informieren.

Vor diesem Hintergrund ist es erforderlich, neben der vom Kunden zu erstellenden Datenschutzerklärung für seinen Kundenbereich auch die gemäß Art. 13, 14 DS-GVO für die Zugriffsprotokollierung erforderlichen Informationen dauerhaft in der Benutzeroberfläche von LEXolution.FLOW zu verankern. Insofern ist es nicht zwingend erforderlich, einen weiteren separaten Menüpunkt einzuführen. Zweckmäßigerweise können diese Informationen auch als nicht editierbares Element in die unter dem Menüpunkt „Datenschutzerklärung“ abrufbare Oberfläche integriert werden. Bei dieser Gestaltungsvariante muss jedoch darauf geachtet werden, dass der entsprechende Menüpunkt in jeder Ansicht verfügbar ist und vom Kunden auch nicht deaktiviert werden kann. Zudem muss transparent dargestellt werden, dass die Zugriffsprotokollierung in die Verantwortungssphäre von STP fällt und der Kunde insoweit nicht im Übrigen aber doch für die Datenverarbeitung verantwortlich ist.

#### **4.2.2.2 Erfüllbarkeit von Auskunftersuchen (Art. 15 DS-GVO)**

Gemäß Art. 15 DS-GVO hat der Verantwortliche auf Antrag einer natürlichen Person Auskunft darüber zu erteilen, ob er die personenbezogenen Daten dieser natürlichen Person verarbeitet sowie über

*„(i) die Verarbeitungszwecke (ii) die Kategorien personenbezogener Daten, die verarbeitet werden, (iii) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen, (iv) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer, (v) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung, (vi) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde, (vii) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten und (viii) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“.*

Soweit ein solcher Antrag von Personen gestellt wird, die nicht Mitarbeiter oder Mandanten des Kunden sind, kann der Kunde die Auskunftserteilung verweigern, soweit er in diesem Zusammenhang Informationen offenbaren müsste, die dem Mandatsgeheimnis unterliegen (§ 29 Abs. 1 Satz 2 BDSG).

Jedenfalls muss der Kunde jedoch dazu der Lage sein, seinen Mandanten, die das Mandantenportal nutzen, sowie gegebenenfalls seinen Mitarbeitern, die den Kundenbereich des Kunden in LEXolution.FLOW betreuen, gemäß Art. 15 DS-GVO Auskunft zu erteilen. Da der Kunde im Back-End seines Kundenbereichs auf alle in seinem Kundenbereich gespeicherten Informationen zugreifen kann, ist es ihm grundsätzlich möglich, die für eine Auskunftserteilung erforderlichen Informationen dort zusammenzusuchen.

Praktisch stellt sich allerdings gerade bei einer umfangreichen Nutzung von LEXolution.FLOW durch den Kunden das Problem, dass der Kunde alle Informationen zu einer bestimmten Person im Rahmen einer manuellen Sichtung des Datenbestandes im Back-End nicht oder häufig nur unvollständig erfassen kann.

Vor diesem Hintergrund sollte in Betracht gezogen werden, dem Kunden Filter- und Suchfunktionen in LEXolution.FLOW zur Verfügung zu stellen, damit dieser Auskunftersuchen auch bei großen Datenbeständen effektiv bearbeiten kann.

Neben der Erteilung einer Auskunft haben die betroffenen Personen einen Anspruch darauf, eine „Kopie“ der von ihnen verarbeiteten personenbezogenen Daten zu erhalten (Art. 15 Abs. 3 DS-GVO). Auch wenn es im Detail umstritten ist, was genau eine Kopie im Sinne dieser Vorschrift ist und unter welchen Voraussetzungen eine Herausgabe verweigert werden kann, gibt Art. 15 Abs. 3 DS-GVO der betroffenen Person nach herrschender Auffassung das Recht, von dem Verantwortlichen, hier also dem Kunden, die Herausgabe eines Datensatzes zu verlangen, der die von der betroffenen Person verarbeiteten personenbezogenen Daten so darstellt, wie sie auch dem Kunden in seinem Kundenbereich vorliegen (vgl. Schmidt-Wudy, in: BeckOK Datenschutzrecht, 31. Edition, Stand: 01.02.2020, Art. 15 DS-GVO Rn. 85).

Praktisch bedeutet dies, dass der Kunde eine Exportfunktion benötigt, die es ihm erlaubt, sämtliche Falldaten, Stammdaten und Nutzungsdaten aus seinem Kundenbereich in LEXolution.FLOW exportieren zu können. Eine solche Exportfunktion ist, wie im Sachverhalt beschrieben, in das Back-End von LEXolution.FLOW integriert, so können Nutzern mit entsprechenden administrativen Rechten Daten von aus LEXolution.FLOW als PDF- oder CSV-Datei exportieren.

Über die Verarbeitung der Protokolldaten muss STP als insoweit Verantwortliche gemäß Art. 15 DS-GVO Auskunft erteilen. Da sich jedoch in der Praxis die Nutzer

wahrscheinlich zunächst nur an den Kunden wenden werden, wäre es sinnvoll, mit den Kunden vertraglich einen standardisierten Prozess zu vereinbaren, in dem Nutzeranfragen mit Blick auf die Verarbeitung der Protokolldaten bearbeitet werden. Insofern wäre es zweckmäßig, den Kunden einen Baustein für die Beantwortung entsprechender Anfragen von Nutzern zur Verfügung zu stellen, in dem die nach Art. 15 Abs. 1 DS-GVO erforderlichen Informationen erhalten sind und in dem im Übrigen für die Herausgabe einer Kopie gemäß Art. 15 Abs. 3 DS-GVO auf STP verwiesen wird.

#### **4.2.2.3 Erfüllbarkeit des Rechts auf Berichtigung (Art. 16 DS-GVO)**

Nach Art. 16 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person ferner das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Die Berichtigung hat dadurch zu erfolgen, dass die gespeicherten Daten in Übereinstimmung mit der Realität gebracht werden (*Herbst*, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Art. 16 DS-GVO Rn. 18). Dies hat abhängig von den Umständen des Einzelfalls durch Berichtigung der Daten oder durch die vollständige oder teilweise Löschung oder die Vervollständigung unvollständiger Daten zu erfolgen.

Aufgrund der Editierbarkeit der in LEXolution.FLOW gespeicherten Daten mithilfe der Back-End-Funktion kann der Kunde ohne Mitwirkung von STP Ansprüche der Nutzer auf Datenberichtigung selbst erfüllen, soweit diese die Falldaten und die Stammdaten der Nutzer betreffen. Sofern im Einzelfall eine direkte Editierung in LEXolution.FLOW nicht möglich sein sollte, weil zum Beispiel in LEXolution.FLOW gespeicherte PDF-Dokumente geändert werden müssen, können diese per Exportfunktion extrahiert, außerhalb von LEXolution.FLOW bearbeitet und anschließend wieder in den Kundenbereich eingestellt werden.

Im Hinblick auf die Protokolldaten müsste wiederum STP für eine ggf. notwendige Berichtigung Sorge tragen, wobei es in der Praxis wohl in der Regel keine im Sinne des Art. 16 DS-GVO unrichtigen Protokolldaten geben wird, da die Protokolldaten lediglich Informationen darüber erhalten und darüber Auskunft geben sollen, welche Interaktionen unter welcher (tatsächlichen oder vorgegebenen) Nutzerberechtigung vorgenommen wurden. Die Daten über eine protokollierte Nutzung eines Nutzers wären mithin auch dann „richtig“, wenn die protokollierte

Nutzung nicht durch den protokollierten Nutzer selbst erfolgt wäre, sondern durch einen Dritten, der sich dessen Nutzerkontos bemächtigt hat.

#### **4.2.2.4 Erfüllbarkeit der Löschpflicht (Art. 17 DS-GVO)**

Nach Art. 17 Abs. 1 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Art. 17 Abs. 1 DS-GVO aufgeführten Gründe zur Löschung erfüllt ist. Spiegelbildlich zu diesem Recht besteht eine Pflicht des Verantwortlichen zur unverzüglichen Löschung der personenbezogenen Daten, wenn die besagten Gründe zur Löschung vorliegen. Von diesen Gründen der Löschung dürften im Zusammenhang mit LEXolution.FLOW vor allem die folgenden maßgeblich sein:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 lit. a) DS-GVO [...] stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt gemäß Art. 21 Abs. 1 DS-GVO Widerspruch gegen die Verarbeitung ein, und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Art. 21 Abs. 2 DS-GVO Widerspruch gegen die Verarbeitung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

Das Recht auf Löschung und die Löschpflicht besteht trotz Vorliegen der vorstehend genannten Voraussetzungen nicht, wenn eine der Ausnahmen in Art. 17 Abs. 3 DS-GVO eingreift. Gleiches gilt, wenn eine Ausnahme des § 35 BDSG eingreift, die vom deutschen Gesetzgeber unter Rückgriff auf die Beschränkungsmöglichkeit des Art. 23 DS-GVO erlassen wurde.

Da sich LEXolution.FLOW aus technischen Gründen nicht für die Dokumentation der anwaltlichen Tätigkeit eignet (siehe hierzu bereits unter Ziff. 4.2.1), ist die Zeitspanne, für die in LEXolution.FLOW verarbeitete personenbezogene Daten aus berufsrechtlichen Gründen und/oder zur Abwehr zivilrechtlicher Ansprüche aufbewahrt werden müssen, kein geeigneter Maßstab für die Bestimmung der Dauer, für die personenbezogene Daten allgemein in LEXolution.FLOW gespeichert werden dürfen.



Vielmehr hängt es von dem Zweck des einzelnen in LEXolution.FLOW modellierten Workflows ab, wie lange die in diesem Rahmen verarbeiteten personenbezogenen Daten in LEXolution.FLOW vorgehalten werden dürfen. Da in LEXolution.FLOW ganz unterschiedliche Prüf-, Beratungs- und Entscheidungsprozesse in Rechtsanwaltskanzleien modelliert werden können, ist es für STP nicht möglich, eine generische Löschroutine in LEXolution.FLOW zu implementieren. Der Kunde muss im Einzelfall bestimmen, wie lange die Daten in LEXolution.FLOW für die von ihm in seinem Kundenbereich angelegten Workflows gespeichert werden können. Entsprechendes gilt für die Dauer der Speicherung der Stamm – und Nutzungsdaten.

Art. 17 DS-GVO beinhaltet keine Pflicht, die Löschung von personenbezogenen Daten zu automatisieren, sodass der Kunde LEXolution.FLOW grundsätzlich auch dann rechtmäßig nutzen kann, wenn er die dort gespeicherten personenbezogenen Daten manuell für eine Löschung auswählen muss. Für die Umsetzung einer solchen manuellen Löschung der Falldaten steht dem Kunden im Back-End seines Kundenbereichs bereits die Bearbeitungsfunktion zur Verfügung. Im Hinblick auf die Stammdaten kann eine Löschung durch Löschung des Benutzers manuell vorgenommen werden.

Für die Nutzungsdaten muss dem Kunden in LEXolution.FLOW ebenfalls eine Funktion zur Verfügung gestellt werden, die es ihm ermöglicht, diese nach eigenem Ermessen zu löschen.

Gleichwohl legt Art. 25 Abs. 1 DS-GVO dem Verantwortlichen, also dem Kunden, die Pflicht auf,

*„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 [...] geeignete technische und organisatorische [zu treffen, ...] die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“.*

Aus dieser Pflicht zur Absicherung der Einhaltung des Datenschutzes durch Technikgestaltung (Privacy by Design) ergibt sich, dass zumindest im Fall einer umfangreichen Nutzung von LEXolution.FLOW, bei der die nicht automatisierte Löschung zur Erfüllung der sich aus Art. 17 DS-GVO ergebenden Löschpflicht mit vertretbarem personellen Aufwand nicht mehr sicher gewährleistet werden kann,

der Kunde mit Funktionen unterstützt werden muss, die ihm eine Automatisierung der Löschung von Daten in seinem Kundenbereich ermöglichen. Es sollte für den Kunden deshalb prospektiv möglich sein, für einzelne Workflow-Elemente und für einzelne Kategorien von Dateien und Dokumenten bei der Workflow-Modellierung Fristen bestimmen zu können, nach deren Ablauf die betreffenden Inhalte automatisch gelöscht werden.

Zudem muss sowohl bei einer manuellen Löschung wie auch bei einer automatisierten Löschung technisch eine physikalische Löschung der betreffenden Daten gewährleistet werden. Die bloße (logische) „Löschung“ eines Datensatzes, beispielsweise durch Entfernung von Verweisen aus der Mandanten-/der Kundensicht oder sonstigen sichtbaren Teilen von LEXolution.FLOW auf die dazugehörigen Datenbankeinträge genügt der sich aus Art. 17 DS-GVO ergebenden Löschpflicht nicht. Vor diesem Hintergrund sollte STP für seine Kunden ein Whitepaper o. Ä. vorhalten, in dem in Abstimmung mit dem Cloud-Infrastrukturprovider die technische Umsetzung der Löschung von Daten beschrieben wird, damit dokumentiert werden kann, dass diese tatsächlich unverzüglich nach der Auslösung einer Löschung durch den Kunden physikalisch gelöscht werden.

#### **4.2.2.5 Erfüllbarkeit des Rechts auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)**

Nach Art. 18 Abs. 1 DS-GVO hat *„jede betroffene Person [...] das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen“*, wenn eine der in Art. 18 Abs. 1 DS-GVO aufgezählten Fälle – wie beispielsweise das Bestreiten der Richtigkeit der personenbezogenen Daten durch die betroffene Person – gegeben ist. Der Anspruch auf Einschränkung muss von der betroffenen Person geltend gemacht werden. Eine Pflicht des Verantwortlichen, ohne Antrag des Betroffenen die Verarbeitung einzuschränken, besteht nach Art. 18 DS-GVO nicht.

Unter „Einschränkung“ im Sinne des Art. 18 DS-GVO ist nach der Legaldefinition in Art. 4 Nr. 3 DS-GVO die *„Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken“* zu verstehen. Wurde die Verarbeitung entsprechend Art. 18 Abs. 1 DS-GVO eingeschränkt, dürfen die Daten – von ihrer Speicherung abgesehen – gemäß Art. 18 Abs. 2 DS-GVO nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden.

Nutzer mit höheren Nutzungsrechten können in Lexolution.Flow gespeicherte Daten selektiv für die weitere Verarbeitung durch Nutzer mit niedrigeren Nut-

zungsrechten sperren. Durch eine entsprechende Rechtevergabe und Ausgestaltung seines Prozesses zur Bearbeitung von Anträgen betroffener Personen auf Einschränkung der Verarbeitung ihrer personenbezogenen Daten kann der Kunde mithilfe dieser Funktion seiner sich aus Art. 18 Abs. 1 DS-GVO ergebenden Pflichten nachkommen.

#### **4.2.2.6 Erfüllbarkeit der Mitteilungspflicht (Art. 19 DS-GVO)**

Der Verantwortliche hat nach Art. 19 DS-GVO allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Art. 16, Art. 17 Abs. 1 und Art. 18 DS-GVO mitzuteilen.

Abweichend von diesem Grundsatz besteht die Mitteilungspflicht nicht, wenn sich die Mitteilung als unmöglich erweist oder mit einem unverhältnismäßigen Aufwand verbunden ist.

Darüber hinaus hat der Verantwortliche die betroffene Person über diese Empfänger zu unterrichten, wenn die betroffene Person dies verlangt.

Ziel der Mitteilungspflicht ist es, den Empfängern der Daten die Erfüllung ihrer Pflichten nach den Art. 16, 17 oder 18 DS-GVO zu ermöglichen, wenn ihnen die personenbezogenen Daten offengelegt und bei dem Empfänger gespeichert wurden und damit nicht dem Zugriff des Verantwortlichen unterliegen (*Herbst*, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Art. 19 DS-GVO, Rdnr. 1). Die Offenlegung kann dabei insbesondere durch Übermittlung, Verarbeitung oder eine andere Form der Bereitstellung erfolgt sein.

Als Empfänger kommt gemäß der Definition des Empfängers in Art. 4 Nr. 9 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, in Betracht, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Da der „Empfänger“ der Definition in Art. 4 Nr. 9 DS-GVO nach nicht „Dritter“ im Sinne des Art. 4 Nr. 10 DS-GVO sein muss, liegt es zunächst nahe, auch vom Kunden im Zusammenhang mit LEXolution.FLOW beauftragte Auftragsverarbeiter, also insbesondere STP und deren Subunternehmer, wie zum Beispiel den Cloud-Infrastrukturprovider, als Empfänger im Sinne des Art. 19 DS-GVO anzusehen.

Dies erschiene angesichts des beschriebenen Zwecks der Mitteilungspflicht nach Art. 19 DS-GVO und der Tatsache, dass der Verantwortliche im Falle einer internen Weitergabe von Daten selbst zur Erfüllung der Pflichten nach Art. 16, 17 und 18 DS-GVO verpflichtet bleibt und die Auftragsverarbeiter insofern verpflichtet sind, den Weisungen des Kunden Folge zu leisten, jedoch als überflüssig.

Als „Empfänger“ gelten nach der Literatur mithin auch keine Personen, die unter Weisung des Verantwortlichen mit personenbezogenen Daten arbeiten (*Gola* in: *Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 4 DS-GVO Rn. 80*). Demgemäß ist es für eine datenschutzkonforme Nutzung von LEXolution.FLOW durch den Kunden nicht erforderlich, dass STP oder die Subunternehmer von STP von einer vom Kunden in LEXolution.FLOW initiierten Berichtigung, Löschung oder Einschränkung der Verarbeitung von personenbezogenen Daten informiert werden.

Ob und in welchem Umfang der Kunde die Exportfunktion von LEXolution.FLOW nutzt, um dort verarbeitete Fall-, Nutzungs- oder Stammdaten an außerhalb des Betriebsmodells von LEXolution.FLOW stehende Dritte weiterzugeben, obliegt dem alleinigen Ermessen des Kunden. Für die Erfüllung der in diesem Fall gegebenenfalls eintretenden Mitteilungspflicht gemäß Art. 19 DS-GVO kann er den Empfänger dieser Daten außerhalb von LEXolution.FLOW, zum Beispiel per E-Mail oder telefonisch, kontaktieren.

#### **4.2.2.7 Erfüllbarkeit des Rechts auf Datenübertragung (Art. 20 DS-GVO)**

Die Nutzer von LEXolution.FLOW haben das Recht, von dem Kunden die Herausgabe der sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu verlangen, soweit es sich hierbei um den Nutzer betreffende Informationen handelt, die der Nutzer selbst in LEXolution.FLOW hochgeladen hat, und sofern die Verarbeitung dieser Informationen

- auf einer Einwilligung des Nutzers (Art. 6 Abs. 1 Satz 1. lit. a) DS-GVO) oder
- auf dem Vertragserfüllungstatbestand (Art. 6 Abs. 1 Satz 1. lit. a) DS-GVO)

beruht (Recht auf Datenübertragung, Art. 20 Abs. 1 DS-GVO). Da LEXolution.FLOW in der Regel im Zusammenhang mit einer Mandatsbeziehung zwischen dem Kunden und dem Nutzer eingesetzt wird, wird der Kunde voraussichtlich die hiermit zusammenhängenden Verarbeitung von personenbezogenen Daten in LEXolution.FLOW auf den Vertragserfüllungstatbestand stützen. In diesen Fällen können die Nutzer von ihrem Recht auf Datenübertragung nach Art. 20 Abs. 1

DS-GVO Gebrauch machen. Einem solchen Verlangen kann der Kunde mithilfe der im Back-End von LEXolution.FLOW bereitgestellten Exportfunktion nachkommen. Das für den Export von Daten aus Lexolution.FLOW zur Verfügung stehende CSV-Format ist zur Erfüllung des Rechts auf Datenübertragung geeignet.<sup>27</sup>.

#### **4.2.2.8 Einschränkung der Verarbeitung nach einem Widerspruch gegen die Verwendung der Stammdaten für die Zwecke der Direktwerbung (Art. 21 Abs.3 und 3 DS-GVO)**

Gemäß Art. 21 Abs. 2 DS-GVO hat der Nutzer das Recht, jederzeit Widerspruch gegen die Verarbeitung der ihn betreffenden personenbezogenen Daten zum Zwecke der Direktwerbung gegenüber dem Kunden zu erheben. In diesem Fall dürfte der Kunde die Benachrichtigungsfunktion von LEXolution.FLOW nicht mehr dazu nutzen, um dem betreffenden Nutzer Werbung zu übersenden (Art. 21 Abs. 3 DS-GVO). Zudem hat der Nutzer regelmäßig auch wettbewerbsrechtlich die Möglichkeit, dem Kunden die Zusendung von werblichen Nachrichten zu untersagen (vgl. § 7 UWG).

Vor diesem Hintergrund sollte in die Benachrichtigungsfunktion von LEXolution.FLOW eine Funktion implementiert werden, die es dem Kunden ermöglicht, für Nutzer selektiv einen Werbewiderspruch zu vermerken, um diese von der Versendung bestimmter Nachrichten ausnehmen zu können.

#### **4.2.2.9 Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten**

Nach Art. 5 Abs. 1 DS-GVO hat die Verarbeitung personenbezogener Daten den darin genannten allgemeinen Grundsätzen der Datenverarbeitung zu genügen. Danach müssen personenbezogene Daten

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

---

<sup>27</sup> Vgl. Artikel-29 Gruppe, *Leitlinien zum Recht auf Datenübertragbarkeit*, Seite 21, abrufbar unter: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611233](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233). Mit dem Wirksamwerden der DS-GVO ist die Artikel-29-Datenschutzgruppe aufgelöst worden. An ihre Stelle ist der Europäische Datenschutzausschuss getreten, ein neues gemeinsames Gremium der europäischen Aufsichtsbehörden. Veröffentlichungen der Aufsichtsbehörden haben zwar keine rechtlich bindende Wirkung, allerdings geben sie die Auffassung der Aufsichtsbehörden wieder und sind demgemäß von wichtiger Bedeutung für die praktische Auslegung und Anwendung der DS-GVO.

- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden [...] („Zweckbindung“);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist [...] („Speicherbegrenzung“);
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)

Der Verantwortliche ist nach Art. 5 Abs. 2 DS-GVO für die Einhaltung dieser Grundsätze verantwortlich und muss deren Einhaltung nachweisen können („Rechenschaftspflicht“).

**a) Rechtmäßigkeit der Verarbeitung**

**aa) Nutzung von LEXolution.FLOW durch den Kunden**

Nach dem in Art. 6 und 9 DS-GVO weiter detaillierten Grundsatz der Rechtmäßigkeit ist eine Verarbeitung personenbezogener Daten nur zulässig, wenn einer der in Art. 6 Abs. 1 DS-GVO genannten gesetzlichen Erlaubnistatbestände eingreift oder die betroffene Person eine Einwilligung zu der Verarbeitung personenbezogener Daten erteilt hat (bzw. im Falle besonderer Arten personenbezogener Daten einer der in Art. 9 Abs. 2 genannten gesetzlichen Erlaubnistatbestände oder eine Einwilligung des Betroffenen vorliegt). Erforderlich ist also nicht ein Erlaubnistatbestand für den Einsatz eines bestimmten (technischen) Mittels – wie zum Beispiel LEXolution.FLOW –, sondern eine Erlaubnistatbestand für die mithilfe von Lexolution.FLOW konkret ausgeführten Datenverarbeitungen.

Da es sich bei LEXolution.FLOW um eine Workflow-Engine handelt, mit der ganz unterschiedliche Prüf-, Beratungs- und Entscheidungsprozesse in Rechtsanwaltskanzleien modelliert werden können, wird der Zweck, der Inhalt und der Umfang der Datenverarbeitung durch den Kunden selbst bestimmt. Demgemäß kann an dieser Stelle nicht allgemein bewertet werden, ob und unter welchen Voraussetzungen Datenverarbeitungen in LEXolution.FLOW gerechtfertigt werden können.

Vorbehaltlich einer Erforderlichkeitsprüfung im Einzelfall dürfte sich jedoch die wohl hauptsächlich erfolgende Verarbeitung von Fall- und Nutzerdaten in LEXolution.FLOW für die Bearbeitung eines Mandats regelmäßig gegenüber dem betreffenden Mandanten auf der Grundlage des Vertragserfüllungstatbestandes in Art. 6 Abs. 1 lit. b) DS-GVO und gegenüber sonstigen Personen auf der Grundlage des Interessenabwägungstatbestandes in Art. 6 Abs. 1 lit. f) DS-GVO legitimieren lassen.

#### **bb) Einsatz von Cookies und Analyse des Nutzerverhaltens**

Trotz der jüngsten Rechtsprechung des Bundesgerichtshofes zur Notwendigkeit einer Einwilligung für das Setzen von Cookies, die der Analyse des Nutzerverhaltens dienen,<sup>28</sup> ergibt sich aus Art. 5 Abs. 3 der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (E-Privacy-Richtlinie), dass zumindest die Verwendung von Cookies, die aus technischen Gründen für den Betrieb von LEXolution.FLOW erforderlich sind, weiterhin auch ohne ausdrückliche Einwilligung des Nutzers zulässig ist. Soweit hiermit eine Verarbeitung personenbezogener Daten verbunden ist, kann diese grundsätzlich auf der Grundlage des Interessenabwägungstatbestandes in Art. 6 Abs. 1 lit. f) DS-GVO gerechtfertigt werden. Demgemäß bedarf der Einsatz der unter Ziff. 1.1.3 beschriebenen Cookies nicht per se der Einholung einer Einwilligung der Nutzer mittels eines Cookie-Banners o. Ä.

Gleichwohl ist die Einholung einer Einwilligung der Nutzer mittels eines Cookie-Banners für alle Cookies als sicherster Weg zu empfehlen und obligatorisch, soweit nicht ausschließlich funktionsnotwendige Cookies im Rahmen von LEXolution.FLOW gesetzt werden. Bei der Implementierung des Cookie-Banners sollten die von der *Datenschutzkonferenz*, einem gemeinsamen Gremium der deutschen Datenschutz-Aufsichtsbehörden, herausgegebenen Hinweise zur Einholung einer Einwilligung mittels eines Cookie-Banners (Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, Seite 9, abrufbar unter: [https://www.datenschutzkonferenz-online.de/media/oh/20190405\\_oh\\_tmg.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf)) berücksichtigt werden.

---

<sup>28</sup>BGH (I. Zivilsenat), Urteil vom 28.05.2020 – I ZR 7/16 - Cookie-Einwilligung II.

Im Hinblick auf die Nutzungsdaten hängt die Frage der datenschutzrechtlichen Zulässigkeit der Auswertung dieser Daten von den Zwecken und dem Umfang der Analyse dieser Daten im Einzelfall ab, so dass an dieser Stelle nicht allgemein beantwortet werden kann, ob die Verarbeitung der Nutzungsdaten rechtmäßig und/oder nur auf der Grundlage einer Einwilligung der betroffenen Nutzer zulässig wäre. Gleichwohl erkennen auch die Datenschutz-Aufsichtsbehörden an, dass es berechnigte Interessen geben kann, die eine Verarbeitung von Nutzungsdaten auch ohne Einwilligung rechtfertigen können (Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Stand: März 2019, Seite 11 ff., abrufbar unter: [https://www.datenschutzkonferenz-online.de/media/oh/20190405\\_oh\\_tmg.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf)), sodass auch die Verarbeitung von Nutzungsdaten in LEXolution.FLOW datenschutzrechtskonform durch den Kunden erfolgen kann.

#### **cc) Zugriffsprotokollierung durch STP zur Gewährleistung der IT-Sicherheit**

Für die in Ziff. 1.1.3 beschriebene Protokollierung unterschiedlicher Informationen zu den auf LEXolution.FLOW erfolgten Zugriffen in temporären Log-Daten ist STP und nicht der Kunde datenschutzrechtlich verantwortlich. Gleichwohl ist die in Ziff. 1.1.3 beschriebene Protokollierung grundsätzlich auf der Grundlage des Interessenabwägungstatbestandes in Art. 6 Abs. 1 lit. f) DS-GVO legitimierbar, soweit die in diesem Zusammenhang verarbeiteten personenbezogenen Daten ausschließlich für die Zwecke der Abwehr sowie der Aufklärung von Angriffen auf die Informationssicherheit von LEXolution.FLOW verwendet werden. Der Verordnungsgeber führt hierzu in Erwägungsgrund 49 zur DS-GVO Folgendes aus:

*„Die Verarbeitung von personenbezogenen Daten durch [...] Betreiber von elektronischen Kommunikationsnetzen und -diensten [...] stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service“-*



*Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.“*

**b) Verarbeitung nach Treu und Glauben**

Das in Art. 5 Abs. 1 lit. a) Var. 2 DS-GVO beschriebene Erfordernis der Verarbeitung nach Treu und Glauben entzieht sich einer scharfen Präzisierung (*Herbst*, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Art. 5 DS-GVO, Rdnr. 13) und lässt sich nur sehr schwer positiv umschreiben. Teilweise wird angenommen, dass dieser Grundsatz die Verwendung verborgener Techniken (z. B. heimliche Videoüberwachung) untersagen wolle. Auch ein Verstoß gegen den Zweckbindungsgrundsatz soll meist als treuwidrig anzusehen und daher durch den Grundsatz untersagt sein (*Pötters*, in: Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 5 DS-GVO Rdnr. 8). Nach anderer Auffassung soll der Grundsatz wegen der begrifflichen Offenheit als ein Auffangtatbestand verstanden werden, der vor allem solche Situationen erfassen solle, in denen die betroffene Person durch die Verarbeitung ihrer personenbezogenen Daten einen Nachteil erfährt, der dem durch die DS-GVO etablierten Gesamtbild des Kräftegleichgewichts zwischen der betroffenen Person und dem Verantwortlichen widerspricht, ohne zwingend gegen ein konkretes gesetzliches Verbot zu verstoßen (*Herbst*, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Art. 5, Rdnr. 18).

Anhaltspunkte dafür, dass eine Verarbeitung personenbezogener Daten in LEXolution.FLOW dem Grundsatz der Datenverarbeitung nach Treu und Glauben widerspräche beziehungsweise LEXolution.FLOW nicht in Übereinstimmung mit dem Grundsatz von Treu und Glauben eingesetzt werden könnte, bestehen nicht. Für die Einhaltung dieses Grundsatzes kommt es vielmehr maßgeblich auf die konkrete Art des Einsatzes von LEXolution.FLOW durch den Kunden, insbesondere die Gestaltung seines Mandantenportals, an.

**c) Grundsatz der Transparenz**

Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten leicht zugänglich, verständlich sowie in klarer und einfacher Sprache abgefasst sind (*Pötters*, in: Gola, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 5 DS-GVO, Rdnr. 10 unter Verweis auf Erwägungsgrund 39). Dem Grundsatz der Transparenz wird daher durch die Bereitstellung einer hinreichend detaillierten und verständlichen Datenschutzerklärung Genüge getan werden müssen (siehe hierzu bereits unter Ziff. 4.2.2.1).

**d) Grundsatz der Zweckbindung**

Nach dem Grundsatz der Zweckbindung müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Da es sich bei LEXolution.FLOW um eine Workflow-Engine handelt, mit der ganz unterschiedliche Prüf-, Beratungs- und Entscheidungsprozesse in Rechtsanwaltskanzleien modelliert werden können, kann der Zweck des Einsatzes von LEXolution.FLOW durch den einzelnen Kunden nur von diesem festgelegt werden. Durch die Möglichkeit, Freigabeerfordernisse in seine mithilfe von LEXolution.FLOW modellierten Workflows zu integrieren, wird der Kunde jedoch bei der Einhaltung des Zweckbindungsgrundsatzes unterstützt. Im Übrigen kann er durch organisatorische Maßnahmen außerhalb von LEXolution.FLOW, zum Beispiel in verbindlichen Prozessbeschreibungen, Richtlinien oder Arbeitsanweisungen für seine Mitarbeiter, sicherstellen, dass die in LEXolution.FLOW verarbeiteten personenbezogenen Daten nur in Konformität mit dem Zweckbindungsgrundsatz verarbeitet werden.

Für die zweckentsprechende Verarbeitung der Protokolldaten ist nicht der Kunde, sondern STP verantwortlich.

**e) Grundsatz der Datenminimierung**

Der Grundsatz der Datenminimierung erfordert es, dass personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind. Die Einhaltung des Grundsatzes der Datenminimierung hat der Kunde unmittelbar in der Hand, so bestimmt er durch die Modellierung der Workflows in seinem Kundenbereich, welche personenbezogenen Daten im Rahmen der im Mandantenportal angebotenen Services vom Nutzer oder aus anderen Quellen erhoben werden.

**f) Grundsatz der Richtigkeit**

Der Grundsatz der Richtigkeit nach Art. 5 Abs. 1 lit. d) DS-GVO fordert, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; es sind dabei alle angemessenen Maßnahmen zu treffen, dass personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Die Einhaltung dieses Grundsatzes ist durch die Umsetzung der bereits im Zusammenhang mit dem Recht auf Berichtigung und auf Löschung erörterten Modalitäten (siehe hierzu Ziff. 4.2.2.3 und 4.2.2.4) gewährleistet.

**g) Grundsatz der Speicherbegrenzung**

Nach dem Grundsatz der Speicherbegrenzung müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Die Einhaltung des Grundsatzes der Speicherbegrenzung ist durch die Umsetzung der bereits im Zusammenhang mit dem Recht auf Löschung erörterten Modalitäten (siehe hierzu Ziff. 4.2.2.4) gewährleistet.

#### **h) Grundsatz der Integrität und Vertraulichkeit**

Der Grundsatz der Vertraulichkeit wird in LEXolution.FLOW einerseits durch die Möglichkeit zur Erstellung von Benutzerkonten und Gruppen mit dedizierten Rechten und andererseits durch Maßnahmen der Transportverschlüsselung und die Verschlüsselung ruhender Daten grundlegend gewährleistet.

Ob die in LEXolution.FLOW implementierten Maßnahmen zur Verschlüsselung dem nach Art. 32 DS-GVO erforderlichen Niveau entsprechen, also ein dem Risiko angemessenes Schutzniveau gewährleisten, ist eine technische Frage, die nicht Gegenstand dieses Memorandums ist.

#### **i) Rechenschaftspflicht**

Der Grundsatz der Rechenschaftspflicht in Art. 5 Abs. 2 DS-GVO schreibt einmal die Verantwortlichkeit für die Einhaltung der in Art. 5 Abs. 1 DS-GVO normierten Grundsätze dem Verantwortlichen zu und verpflichtet diesen zudem, die Einhaltung dieser Grundsätze nachweisen zu können.

Diese Nachweispflicht ist von besonderer Bedeutung im Zusammenhang mit Überprüfungen durch die Aufsichtsbehörden, die nach Artikel 58 Abs. 1 lit. a) DS-GVO auch die Befugnis haben, den Verantwortlichen zur Bereitstellung von Informationen anzuweisen.

Der Grundsatz der Rechenschaftspflicht schreibt dabei nicht vor, in welcher Form dieser Nachweis der Einhaltung der Grundsätze in Art. 5 Abs. 1 DS-GVO zu erfolgen hat. Die Form des Nachweises wird jedoch in einzelnen Bestimmungen der DS-GVO konkretisiert. Ein zentraler Baustein zur Erfüllung der Rechenschaftspflicht ist das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DS-GVO (*Herbst*, in: Kühling/Buchner, DS-GVO BDSG, 2. Auflage 2018, Art. 5 DS-GVO Rdnr. 89), das typischerweise in einer dafür vorgesehene dedizierten Applikation geführt wird. In diesem Verzeichnisses kann der Kunde zur Erfüllung seiner Rechenschaftspflicht sein auf LEXolution.FLOW basierendes Mandantenportal und die hiermit einhergehende Verarbeitung personenbezogener Daten zur Erfüllung der Rechenschaftspflicht dokumentieren.

Ferner erhält der Kunde mit der für LEXolution.FLOW obligatorisch mit STP abzuschließenden Auftragsverarbeitungsvereinbarung einen Nachweis für die ordnungsgemäße Beauftragung von STP als Auftragsverarbeiter nach Maßgabe des Art. 28 DS-GVO. Aus dieser Auftragsverarbeitungsvereinbarung ergibt sich zudem ein Informations- und Auditrecht des Kunden gegenüber STP nach Maßgabe des Art. 28 Abs. 3 Satz 2 lit. h) DS-GVO, sodass der Kunde hinreichende Möglichkeiten hat, auch zum datenschutzkonformen Betrieb von LEXolution.FLOW Rechenschaft, insbesondere gegenüber den Aufsichtsbehörden, abzulegen.

#### **4.2.2.10 Einhaltung der Grundsätze für die Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen**

Nach den vorliegenden Informationen findet die Datenverarbeitung innerhalb LEXolution.FLOW sowie bei Versand der E-Mails unter Nutzung von LEXolution.FLOW über den angebondenen Dienstleister Mailjet ausschließlich innerhalb Deutschlands statt. Besondere datenschutzrechtliche Anforderungen an die Übermittlung personenbezogener Daten in Drittländer oder berufsrechtliche Anforderungen an die Inanspruchnahme von Dienstleistern aus dem Ausland sind daher vorliegend nicht relevant.

#### **4.2.3 Sonstige zu prüfende Rechtspflichten**

##### **4.2.3.1 Impressumspflicht und weitere Informationspflichten**

###### **a) Impressumspflicht gemäß §5 TMG**

Als elektronischer Informations- und Kommunikationsdienst ist LEXolution.FLOW als Telemedium einzuordnen und fällt damit in den Anwendungsbereich des Telemediengesetzes (§ 1 Abs. 1 Satz 1 TMG).

Gemäß § 5 Absatz 1 TMG ist der Diensteanbieter eines in der Regel gegen Entgelt angebotenen Telemediums dazu verpflichtet, die im Katalog des § 5 Abs. 1 TMG spezifizierten Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar in seinem Telemedium zu halten. Da bereits im Fall einer auch nur entfernten wirtschaftlichen Förderung eines Unternehmens mittels des Telemediums die Entgeltlichkeit zu bejahen ist (vgl. *Ott*, in: BeckOK InfoMedienR, 27. Edition, Stand: 1.2.2020, § 5 TMG Rdn. 11), unterliegt LEXolution.FLOW der Impressumspflicht gemäß Art. 5 Abs. 1 TMG.

In persönlicher Hinsicht ist jeder Diensteanbieter verpflichtet, das Impressum für das von ihm betriebene Telemedium vorzuhalten. Folglich ist zunächst der Kunde verpflichtet, für seinen Kundenbereich ein Impressum vorzuhalten, das inhaltlich den Anforderungen gemäß § 5 Abs. 1 TMG genügt. Hierfür steht ihm in LEXoluti-

on.FLOW die Möglichkeit zur Verfügung, in der Menüleiste des Mandantenportals ein Impressum als Freitext dauerhaft zu verlinken. Vorausgesetzt, dass diese Verlinkung in jeder Ansicht seines Mandantenportals verfügbar ist, kann er hiermit ein den gesetzlichen Anforderungen genügendes Impressum für sein Mandantenportal bereitstellen.

Ob darüberhinausgehend auch STP verpflichtet ist, ein Impressum vorzuhalten, hängt davon ab, ob sich STP nach dem Bild eines klassischen Hosting-Providers auf das schlichte Zur-Verfügung-Stellen des Service als White-Label-Lösung beschränkt oder ob STP, beispielsweise durch die Gestaltung des Back-Ends, mit einem eigenständigen Angebot gegenüber den Nutzern auftritt. Im letzteren Fall unterläge STP insoweit der Impressumspflicht gemäß § 5 Abs. 1 TMG (vgl. *Spindler*, in: *Spindler/Schmitz*, *Telemediengesetz*, 2. Auflage 2018, § 5 TMG Rn. 13).

**b) Informationspflichten nach der Verordnung über Online-Streitbeilegung in Verbraucherangelegenheiten und nach dem Verbraucherstreitbeilegungsgesetz**

Gemäß Art. 14 Abs. 1 der Verordnung (EU) Nr. 524/2013 über Online-Streitbeilegung in Verbraucherangelegenheiten (ODR-Verordnung)

*„[stellen] in der Union niedergelassene Unternehmer, die [...] Online-Dienstleistungsverträge eingehen, [...] auf ihren Websites einen Link zur OS-Plattform ein. Dieser Link muss für Verbraucher leicht zugänglich sein. In der Union niedergelassene Unternehmer, die [...] Online-Dienstleistungsverträge eingehen, geben zudem ihre E-Mail-Adressen an.“*

Ferner hat gemäß § 36 Verbraucherstreitbeilegungsgesetz (VSBG) jeder Unternehmer

*„der eine Webseite unterhält oder Allgemeine Geschäftsbedingungen verwendet, [hat] den Verbraucher leicht zugänglich, klar und verständlich*

*1. in Kenntnis zu setzen davon, inwieweit er bereit ist oder verpflichtet ist, an Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle teilzunehmen, und*

*2. auf die zuständige Verbraucherschlichtungsstelle hinzuweisen, wenn sich der Unternehmer zur Teilnahme an einem Streitbeilegungsverfahren vor einer Verbraucherschlichtungsstelle verpflichtet hat oder wenn er auf Grund von Rechtsvorschriften zur Teilnahme verpflichtet ist [...]“*

Diese Pflichten gelten grundsätzlich auch für Rechtsanwälte, die Verbraucher beraten, sodass solche Kunden verpflichtet sind, diese Informationen in ihrem mittels LEXolution.FLOW betriebenen Mandantenportal vorzuhalten. Die für die Erfüllung dieser Pflichten notwendigen Informationen können in das Impressum aufgenommen werden, das in der Menüleiste des Mandantenportals verlinkt ist.

Zudem sind Rechtsanwälte auch Dienstleistungserbringer im Sinne der Verordnung über Informationspflichten für Dienstleistungserbringer (Dienstleistungs- Informationspflichten-Verordnung - DL-InfoV) und müssen die dort geregelten Informationspflichten erfüllen. Die gemäß § 2 DL-InfoV stets zur Verfügung stehende Informationen können den Dienstleistungsempfängern, also den Nutzern des Mandantenportals, ebenfalls im Rahmen einer Ergänzung des Impressums zugänglich gemacht werden.

#### **4.2.3.2 Pflichten im Elektronischen Geschäftsverkehr und für Fernabsatzverträge**

Bei allen Verträgen, die der Kunde über sein Mandantenprotal mit seinen Mandaten abschließt, handelt es sich um Verträge im elektronischen Geschäftsverkehr. Hierfür gelten sowohl dann, wenn es sich bei dem Mandanten um einen Verbraucher handelt, wie auch dann, wenn es sich um einen Unternehmer handelt, die in § 312i Abs. 1 BGB geregelten Pflichten:

- Nach § 312i Abs. 1 Satz 1 Nr. 1 BGB muss der Kunde angemessene, wirksame und zugängliche Mittel zur Verfügung stellen, mit deren Hilfe der Mandant Eingabefehler vor Abgabe einer Bestellung erkennen und beseitigen kann. Dies bedeutet insbesondere, dass die Bestellung vor Absendung dem Kunden zur Korrektur lesbar und korrigierbar auf dem Bildschirm dargestellt werden muss und erst danach eine Bestellung erfolgen kann.
- Nach § 312i Abs. 1 Satz 1 Nr. 2 BGB gibt es zudem Informationspflichten. Nach Art. 246c Nr. 1 EGBGB muss der Kunde über die einzelnen technischen Schritte informieren, die zu einem Vertragsschluss führen; darüber, ob der Vertragstext nach dem Vertragsschluss vom Kunden gespeichert wird und ob er dem Mandanten zugänglich ist; darüber, wie Eingabefehler erkannt und berichtigt werden können; über die für den Vertragsschluss zur Verfügung stehenden Sprachen und über sämtliche einschlägigen Verhaltenskodizes, denen sich der Kunden unterwirft sowie über die Möglichkeit des elektronischen Zugangs zu diesen Regelwerken. Die erforderlichen Informationen können, wenn dies hinreichend transparent geschieht, grundsätzlich auch in die einschlägigen Nutzungs- oder Beratungsbedingungen integriert werden, wenn diese

im Rahmen der Registrierung für das Mandantenportal bzw. Bestellung eines Services leicht abrufbar sind (vgl. *Schirmbacher*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Auflage 2019. 312i BGB Rn.48 ff.)

- Nach § 312i Abs. 1 Satz 1 Nr. 3 BGB muss der Zugang einer Bestellung zudem unverzüglich auf elektronischem Weg bestätigt werden. Dies kann durch den Versand einer Bestätigungs-E-Mail realisiert werden.
- Schließlich ergibt sich aus § 312i Abs. 1 Satz 1 Nr. 4 BGB die Pflicht des Kunden, seinem Mandanten die Möglichkeit zu verschaffen, die Vertragsbestimmungen des über das Mandantenportal abzuschließenden Vertrages einschließlich der Allgemeinen Geschäftsbedingungen bei Vertragsschluss abzurufen und in wiedergabefähiger Form zu speichern. Dieser Anforderung wäre grundsätzlich Genüge getan, wenn dem Nutzer im Rahmen der Verlinkung auch eine Download-Möglichkeit für die einschlägigen Beratungs- oder Nutzungsbedingungen angeboten wird oder dem Nutzer diese mit der Bestätigungsemail übersandt werden können.

Soweit der Kunde mithilfe des Mandantenportals auch Verträge mit Mandanten abschließt, die Verbraucher sind, ergeben sich zusätzliche Pflichten aus § 312j BGB:

- Zunächst muss der Kunde spätestens bei Beginn des Bestellvorgangs in seinem Mandantenportal klar und deutlich angeben, ob Lieferbeschränkungen bestehen und welche Zahlungsmittel er akzeptiert (§ 312j Abs. 1 BGB).
- Ferner muss der Unternehmer gemäß Art. 246a § 1 Abs. 1 Satz 1 EGBG Informationen zu seinen Leistungen, seinen Preisen, der evtl. (Mindest-) Vertragsdauer und den Kündigungsmöglichkeiten klar und verständlich besonders hervorgehoben zur Verfügung stellen, unmittelbar, bevor der Kunde seine Bestellung abgibt (§ 312j Abs. 2 BGB). Im Prinzip müssen die oben genannten Informationen und nur diese in der unmittelbaren Nähe klar und darstellungstechnisch hervorgehoben dargestellt werden und zwar so, dass der Kunde sofort bestellen kann, ohne dass es weitere Zwischenschritte gibt.
- Eine letzte Anforderung enthält § 312j Abs. 3 BGB („Button-Lösung“): Die Schaltfläche, die der Mandant nutzen muss, um eine verbindliche Bestellung abzugeben, muss ihm deutlich machen, dass er einen kos-

tenpflichtigen Vertrag abschließt. Bei dem üblichen Verfahren, in dem der Kunde bestellt, schlägt das Gesetz die Worte „zahlungspflichtig bestellen“ vor (§ 312j Abs. 3 S. 2 BGB). Zusätze oder andere Formulierungen sind zwar möglich, da das Gesetz auch andere Formulierungen zulässt. Verwendet man sie aber, besteht ein erhöhtes Risiko, dass die Formulierung den Anforderungen des Gesetzes evtl. nicht entspricht.

Zudem ist zu beachten, dass die vorstehenden Pflichten gemäß §§ 312i, 312j BGB keine Entgeltlichkeit des abzuschließenden Vertrages voraussetzen. Dies hat zur Konsequenz, dass bereits bei dem Abschluss eines Vertrages über die Nutzung eines Mandantenportales im Rahmen der Registrierung die vorstehenden Regelungen zu beachten sein können (vgl. *Schirmbacher*, in: Spindler/Schuster, *Recht der elektronischen Medien*, 4. Auflage 2019, 312i BGB Rn.9; *Wendehorst*, in: *Münchener Kommentar zum BGB*, 8. Auflage 2019, § 312i BGB Rn. 34 ff.).

Nach der Rechtsprechung des Bundesgerichtshofes können Anwaltsverträge zudem den Regeln für den Fernabsatz unterfallen (BGH, Urteil vom 23.11.2017 – IX ZR 204/16). Wenn ein Kunde also über sein Mandantenportal Anwaltsverträge mit Verbrauchern abschließt, handelt es sich nach dieser Rechtsprechung grundsätzlich um Fernabsatzverträge (vgl. § 312c BGB). Es sind dann zusätzlich zu den vorstehend dargelegten Pflichten im elektronischen Rechtsverkehr weitere Informationspflichten gemäß § 312d Abs.1 Satz 1 i.V. Art. 246a EGBGB im Zusammenhang mit dem Vertragsschluss zu erfüllen.

\*\*\*