2. Stakeholder

2.1. Relevante Stakeholder

Informationssicherheit und Datenschutz sind kein reiner Selbstzweck oder der Versuch einer Selbstbeschäftigung. Es scheint aber ohne nähere Betrachtung nicht völlig klar, welche Einflüsse oder Interessen Stakeholder im Umfeld der Kanzlei bezüglich dieser Themen nehmen oder verfolgen. Es folgt eine Auflistung, welche die relevanten Stakeholder identifiziert und anhand von zwei Dimensionen einordnet. Als Dimensionen zur Einordnung werden das *Interesse an der Umsetzung (I)* und *Einfluss auf die Notwendigkeit (E)* im Hinblick auf Informationssicherheit und Datenschutz herangezogen und diese mit Punkten auf einer Skala von 0 (geringes/-er Interesse/Einfluss) bis 3 (großes/-er Interesse/Einfluss) bewertet. Anhand dieser Punktevergabe und der Übertragung in einen Quadranten ist die Ableitung von Haltungsvorschlägen gegenüber den Stakeholdern möglich.

2.1.1. Klienten

„Ohne Klienten kein Umsatz, ohne Umsatz keine Kanzlei": Über diese Aussage dürfte noch Einigkeit herrschen. „Ohne Informationssicherheit und Datenschutz keine Kunden" mutet als Behauptung schon etwas gewagter an. Die Praxis zeigt, dass Informationssicherheit und Datenschutz keine Kriterien sind, nach denen Kunden ihre Steuerberatungskanzleien bewusst auswählen. Um zu verdeutlichen, warum sich trotzdem noch keine Entspannung einstellen sollte, folgt ein kurzer Ausflug in das Kano-Modell der Kundenzufriedenheit. Nachdem ein Ausflug nun grundsätzlich etwas Kurzweiliges sein sollte, bleibt dieser wirklich kurz.

Kriterien, nach denen Kunden Produkte oder Dienstleistungen auswählen, lassen sich gemäß dem Kano-Modell in fünf Kategorien einteilen:

- **Basismerkmale** werden vom Kunden als selbstverständlich gesehen und diesem nur bei Nichtvorhandensein bewusst. Ein Fehlen der Basismerkmale wird als überproportional negativ gewertet.
- **Leistungsmerkmale** werden bewusst vom Kunden wahrgenommen, erwartet und je nach Erfüllung positiv oder negativ gewertet.
- **Begeisterungsmerkmale** werden vom Kunden nicht erwartet, aber bei Vorhandensein überproportional positiv gewertet.
- **Unerhebliche Merkmale** haben wenig bis gar keinen Einfluss auf die Wertung des Kunden.
- **Rückweisungsmerkmale** haben keinen positiven Einfluss auf den Kunden, werden bei Vorhandensein allerdings als negativ gewertet.

Der Ausflug ist schon beendet. Es entsteht aber vielleicht schon eine Ahnung, warum sich diese Sichtweise in Bezug auf Informationssicherheit und Datenschutz durchaus anbietet. Es ist schwer vorstellbar, dass ein potentieller Klient einer Steuerberatungskanzlei diese bewusst auswählt, weil er ganz begeistert davon ist, dass diese ihre Systeme und seine Daten ganz besonders sicher und datenschutzkonform betreibt und verarbeitet. Das vorliegende Merkmal des Datenschutzes und der Informationssicherheit fällt somit unter den klassischen Fall eines Ba-

sismerkmals und bedeutet vereinfacht gesagt, dass damit wenig zu gewinnen, aber **überproportional viel zu verlieren** ist!

Bei den zuvor genannten Dimensionen Interesse an der Umsetzung (I) und Einfluss auf die Notwendigkeit (E) setzen wir für Klienten also an: I = 1 und E = 2.

2.1.2. Mitarbeiter des Klienten

Die Mitarbeiter des Klienten haben, ähnlich wie der Klient selber, meist keine bewussten Erwartungen an die Informationssicherheit und den Datenschutz in der Kanzlei. Genau wie der Klient selber ist das erforderliche Maß an Informationssicherheit und Datenschutz eine nicht bewusst formulierte Selbstverständlichkeit, welche die Mitarbeiter von ihrem Arbeitgeber und in weiterer Folge auch von dessen „Dienstleistern" erwarten. Eine Mitsprachemöglichkeit bei der Auswahl eines Steuerberaters ist bei den Mitarbeitern des Klienten nicht zu erwarten. Sie müssen hier auf die Sorgfalt und Urteilsfähigkeit ihres Arbeitgebers vertrauen. Eine Regung ist allerdings, wie beim Klienten selber, im Falle von offensichtlich werdenden Problemen in der Informationssicherheit und dem Datenschutz durchaus zu erwarten.

Wir nehmen für Mitarbeiter des Klienten also an: I = 1 und E = 1.

2.1.3. Mitarbeiter der Kanzlei

Die Mitarbeiter der Kanzlei sind im Hinblick auf den Datenschutz und Informationssicherheit mehrfach beteiligt. Zum einen werden deren personenbezogene Daten durch die Kanzlei als Arbeitgeber verarbeitet, zum anderen sind sie es, die Daten des Klienten verarbeiten. Sie müssen die Informationssicherheit und den Datenschutz in der Kanzlei täglich leben und tragen maßgeblich dazu bei, die zu Papier gebrachten Maßnahmen zum Datenschutz und der Sicherstellung der Informationssicherheit in der Praxis zu leben. Der Faktor des Mitarbeiters ist somit eine nicht zu unterschätzende Einflussgröße für eine wirksame Umsetzung der Informationssicherheit und des Datenschutzes. Unglücklicherweise werden Vorschriften, Abläufe und Maßnahmen (zB Zwei-Faktor-Authentifizierung) von Mitarbeitern immer wieder als hinderlich oder zumindest aufwendig gesehen, weshalb das Interesse an der Umsetzung häufig enden wollend ist.

Für Mitarbeiter der Kanzlei setzen wir an: I = 1 und E = 3.

2.1.4. Interessenvertreter – Kammer der Steuerberater und Wirtschaftsprüfer (KSW)

Die KSW sieht sich selber in einer Doppelfunktion hinsichtlich ihrer Aufgaben.[1] Zum einen als Behörde, welche einerseits bspw Aufgaben wie Prüfungen, Anerkennungen und Evidenzen über deren Mitglieder führt. Andererseits als Interessenvertretung, welche somit auch Einfluss auf die Gesetzgebung ausübt und die entsprechende fachliche Information zur Auslegung und Umsetzung liefert. Sie nimmt daher ganz klar eine unterstützende und fördernde Rolle bezüglich Informationssicherheit und Datenschutz ein.

Wir halten also fest: I = 2 und E = 2.

1 Homepage der KSW: https://www.ksw.or.at/desktopdefault.aspx/tabid-30/ (abgerufen am 2. 9. 2018).

2.1.5. Mitbewerber

Die Einschätzung des Mitbewerbes ist nicht immer ganz einfach. Niemand lässt sich gerne in die Karten blicken, wenn es um so heikle Bereiche wie dem Umgang mit Daten in der Kanzlei oder der Sicherheit der eigenen Informationssysteme geht. Einen guten Ansatz bildet die genaue Sichtung des Webauftrittes. Ein besonderes Augenmerk sollte gerichtet werden auf:

- Inhalt und Umfang der obligatorischen Datenschutzerklärung;
- Vorhandene Zertifizierungen oder Gütesiegel, auf die hingewiesen wird;
- Weiterbildungsmaßnahmen von Mitarbeitern des Mitbewerbes, über die berichtet wird;
- Kooperationspartner oder Dienstleister, auf die der Mitbewerb zurückgreift;
- Beworbene Beratungsleistungen zum Thema Informationssicherheit und Datenschutz.

Falls sich im Rahmen von Weiterbildungen oder Fachveranstaltungen die Gelegenheit bietet, kann auch die Chance genützt werden, Mitarbeiter des Mitbewerbes anzusprechen und sich über die Themen auszutauschen. Spannende Fragen könnten sein:

- Wo ist Informationssicherheit und Datenschutz bei Ihnen organisatorisch angesiedelt?
- Wie schätzen Sie die Wichtigkeit von Maßnahmen zur Gewährleistung einer adäquaten Informationssicherheit ein?
- War die Umsetzung der Datenschutz-Grundverordnung schon ein Thema bei Ihnen?

Im ungezwungenen Rahmen und in Pausen kann so oft mehr in Erfahrung gebracht werden als in einer Stunde mühevoller Internetrecherche.

Allgemein gesehen kann eine Beobachtung des Mitbewerbes sicherlich etwas Orientierung geben. Die Beeinflussung durch die vermutlich sehr eingeschränkte Sicht in die Überlegungen und Maßnahmen, die der Mitbewerb zu diesen Themen anstellt, sollte aber nicht zu schwer wiegen.

Unsere Bewertung ergibt: I = 1 und E = 0.

2.1.6. Gesetzgeber

Eine ausführlichere Auseinandersetzung mit konkreten Gesetzen wird in den folgenden Kapiteln noch erfolgen. An dieser Stelle wird erst einmal ein kurzer Blick auf die Interessen an der Umsetzung und Einfluss auf die Notwendigkeit von Informationssicherheits- und Datenschutzmaßnahmen durch den Gesetzgeber geworfen.

Als Beispiel von enormer Tragweite ist sicherlich die Anwendbarkeit der Datenschutz-Grundverordnung seit Mai 2018 zu sehen. Angesichts der Auswirkungen auf alle Bereiche der Wirtschaft und weit darüber hinaus scheint der Einfluss des Gesetzgebers kaum zu übertreffen. Die Frage nach den Interessen, welche damit verfolgt werden, stellt sich schnell.

Die Datenschutz-Grundverordnung (DSGVO):

Der Gesetzgeber sieht den Schutz personenbezogener Daten als Grundrecht. Die DSGVO beabsichtigt einerseits, diesen Schutz auf einem einheitlichen Niveau in der EU zu gewährleisten, und andererseits, einheitliche Rahmenbedingungen für die einzelnen Ak-

teure wie Staaten, Unternehmen, Vereinigungen und natürlichen Personen zur Verarbeitung dieser Daten sicherzustellen. Sie findet Anwendung auf die Datenverarbeitung durch Verantwortliche in der EU und auf die Verarbeitung von Daten von Personen, die sich in der EU befinden, durch Verantwortliche außerhalb der EU.

Es könnte nun der Einwand erfolgen, dass sich hinter einer Gesetzgebung noch viele weitere Stakeholder wie Interessenvertretungen, Lobbyisten, Politiker, ... verbergen. Diesem Einwand wäre je nach notwendiger Betrachtungstiefe sogar zu folgen. Um einen Überblick zu zeichnen, wird der Gesetzgeber aber als ausreichend umrissener Stakeholder mit schwerwiegenden Interessen und unmittelbarem Einfluss auf die Kanzlei angenommen.

Wir halten also fest: I = 3 und E = 3.

2.1.7. Aufsichtsbehörden

Aufsichtsbehörden nehmen Einfluss indem diese einerseits im Rahmen ihrer Aufgaben eine Aufsichts- und Kontrollfunktion erfüllen und andererseits bestehende Gesetze im Rahmen von Verfahren auslegen und für die Praxis konkretisieren und entscheiden können.

In Österreich trägt die Datenschutzbehörde für die Einhaltung des Datenschutzes Sorge. Dafür verfügt sie über zahlreiche Befugnisse. Diese umfassen bspw den Zugang zu allen personenbezogenen Daten, Geschäftsräumen und Datenverarbeitungsanlagen und natürlich die Verhängung von existenzbedrohenden Bußgeldern. Sie muss dabei nicht von sich aus tätig werden. In der Vergangenheit wurde sie in der Regel durch Beschwerden von Betroffenen, denen die DSB verpflichtet ist nachzugehen, auf einen Sachverhalt aufmerksam. Der Weg einer Beschwerde an die DSB steht fast allen Stakeholdern als Betroffenen offen.

Für die Einhaltung der Informationssicherheit lässt sich in Österreich keine konkrete Behörde bestimmen. Eine Vernachlässigung der Informationssicherheit kann vielfältige Konsequenzen nach sich ziehen. Jede Vernachlässigung kann für sich gegen andere Gesetze, Richtlinien und Normen verstoßen. Gesetzesmaterien zum Informationsschutz im Hinblick auf die Tätigkeiten in der Kanzlei werden in späterer Folge noch behandelt.

Wir setzen für Aufsichtsbehörden folgende Punkte an: I = 3 und E = 3.

2.1.8. Partner und Gesellschafter

Die Verbindlichkeit, Vertraulichkeit und das Berufsgeheimnis sind fundamentale Prinzipien in der Kanzlei. Eigentümer sowie die Personen die mit der Führung der Kanzlei betraut sind müssen Maßnahmen treffen, um diese Prinzipien umzusetzen. Informationssicherheit und Datenschutz stellen wiederum Konzepte dar, die die Einhaltung jener Prinzipien gewährleisten sollen. Die unbedingte Notwendigkeit, diese Konzepte auch in die tägliche Arbeit in der Kanzlei einfließen zu lassen, wird durch die gesetzlichen Regelungen des Datenschutzes und der Informationssicherheit untermauert. Unter ständiger Abwägung des Mitteleinsatzes im Verhältnis zur Wirksamkeit muss ein hohes Interesse bestehen, die Informationssicherheit und den Datenschutz in der Kanzlei zu gewährleisten.

Wir bewerten Partner und Gesellschafter mit: I = 3 und E = 2.

Es wären ohne Zweifel noch weitere Stakeholder wie zB Banken denkbar. Die Aufzählung konzentriert sich aber auf jene mit den größten Einfluss- oder Interessenpotentialen. Es kann interessant sein, eine eigene Liste der bedeutendsten Stakeholder zu erstellen und zu überlegen, welchen Einfluss diese auf Maßnahmen und Überlegungen im Hinblick auf Informationssicherheit und Datenschutz in der betreffenden Kanzlei tatsächlich nehmen.

2.2. Analyse der Stakeholder

Es ist nun an der Zeit, das Geheimnis hinter den gewählten Dimensionen *Interesse an der Umsetzung (I)* und *Einfluss auf die Notwendigkeit (E)* zu lüften. Auf zwei Achsen werden die Stakeholder gemäß ihrer Bewertung eingetragen und je nach Quadrant, in dem sie sich befinden, wird eine der vier Haltungsempfehlungen (beobachten, informiert halten, Zufriedenheit erhalten, sorgfältig managen) für den Umgang mit der betreffenden Gruppe abgeleitet.

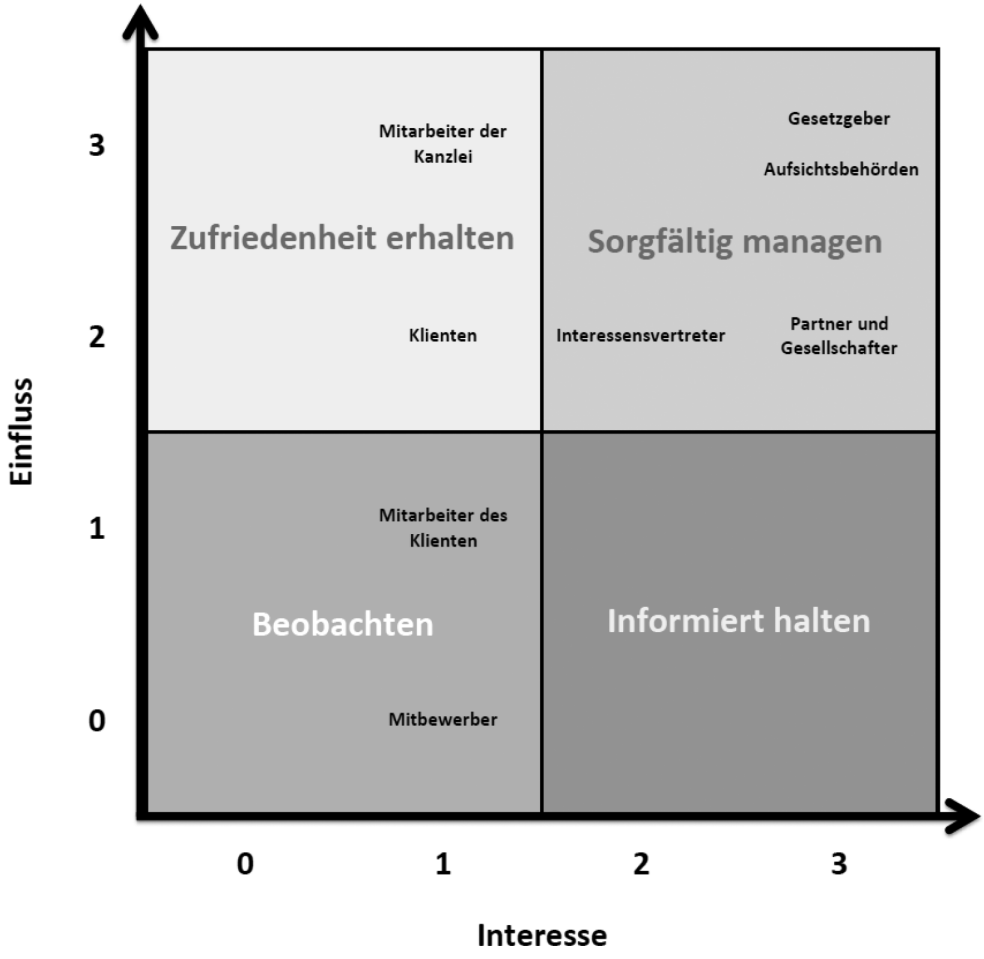

Abbildung 1: Stakeholder Matrix mit ausgefüllten Quadranten und Haltungsempfehlungen

Entsprechend den angesetzten Werten ergibt sich das oben gezeichnete Bild, welches die folgenden Empfehlungen zur Haltung gegenüber den Stakeholdern stützen.

2.2.1. Klienten

Es gilt die Zufriedenheit des Klienten zu erhalten, indem die Einhaltung der Informationssicherheit und des Datenschutzes, welche eine größtenteils unbewusste Selbstverständlichkeit für den Klienten darstellen, gewährleistet wird. Die Verhinderung von Zwischenfällen im Datenschutz und der Informationssicherheit, welche dem Kunden negativ auffallen und auf eine Mangelhaftigkeit der Maßnahmen in der Kanzlei hinweisen würden, muss angestrebt werden.

2.2.2. Mitarbeiter des Klienten

Die Mitarbeiter des Klienten sollten hinsichtlich ihrer Reaktion auf Maßnahmen zur Hebung der Informationssicherheit und des Datenschutzes (zB elektronische Übermittlung von passwortgeschützten Verdienstnachweisen) beobachtet werden und im Falle eines steigenden Interesses vorbeugend mit Informationen versorgt werden („informiert halten").

2.2.3. Mitarbeiter der Kanzlei

Die Zufriedenheit der Mitarbeiter in der Kanzlei sollte durch wirkungsvolle und praxisverträgliche Maßnahmen zur Sicherstellung der Informationssicherheit und des Datenschutzes gehalten werden. Es gilt, Verständnis für notwendige, ggf aufwändigere Abläufe und Vorgehensweisen zu fördern und durch passende Weiterbildungsangebote die Aufmerksamkeit für Informationssicherheit und Datenschutz zu heben.

2.2.4. Interessenvertreter – Kammer der Steuerberater und Wirtschaftsprüfer (KSW)

Sorgfältig zu managen bedeutet hinsichtlich der Interessenvertretung, die Informationen und Aussagen genau zu verfolgen und für die eigene Kanzlei umzusetzen. Eine starke Interessenvertretung bietet unter Beteiligung ihrer Mitglieder außerdem die Möglichkeit, durch ihr Gewicht Änderungen in der Gesetzgebung bzw in deren Auslegung in Gang zu bringen oder verbindliche Normen und Mindeststandards in der Branche zu etablieren.

2.2.5. Mitbewerber

Der Mitbewerb sollte bezüglich seiner Maßnahmen zur Informationssicherheit und zum Datenschutz zumindest beobachtet werden, um aus dessen Fehlern zu lernen oder durch dessen Ideen zu profitieren. Ein möglichst objektives Bild des Mitbewerbers hilft beim Vergleich des eigenen Reifegrades der Maßnahmen zur Informationssicherheit und zum Datenschutz im Kanzleiumfeld.