VISCHER

Digital Business

VISCHER

Digital Business

Inhalt

Vorwort

Dr. Rolf Auf der Maur

Die Digitalisierung hat im Verlauf der letzten 25 Jahre sämtliche Geschäftsbereiche erfasst und teilweise regelrecht auf den Kopf gestellt. Aber erst die allgemeine Verfügbarkeit von Breitbandinternet – heute eine Selbstverständlichkeit auf jedem Smartphone – hat einen Strukturwandel in Gang gesetzt, der inzwischen wohl jede Branche erfasst hat.

Digitalisierung ermöglicht es, Informationen und Daten jeglicher Art zu codieren und in kleinste Pakete zu zerlegen. Die codierten Datenpakete lassen sich über verschiedenste Kommunikationsnetze von jedem beliebigen Standort an jeden anderen Ort auf der Welt transportieren. Datenpakete reisen per Internet-Protokoll (oder IP-Technologie) ähnlich wie ein ISO-Container im Güterverkehr, der nacheinander per Schiff, Bahn und Lastwagen transportiert werden kann, um an sein Ziel zu gelangen. Landesgrenzen spielen für die Kommunikation über Internet keine Rolle – im Gegensatz natürlich zur Regulierung, die sich mit grosser Verzögerung den neuen Realitäten anpasst.

IP-Technologie und die darauf basierenden Informations- und Kommunikationstechnologien und -Dienste durchdringen und verbinden alle Bereiche von Wirtschaft und Gesellschaft. Sie ermöglichen es Unternehmen, ihre Geschäftsprozesse bis hin zum einzelnen Kunden oder Aussendienstmitarbeiter durchgängig zu digitalisieren und Geschäftsprozesse ganz neu zu gestalten.

VISCHER hat sich seit seiner Gründung im Jahre 2000 proaktiv mit der Entwicklung von Informations- und Kommunikationstechnologien befasst. In dieser Zeit durften unsere ICT-Spezialisten zahlreiche Klienten bei der Ausgestaltung neuer Geschäftsmodelle unterstützen. Besonderes Augenmerk richten wir auf stark regulierte Branchen wie Finanzwesen, Energie, Telekommunikation, Medien und Gesundheit. In diesen Branchen sind innovative Ansätze, ein gutes Einvernehmen mit Regulatoren und zuweilen auch die Mitgestaltung der relevanten Standards besonders gefragt. Heute bringen wir unsere digitale Kompetenz in sämtlichen Branchen und Rechtsgebieten zur Anwendung, in denen unsere 25 Spezialistenteams tätig sind.

Mit dieser Publikation geben wir einen kleinen Einblick in die Fülle unserer Erfahrungen und Klientenprojekte rund um digitale Geschäftsprozesse.

Wir wünschen viel Spass und hoffentlich einige neue Erkenntnisse bei der Lektüre.

Zürich, Basel, November 2016

Grundlagen des digitalen Geschäftsverkehrs

1 Die elektronische Unterschrift

Dr. Peter Kühn, LL.M.

Die elektronische Unterschrift entspricht einem stetig wachsenden Bedürfnis in der Praxis. Es geht insbesondere darum, zweiseitige Verträge auf elektronischem Wege gültig abschliessen zu können. Aber auch bei einseitigen Rechtsgeschäften (wie z. B. Kündigungen oder Anträgen bei Behörden und Gerichten) stellt sich immer wieder die Frage nach der Möglichkeit oder der Formgültigkeit elektronisch abgegebener Erklärungen.

Eigenhändige Unterschrift als Regelfall der Schriftlichkeit

Nach dem Grundsatz der Formfreiheit unter Schweizer Recht bedürfen Verträge und Erklärungen grundsätzlich keiner besonderen Form und können daher auch elektronisch (z. B. per E-Mail) erfolgen. Anderes gilt, wenn ein Formerfordernis von den Parteien vereinbart wurde oder gesetzlich angeordnet ist (siehe nur z. B. im Bereich des Arbeitsrechts: Personalverleihverträge, Leiharbeits- und Einsatzverträge, entgeltliche Arbeitsvermittlungsverträge mit Stellensuchenden, Lehrverträge, Handelsreisendenverträge etc.). Häufigstes Formerfordernis in der Praxis ist die Schriftform. Ist Schriftlichkeit einzuhalten, erfordert dies grundsätzlich eigenhändige Unterschriften.

Schriftlicher Vertragsschluss per E-Mail?

Es wäre nach überwiegender Auffassung formunwirksam, einen Vertrag mit Schriftformerfordernis rein per E-Mail abzuschliessen oder eine schriftliche Kündigung nur per E-Mail zu versenden. Allerdings geschieht dies in der Praxis immer wieder. Konsequenz ist die (Form-)Unwirksamkeit, auch wenn dies den Beteiligten mitunter nicht bewusst ist. Komplexe Fragen nach einer möglichen Heilung, nachträglichen Genehmigung, allfälligen Novation oder auch bereicherungsrechtlicher Rückabwicklung können sich dann stellen.

Zulässig dürfte es hingegen sein, wenn die – eigenhändig unterzeichneten – Willensäusserungen in einem eingescannten PDF verkörpert und der E-Mail angehängt sind. Dann ist von einer ausreichenden Perpetuierung und Unveränderbarkeit der Erklärungen auszugehen, was dem Schriftformerfordernis in der Regel genügt (wenngleich insbesondere verschiedene Behörden, wie z. B. die FINMA, insoweit teilweise strengere Anforderungen stellen).

Die qualifizierte elektronische Signatur als echte digitale Alternative

Eine Alternative zur eigenhändigen Unterschrift bietet die sogenannte qualifizierte elektronische Signatur. Diese kann erhebliche Vereinfachungen in der Handhabung und Dokumentenverwaltung gerade bei Massenverträgen mit Schriftformerfordernis mit sich bringen.

Es ist im Übrigen nicht zwingend erforderlich, dass die Unterschriften sämtlicher Vertragspartner entweder alle eigenhändig oder alle elektronisch erfolgen. Es wäre daher möglich, dass nur eine Partei elektronisch unterzeichnet und der oder die anderen Vertragspartner eigenhändig.

Rechtsgrundlage der elektronischen Unterschrift ist Art. 14 Abs. 2bis des Schweizerischen Obligationenrechts (OR): Danach ist die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichgestellt, wenn sie auf einem qualifizierten Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes über die elektronische Signatur (ZertES und der entsprechenden Ausführungsverordnung VZertES) beruht.

Wichtig zu wissen ist, dass nur Zertifikate von in der Schweiz akkreditierten Anbietern für die elektronische Unterschrift zulässig sind. Die Schweizerische

Akkreditierungsstelle (SAS) veröffentlicht die Liste der anerkannten Anbieterinnen von Zertifizierungsdiensten. Derzeit sind lediglich vier Stellen erfasst:

- Swisscom (Schweiz) AG,
- QuoVadis Trustlink Schweiz AG,
- SwissSign AG und
- das Bundesamt für Informatik und Telekommunikation.

Die Zertifikate einer Vielzahl renommierter ausländischer Anbieter (z. B. Adobe Sign [vorher EchoSign], DocuSign etc.) können somit derzeit in der Schweiz nicht rechtsgültig verwendet werden.

Im Besonderen: Die SuisseID

Der für Privatpersonen und Unternehmen momentan wichtigste digitale Schweizer Standard für qualifizierte elektronische Signaturen (aber auch für die Online-Authentifizierung) ist die SuisseID. Anbieter sind QuoVadis einerseits und SwissSign/Schweizerische Post andererseits.

Welches konkrete Angebot den eigenen Bedürfnissen am ehesten entspricht, muss jede Person bzw. jedes Unternehmen für sich selbst entscheiden. Möglich sind sowohl reine Online- als auch Hardware-basierte Lösungen mit Smartcard, USB-Stick oder Token.

Ein weiterer Vorteil der SuisseID ist die sowohl technische als auch organisatorische EU-Kompatibilität. Die SuisseID basiert auf den europäischen Telekommunikationsstandards ETSI und verwendet ebenfalls die sogenannte Security-Assertion-Markup-Language (SAML). Sie stellt daher keine proprietäre Schweizer Lösung dar und kann grundsätzlich auch in internationalen Unternehmen implementiert werden.

Einschätzung und Ausblick

Nach unserer Einschätzung sind gemäss ZertES gültige elektronische Signaturen in der Schweiz weitestgehend akzeptiert. Der effektive Einsatzbereich in der Praxis ist allerdings nach wie vor beschränkt. Die grosse Mehrzahl der Verträge wird auf herkömmlichem Weg (eigenhändig) unterzeichnet. Über den Bereich der Verträge hinaus findet man elektronische Unterschriften oft in den Berichten der Revisionsstelle und in Dokumenten, die zur Verbreitung an einen grösseren Personenkreis bestimmt sind (z. B. Geschäftsberichte, Einladungen zu Generalversammlungen etc.), noch vergleichsweise selten hingegen in E-Mails. Weitere stark ausbaufähige Einsatzgebiete der elektronischen Signatur bestehen im elektronischen Rechtsverkehr (ERV) mit Behörden und Gerichten. Beispielsweise hat die FINMA am 16. September 2016 ihre digitale Zustellplattform lanciert: Wer dem Schriftlichkeitserfordernis unterliegende Dokumente darüber einreichen möchte, muss eine qualifizierte elektronische Signatur benutzen.

Wir gehen davon aus, dass die Digitalisierung unaufhaltsam fortschreitet und damit auch die qualifizierte elektronische Signatur bzw. SuisseID in der Schweiz künftig immer weitere Verbreitung erfahren wird. Dies auch angesichts der wachsenden Funktionalität (z. B. Video- und Online-Authentifizierung bei Bankkundenbeziehungen und Vermögensverwaltungsverträgen). Sofern nicht bereits geschehen, dürfte es sich daher zumindest lohnen, einen Blick auf die Möglichkeiten und Einsatzgebiete elektronischer Unterschriften zu werfen.

Allerdings ist die technische wie rechtliche Entwicklung derzeit stark im Fluss: Am 1. Juli 2016 ist die neue EU-Signaturverordnung (eIDAS) in Kraft getreten. Die eIDAS-Verordnung schafft einheitliche Rahmenbedingungen für die grenzüberschreitende Nutzung elektronischer Identifizierungsmittel und Vertrauensdienste.

Bereits haben sich verschiedene Branchengrössen wie Adobe, Bundesdruckerei/D-Trust und Intarsys Consulting aus Deutschland, SwissSign und viele andere mehr zum sogenannten Cloud Signature Consortium (CSC) zusammengeschlossen, um bis Ende 2016 einen offenen Standard für cloudbasierte digitale Signaturen und Siegel für Mobilgeräte und Online-Anwendungen zu entwickeln.

2 Online-Shop als erster Schritt ins E-Commerce

Elias Mühlemann

Rehana Harasgama

Wer die Möglichkeiten des digitalen Zeitalters wirtschaftlich nutzen will, fasst meist als Erstes die Errichtung eines Online-Shops ins Auge. Die potenzielle Kundenbasis kann dadurch ohne grösseren Aufwand vervielfacht werden. Was ist aber zu beachten, damit der betriebseigene Online-Shop nicht zur digitalen Falle wird?

Dieser Artikel zeigt auf, wie mit der Befolgung weniger Punkte das juristische Risiko von Online-Shops wesentlich reduziert werden kann.

Herausforderungen im Online-Handel

Um dem Online-Shop den richtigen juristischen Rahmen zu geben, ist zunächst die beabsichtigte Kundenbeziehung zu definieren. Dabei stellen sich insbesondere folgende Fragen:

- *Notwendige/gewünschte Informationen über den Kunden:* Welche Informationen sind notwendig, damit das Geschäft erfolgreich abgewickelt werden kann?
- *Geografische Verfügbarkeit des Shops:* Sollen Produkte auch ins Ausland verkauft/geliefert werden?

Die Intensität und Komplexität der beabsichtigten Kundenbeziehung beeinflussen sowohl die technische wie auch die juristische Umsetzung eines Online-Shops.

Einzuhaltende Rechtsnormen

Über den unlauteren Wettbewerb (UWG) hat der Schweizer Gesetzgeber in Art. 3 Abs. 1 lit. s des Bundesgesetzes folgende Mindeststandards definiert, die zwingend einzuhalten sind:

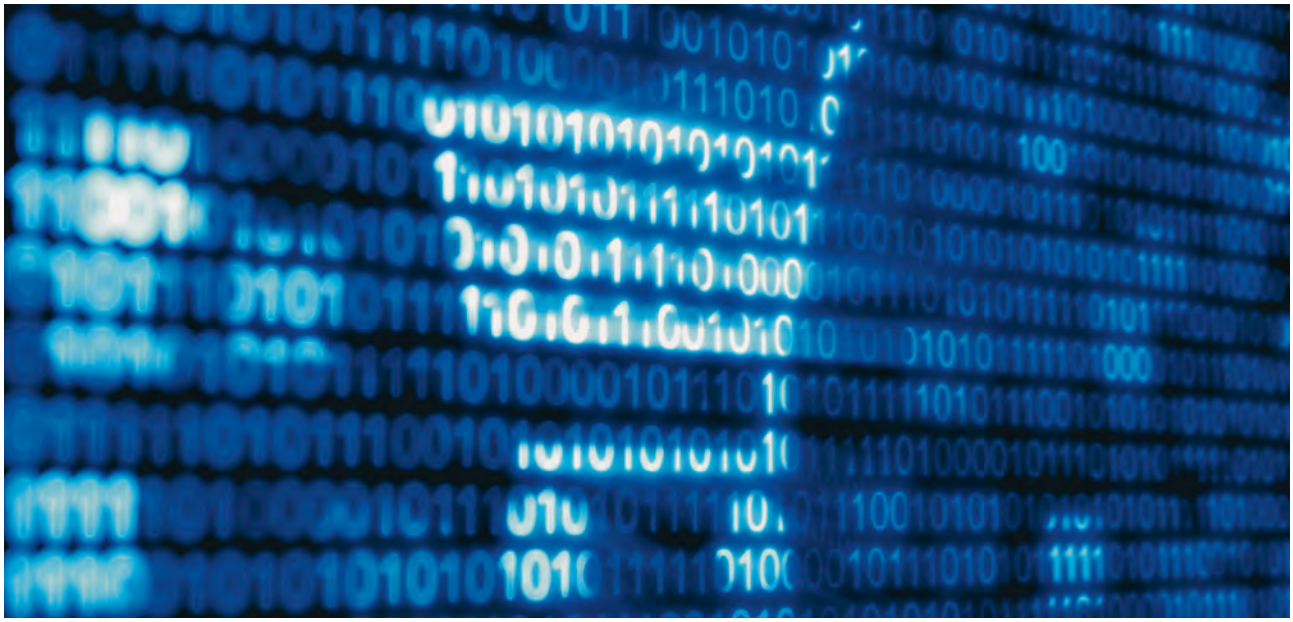
- Vollständige Angabe der Identität und Kontaktadresse des Betreibers
- Hinweis auf die einzelnen technischen Schritte zum Vertragsabschluss
- Angebot von technischen Mitteln, um Falschangaben in der Bestellung zu erkennen und anzupassen
- Bestellungen sind vom Betreiber sofort zu bestätigen

Werden im Rahmen des Kaufprozesses *vom Kunden* (sensible/personenbezogene) Daten verlangt, sind zusätzliche Vorschriften zu beachten. Oft wollen Betreiber von Online-Shops mehr Daten sammeln, als dies tatsächlich für den Kaufprozess notwendig wäre. Dies dient u. a. der Analyse ihrer Kundschaft oder ihrem Online-Marketing. Das Datenschutzgesetz (DSG) setzt diesem Wunsch der Online-Shop-Betreiber Grenzen. So dürfen nur Daten erhoben werden, die dem in der Datenschutzerklärung vorab genannten Zweck der Datenbearbeitung dienen. Entsprechend müssen Kunden z. B. über eine allfällige Weitergabe ihrer Daten an Dritte informiert werden. Mithilfe von technischen und organisatorischen Schutzmassnahmen ist zudem sicherzustellen, dass die erhobenen Daten vor unbefugten Bearbeitungen geschützt sind. Insbesondere dürfen Personendaten nur dann ins Ausland übermittelt werden, wenn dort ein angemessenes Datenschutzniveau gewährleistet werden kann.

Im *grenzüberschreitenden Datenverkehr* ist seit dem 25. Mai 2016 zudem die neue Datenschutz-Grundverordnung (DS-GVO) der EU zu beachten (Umsetzung der Mitgliedsstaaten bis spätestens am 25. Mai 2018). Unternehmen, die u. a. Produkte oder Dienstleistungen grenzüberschreitend – also in der EU – anbieten oder ihre Daten an einen Provider in der EU (z. B. in ein externes Datenzentrum oder eine Cloud) auslagern, haben strengere Anforderungen bezüglich der Einwilligung zur Datenbearbeitung sowie weitergehende Informationspflichten zu beachten:

Nach DS-GVO ist eine stillschweigende Einwilligung zur Datenbearbeitung (z. B. im Rahmen von Allgemeinen Geschäftsbedingungen) nicht ausreichend. Der «Einwilligungsakt» muss unmissverständlich sein und die Einwilligung muss klar von anderen Sachverhalten getrennt erfolgen. So darf bspw. ein Kästchen zur Einwilligung für den Empfang eines Newsletters nicht bereits (vor-)angekreuzt sein.

In Online-Shops sind Kunden vor Vertragsabschluss deutlich auf die anwendbaren AGB hinzuweisen, ansonsten entfalten diese keine Wirkung. AGB dürfen zudem inhaltlich nicht gegen Treu und Glauben verstossen: Klauseln, die ungewöhnlich sind, werden nicht zum Vertragsinhalt, sofern der Kunde nicht besonders auf diese Klauseln (bspw. durch Hervorhebung) aufmerksam gemacht wird.



Die neuen Informationspflichten beinhalten u. a. die genaue Angabe von Name und Kontaktdaten des verantwortlichen Datenbearbeiters sowie in gewissen Fällen auch des Datenschutzbeauftragten. Weiter ist auf der Webseite darauf hinzuweisen, wie lange die Daten aufbewahrt werden und dass ein Auskunftsrecht des Kunden bez. seiner bearbeiteten Daten besteht. Im Widerhandlungsfall droht eine Busse von maximal 20 Mio. EUR oder bis zu 4 % des weltweiten Jahresumsatzes, je nachdem was höher ist.

Handlungsempfehlungen

Juristisches Kernstück jedes Online-Shops sollten die AGB bilden. Aus Sicht des Online-Shop-Betreibers haben diese idealerweise folgenden Inhalt:

- Beschrieb des Kaufprozesses inkl. Zahlungsverkehr
- Gewährleistungs- und Haftungsausschluss bzw. -beschränkung
- Behandlung und Umgang mit Urheberrechten
- Festlegung des anwendbaren Rechts und des Gerichtsstands

Ungewöhnlich sind Klauseln, die einen geschäftsfremden Inhalt aufweisen. Unklare AGB-Bestimmungen werden zulasten des Erstellers ausgelegt. Treuwidrig zum Nachteil von Konsumenten formulierte AGB sind ebenfalls unzulässig.

Sorgfältig formulierte und auf den tatsächlichen Inhalt des Online-Angebots abgestimmte AGB (Vorsicht bei Änderung des Kaufangebots oder des Kaufprozesses!) minimieren die juristischen Risiken für Betreiber von Online-Shops deutlich. Viele juristische Auseinandersetzungen im Zusammenhang mit Online-Shops und -Plattformen könnten durch die sorgfältige Ausformulierung (bzw. Aktualisierung) von AGB verhindert werden.

Weiter ist der Kunde mithilfe einer *Datenschutzerklärung* auf der Webseite zu informieren, zu welchen Zwecken die Daten verwendet und wie sie geschützt werden. Schliesslich ist sicherzustellen, dass die gesammelten Daten tatsächlich im Einklang mit dem Datenschutzgesetz und der eigenen Datenschutzerklärung bearbeitet werden. Beim Anbieten von Waren und Dienstleistungen über die Landesgrenzen hinaus sind allenfalls weitere Massnahmen zu ergreifen, um ausländische Vorschriften, wie z. B. die DS-GVO, einzuhalten.

3 Blockchain: Von der virtuellen Währung zur technischen Revolution?

Manuel Blättler

Dominic A. Wyss

Blockchain ist die Technologie der Stunde – Grundlage unzähliger Start-ups – und zugleich Bedrohung und Heilsbringer für traditionelle Finanzinstitute. Die hinter der digitalen Währung Bitcoin stehende Technologie löst sich langsam aus dem Schatten der krisengeplagten Kryptowährung. Von einem blossen Hype kann nicht mehr gesprochen werden. Die Anwendungsmöglichkeiten von Blockchain scheinen unbegrenzt zu sein. Ebenso vielfältig sind die mit den entsprechenden Anwendungen verbundenen rechtlichen Fragen.

Eines der vielversprechenden Anwendungsgebiete der Blockchain-Technologie ist der sogenannte Smart Contract, der im Folgenden näher behandelt werden soll.

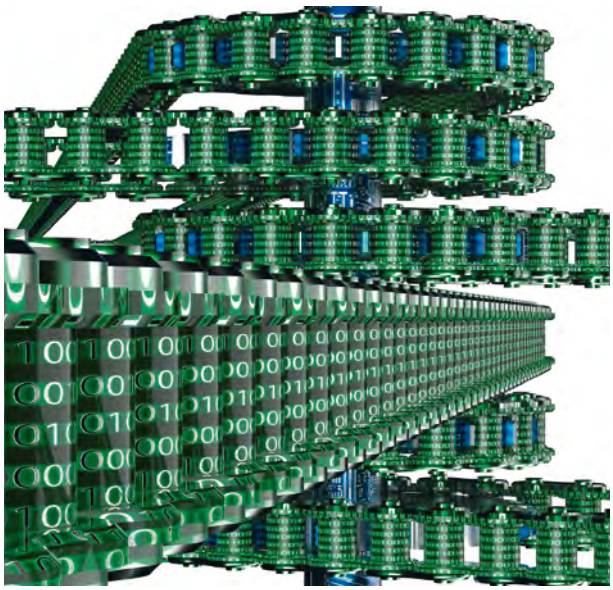
Was ist Blockchain?

Die Blockchain-Technologie lässt sich als ein digitales, dezentralisiertes Register beschreiben, bei dem alle Teilnehmer über eine Kopie aller bisher in einem Blockchain-Netzwerk durchgeführten Transaktionen verfügen. Die wachsende Anzahl von Datensätzen bzw. Datenblöcken wird verschlüsselt, wie eine Kette fortgeführt, auf verschiedenen Rechnern abgelegt und verwaltet. Angaben, die sich nicht in einer Mehrheit der geteilten bzw. dezentralisierten Register widerspiegeln, werden eliminiert. Aufgrund dieser kollektiven Verifizierung der Daten gilt das Blockchain-System als unveränderbar und kaum fälschbar. Auch ermöglicht die dezentrale Registerführung, zentrale Stellen, wie z. B. Banken oder Clearingstellen, auszuschalten. Durch die Technologie könnten Transaktionen vergünstigt und rascher abgewickelt werden.

Wo kann Blockchain eingesetzt werden?

Die wohl bekanntesten Anwendungen der Blockchain-Technologie sind Kryptowährungen, d. h. virtuelle Währungen, basierend auf den Prinzipien der Kryptografie. Hier steht insbesondere der Bitcoin im Scheinwerferlicht, in jüngster Vergangenheit jedoch zunehmend mit negativen Schlagzeilen.

Was momentan (noch) nicht im Vordergrund steht, sind andere Anwendungsmöglichkeiten der Blockchain-Technologie. Diese sind praktisch unbegrenzt und führen zur digitalen Goldgräberstimmung. Blockchain könnte in all denjenigen Bereichen verwendet werden, die heute auf zentralen Registern beruhen. Zu denken ist dabei z. B. an Register für Immaterialgüterrechte, das Grundbuch, Waffenregister, Register für Kunstwerke etc. Darüber hinaus ist die Technologie auch in anderen Bereichen anwendbar, die heute weitgehend auf Vertrauen basieren. Dies gilt vor allem im Bereich von Verträgen, wo sogenannte Smart Contracts eingesetzt werden können.



Was sind Smart Contracts?

Smart Contracts sind sich selbst ausführende oder selbst vollziehende Verträge, die in einer Blockchain gespeichert und repliziert werden können. Die Vertragsbestimmungen werden dabei in einem Code abgebildet. Die vordefinierten Vertragsregeln werden dann von einem Computer strikt automatisch ausgeführt. Je nach Programmierung können damit Vertragsteile oder der gesamte Vertrag automatisiert werden. Ein einfaches Beispiel: Sobald die vereinbarte Zahlung eingetroffen ist, wird automatisch der Versand eines Produktes ausgelöst.

Was sind die Vorteile von Smart Contracts?

Sämtliche Nutzer eines Blockchain-Netzwerkes verfügen über eine Kopie des Vertragscodes und sorgen hierdurch dafür, dass der Vertrag nicht einseitig abgeändert werden kann. Ausserdem vollziehen sich – im Idealfall – die vereinbarten Leistungen bei Vorliegen der vordefinierten und vereinbarten Voraussetzungen automatisch. Die Leistungen können, wenn die vordefinierten Voraussetzungen erfüllt sind, nicht mehr grundlos oder böswillig verweigert werden. Dadurch ermöglichen Smart Contracts auch Geschäfte zwischen Parteien, die sich nicht vertrauen. Damit würde sich die Anzahl potenzieller Geschäftskunden für ein Unternehmen schlagartig vervielfachen. Darüber hinaus bestehen grundsätzlich keine Schwierigkeiten bei der Auslegung einer Vertragsklausel. Der Code vollzieht diese nämlich automatisch und strikt nach den vorgegebenen Regeln, ohne Interpretationsspielraum. Die Rechtsunsicherheit, die dem Abschluss von Verträgen entgegensteht, wäre somit eliminiert. Dies zumindest in der Theorie.

Welche rechtlichen Fragen stellen sich bei Smart Contracts?

Gerade der strikte Vollzug bzw. die strikte Ausführung von Smart Contracts ist rechtlich nicht unproblematisch. Der Code kann und darf nachträglich nicht mehr angepasst werden. Ermessen – ein wichtiger Bestandteil vieler Vertragsklauseln und ein Instrument, um dem Einzelfall gerecht zu werden – kann in einen Smart Contract nicht integriert werden. Die Unabänderbarkeit des definierten Codes sowie dessen starrer Vollzug können somit zu Ergebnissen führen, die keine der Parteien so gewollt hat bzw. die im Einzelfall nicht angemessen sind. Dies führt zu unzähligen Fragen an der Schnittstelle zwischen Recht und Technik. Wie soll z. B. die Möglichkeit, dass eine der Parteien bei Vertragsschluss einem Irrtum unterlegen ist, abgebildet werden? Was passiert, wenn die gelieferte Ware mangelhaft ist?

Weiter stellen sich auch neue haftungsrechtliche Fragen. Wer ist beispielsweise haftbar für einen fehlerhaften Code? Auch bewegt sich ein Smart Contract nicht in einem rechtsfreien Raum. Er untersteht wie herkömmliche Vereinbarungen einem nationalen Recht. Welches Recht soll nun aber auf einen Vertrag anwendbar sein, der dezentral und mit grosser Wahrscheinlichkeit auf Servern in einer Vielzahl von Jurisdiktionen abgespeichert ist? Kann allenfalls eine Rechtswahlklausel in den Vertrag eingebaut werden? Was passiert, wenn der Code zwingendes Recht nicht einhält und wer trägt dafür die Verantwortung?

Was bringt die Zukunft?

Die Blockchain-Technologie hat das Potenzial, die bestehenden Märkte und althergebrachten Geschäftsmodelle fundamental zu verändern. Die Zukunft wird zeigen, wie weitreichend die Veränderung tatsächlich sein wird. Fraglich ist dabei insbesondere, ob sich durch die Blockchain-Technologie Abläufe vollständig automatisieren lassen. Wir werden die Entwicklung in jedem Fall verfolgen und Klienten bei der Umsetzung begleiten.

4 Zum Moralmodul in selbstfahrenden Autos

Dr. Benedict F. Christ, LL.M.

Gegenwärtig wird häufig von ethischen Herausforderungen für selbstfahrende Autos gesprochen und ein Moralmodul für Autos gefordert.

Trolley-Problem

Hintergrund ist ein Fallbeispiel folgender Art, auch als Trolley-Problem bekannt. Ein Auto ist unterwegs. Völlig überraschend befindet sich eine Gruppe von Kindern auf der Fahrbahn. Der Lenker hat nur noch die Möglichkeit, in die Kinder zu rasen oder die Kindergruppe zu schonen, indem er sein Auto auf das Trottoir lenkt, wo er einen Greis überfahren wird.

Anders als ein Mensch könnte die Steuerung (bzw. das Moralmodul) eines selbstfahrenden Autos für eine solche Entscheidung in Zukunft sogar jede Menge Informationen zu den Beteiligten abrufen. Sie könnte zum Beispiel die kumulierten Lebenserwartungen der beiden Gruppen und vieles mehr gegeneinander abwägen, bevor eine Gruppe geopfert wird. Wohl angesichts dieser neuen Möglichkeiten wird das Trolley-Problem im Zusammenhang mit selbstfahrenden Autos häufig aufgegriffen. Dabei wird etwa diskutiert, ob es wünschbar sei, einen solchen Entscheid einem Rechner zu überlassen, wie ein solcher Entscheid zu fällen sei und ob der Gesetzgeber zunächst Regeln dazu aufstellen sollte.

Die Fragestellung ist zwar intellektuell spannend und reizvoll, hat aber wenig praktische oder rechtliche Relevanz.

Akademische Fragestellung

Zunächst scheint das Beispiel an den Haaren herbeigezogen. Nur ein extrem kleiner Bruchteil der korrekt fahrenden Lenker dürfte je in diese Situation gelangen. Korrekt fahren heisst unter anderem, gegenüber Kindern, Gebrechlichen, alten Leuten und anderen Personen, bei denen Anzeichen von inkorrektem Verhalten bestehen, besondere Vorsicht walten zu lassen. Dazu gehört insbesondere, die Geschwindigkeit anzupassen. Entsprechend kann der Lenker in solchen Situationen rechtzeitig bremsen. Selbst wenn die Situation des Trolley-Problems einträte, hätte ein Mensch kaum Zeit, Güterabwägungen zu treffen.

Das selbstfahrende Auto wird programmiert sein, die Verkehrsregeln ständig einzuhalten. Wäre dies nicht der Fall, wäre es als Produkt nicht sicher und dürfte gar nicht in Verkehr gebracht werden. Das selbstfahrende Auto muss also vorsichtig und angepasst fahren. Überdies verfügt es über eine Vielzahl von Sensoren, die das Umfeld des Wagens gleichzeitig überwachen. Ein Mensch seinerseits kann immer nur einen Punkt gleichzeitig beobachten. Somit wird das selbstfahrende Auto also sehr viel besser und oft früher erkennen, ob Grund besteht, die Geschwindigkeit anzupassen. Auch braucht es, anders als der Mensch, praktisch keine

Reaktionszeit. Bei Überraschungen ist also sein Bremsweg deutlich kürzer. Damit wird das selbstfahrende Auto wesentlich zur Verkehrssicherheit beitragen. Das Trolley-Problem wird sich somit, wenn überhaupt, in Zukunft noch viel weniger stellen.

Menschenwürde ist unantastbar

Rechtlich ist das Trolley-Problem in der Schweiz weder für Menschen noch selbstfahrende Autos ein Dilemma. Sowohl gemäss Schweizerischer Bundesverfassung als auch Europäischer Menschenrechtskonvention ist die Würde des Menschen zu achten und zu schützen. Die Menschenwürde verbietet es unter anderem, einem individuellen Menschen einen Wert zu geben oder Menschen gegeneinander aufzurechnen.

Hauptbeteiligte im Trolley-Problem sind auf der einen Seite der Autolenker und auf der anderen Seite die Kindergruppe, die unbedacht, mithin unter Verletzung der Strassenverkehrsregeln, die Strasse betritt. Der Greis ist hingegen völlig unbeteiligt und nur zufällig zugegen. Wer das Überfahren des Greises rechtfertigen will, muss von höherwertigen und minderwertigen Menschen ausgehen. Dieses Konzept gibt es beim Notstand, bei dem zum Schutz eines höherrangigen Rechtsguts (etwa des Lebens) in ein nachrangiges (etwa Eigentum) eingegriffen werden darf. Allerdings darf dieses Konzept nicht auf den Menschen übertragen werden. Jeder Mensch ist gleich viel wert und die Rettung eines Menschen rechtfertigt nicht die Tötung eines unbeteiligten Dritten. Darum darf der Lenker sein Auto nicht in den unbeteiligten Greis lenken.

Diese Regel gilt für Autosteuerungen ebenso wie einen menschlichen Lenker. Entsprechend einfach ist die Antwort auf die Frage, ob ein selbstfahrendes Auto ein Moralmodul benötigt. Ein Moralmodul ist nicht erforderlich, es reichen starke Bremsen.

5 Regulatorische Entwicklungen in der «Sharing Economy»

Barbara Schroeder de Castro Lopes, LL.M.

Im Bereich der «Sharing Economy» ist seit 2013 europaweit ein starkes Wachstum zu beobachten. Allerdings verwischt das Phänomen der «Sharing Economy» bislang klare Linien zwischen Konsument und Anbieter, Beschäftigten und Selbstständigen oder gewerbsmässiger und nicht gewerbsmässiger Erbringung von Dienstleistungen. Braucht es hier «mehr» Regulierung? Oder genügt «Selbstregulierung»? Was haben Investoren zu beachten?

Das Phänomen der «Sharing Economy»

Entgegen dem Anschein handelt es sich nicht um eine Entwicklung, die primär von uneigennützigem Teilen geprägt ist. Die meisten Formen der «Sharing Economy» sind gewinnorientiert. Das Besondere ist vielmehr, dass über das überall verfügbare Breitbandinternet auf dem Smartphone Anbieter und Nachfrager bequem und mit grosser Geschwindigkeit zusammengeführt werden können. Es wird daher auch von «Access» – oder «Collaborative Economy» gesprochen. Charakteristisch für die Online-Plattformen der «Sharing Economy» ist, dass über diese Plattformen vorgenommene Transaktionen im Allgemeinen nicht mit einer Eigentumsübertragung verbunden sind, sondern die meist vorübergehende Nutzung einer Sache zum Gegenstand haben. Zudem wird eine Plattform für Anbieter umso attraktiver, je mehr potenzielle Nachfrager diese Plattform nutzen. Umgekehrt gilt dies genauso. Diese sogenannten indirekten Netzwerkeffekte führen dazu, dass Plattformmärkte oft von wenigen Betreibern dominiert sind.

Mit dem Markteintritt von Airbnb, Uber und anderen Anbietern wurden zum Teil hochregulierte Branchen durcheinandergewirbelt. Flexibilität und niedrige Transaktionskosten sind die offensichtlichen Wettbewerbsvorteile der in der «Sharing Economy» aktiven Unternehmen. Durch eine effizientere Nutzung von Ressourcen sinkt auch die Umweltbelastung. Konsumenten kommen in den Genuss eines grösseren und oft auch kostengünstigeren Angebots, als wenn nur traditionelle Anbieter in Betracht gezogen werden. Angesichts der Einfachheit des Konzepts und der offensichtlichen Vorteile werden Investitionen in die «Sharing Economy» für Unternehmen jeder Grösse attraktiv. Und auch aus der Sicht der unter Druck geratenen Unternehmen dürfte lediglich der Ruf nach mehr Regulierung alleine langfristig nicht Erfolg versprechend sein.

Regulatorische Entwicklungen: Stand der Dinge in der Schweiz und …

Nichtsdestotrotz ist es dringend ratsam, bereits im Vorfeld von Investitionen an mögliche regulatorische Entwicklungen zu denken.

In der Schweiz sind zwar bis anhin keine nennenswerten Regulierungsbestrebungen auszumachen. Hochrangige Behördenvertreter äussern die Ansicht, dass – auch wegen der erhöhten Transparenz und Sozialkontrolle im Internet mittels Bewertungssystemen, Erfahrungsberichten oder Vergleichsportalen – Selbstregulierung ausreiche: Wer sich nicht korrekt verhalte, überlebe nicht lange, denn: Reputation sei Kern des Geschäftsmodells. Bestehende Regulierungen reichen aus – im Einzelfall entscheiden die Gerichte.

Trotzdem dürften sich mit zunehmendem Erfolg der «Sharing Economy» die kritischen Fragen beispielsweise zu Hygiene, Sicherheit, Steuern, Sozialabgaben, Versicherungen, Geldwäscherei etc. mehren. Bei aller – durchaus gerechtfertigten – Skepsis gegenüber voreiligen regulatorischen Eingriffen dürfte in der Folge auch der Druck auf die Behörden mit der Forderung nach «gleich langen Spiessen» steigen. Bereits jetzt ist der Bundesrat dazu aufgefordert worden, in einem Bericht eine

ökonomische und rechtliche Analyse zu erstellen und allfälligen Handlungsbedarf zu eruieren. Auch sind die Wettbewerbsbehörden schon mit Klagen über mögliche Wettbewerbsverzerrungen seitens der traditionellen Anbieter konfrontiert. Aus volkswirtschaftlicher Perspektive ist schliesslich anzumerken, dass sich Rechtsunsicherheit als Innovations- und Wachstumsbremse auswirken könnte.

… ein Blick in die regulatorische «Kristallkugel»: Nicht mehr, sondern besser

Eine Hilfestellung bei der Antizipation künftiger Regulierungstrends bietet oft ein Blick auf unsere Nachbarn, dies umso mehr in einem stark internationalisierten Bereich wie der digitalen Wirtschaft und angesichts des nur beschränkten unternehmerischen Interesses am schweizerischen Markt alleine. In einigen EU-Mitgliedsstaaten ist es bereits – neben Ergänzungen von branchenspezifischen Regelungen – im Fall von «Uber Pop» zu Totalverboten gekommen. Um eine mit einem regulatorischen Flickenteppich lokaler Regelungen verbundene Rechtsunsicherheit zu vermeiden und solche Totalverbote möglichst auf ein Minimum zu beschränken, hat sich die EU-Kommission dem Thema der «kollaborativen Wirtschaft» im Rahmen der Strategie für einen digitalen Binnenmarkt angenommen. Am 2. Juni 2016 hat die EU-Kommission entsprechende Leitlinien zur Regulierungspraxis veröffentlicht, welche Behörden und Marktteilnehmern Orientierungshilfen bieten sollen. Zentrale und branchenübergreifende Empfehlungen dieser Leitlinien betreffen unter anderem die folgenden Themen:

Marktzugang

Die Regulierung des Marktzugangs – beispielsweise in Form von Bewilligungsvorschriften – hat die spezifischen Besonderheiten der «Sharing Economy» zu berücksichtigen und insbesondere die folgenden Unterscheidungen zu treffen: Handelt es sich um eine Plattform, die die entsprechende Dienstleistung selbst anbietet oder tritt sie lediglich als Vermittlerin auf? Und: Handelt es sich um einen Privaten, der nur gelegentlich bestimmte Dienstleistungen erbringt oder um einen gewerblichen Anbieter? Um die jeweiligen Gruppen zu unterscheiden, hat sich innerhalb der EU der Einsatz von – gegebenenfalls auch branchenspezifischen – «Schwellenwerten» als sogenannte *«best practice»* etabliert. Diese berücksichtigen das erzielte Einkommen wie auch die Dauer der Dienstleistungserbringung. Insbesondere bei lediglich vermittelnden Plattformen und privaten Gelegenheitsanbietern soll auf Marktzugangshürden möglichst verzichtet werden.

Konsumentenschutz

Aus regulatorischer Sicht besteht die Herausforderung darin, dass die Regeln zum Schutz der Konsumenten nicht von privaten und gelegentlichen Dienstleistungserbringern, sondern lediglich von gewerblichen Anbietern zu beachten sind. Genau diese Trennlinie ist aber bei «Sharing Economy»-Plattformen schwer zu ziehen. Um Privatpersonen nicht mit unverhältnismässigen Informationspflichten und anderen administrativen Bürden zu belasten und somit die Attraktivität der Plattform nicht zu gefährden, empfiehlt die EU-Kommission für die Abgrenzung der beiden Gruppen Kriterien wie Häufigkeit der Dienstleistung oder Umsatzhöhe zu berücksichtigen. Zudem regt sie den Gebrauch von Gütesiegeln an.

Arbeitnehmerschutz und Scheinselbstständigkeit

Mit der Qualifikation als Arbeitnehmer ist die Beachtung zahlreicher zwingender Gesundheits- und Sozialvorschriften verbunden. Soweit an die auch für die Schweiz relevante und im Rahmen der Personenfreizügigkeit entwickelte EU-Definition des Arbeitnehmerbegriffs angeknüpft wird, gibt die Kommission Orientierungshilfen für deren Auslegung im Kontext der «Sharing Economy». Demnach ist unter anderem zur Beurteilung der charakteristischen Weisungsgebundenheit des Arbeitnehmers wesentlich, ob anhand des Vertrags mit der Online-Plattform der Dienstleistungserbringer frei wählen kann oder nicht, welche Dienstleistung er erbringt und auf welche Weise. Nicht entscheidend ist hingegen, ob eine kontinuierliche Leitung oder Beaufsichtigung ausgeübt wird. Tätigkeiten von wirtschaftlich untergeordneter Bedeutung sollen aber nicht dem Arbeitnehmerschutz unterstellt werden.

Besteuerung

Auch Dienstleistungserbringer in der «Sharing Economy» unterstehen der Steuerpflicht. In Betracht kommen die Einkommens- und Gewinnsteuer natürlicher bzw. juristischer Personen sowie die Mehrwertsteuer und Tourismusabgaben. Als *«best practice»* in den EU-Staaten hat sich die Zusammenarbeit zwischen Plattformbetreibern und Steuerbehörden zur Erfassung der wirtschaftlichen Tätigkeit erwiesen, wobei gleichzeitig auf die Einhaltung von Datenschutzbestimmungen zu achten ist.

Insgesamt kann die vorläufige Schlussfolgerung gezogen werden, dass bislang auf europäischer wie auch auf schweizerischer Ebene ein Trend nicht zu mehr, sondern zu besserer und auf die besonderen Bedürfnisse der «Sharing Economy» angepasstere Regulierung auszumachen ist. Auch die Abschaffung von nicht mehr zeitgemässem Regulierungsballast für traditionelle Anbieter wird empfohlen.

Empfehlungen an die Betreiber von Online-Plattformen der «Sharing Economy»

Bestehende und künftige Marktteilnehmer tun gut daran, sich frühzeitig mit allfälligen branchenspezifischen Bestimmungen, allgemeinen Regelungen und Regulierungstrends vertraut zu machen und aktiv den Kontakt zu den Behörden zu suchen. Eine Garantie, dass das eigene Geschäftsmodell mittel- und langfristig in einer regulierungsfreien Grauzone bleibt, gibt es nicht.

6 Datenschutz und Datensicherheit als Chance für Innovation

Delia Fehr-Bosshard, LL.M.

Steigende regulatorische Anforderungen an den Datenschutz und die Datensicherheit stellen Unternehmen vor Herausforderungen. Innovativen Anbietern eröffnen sich aber auch Chancen für die Differenzierung des eigenen Angebots und der entsprechenden Positionierung.

Bedürfnis der Konsumenten nach mehr Kontrolle

«I have read and agree to the Terms» trifft für Datenschutzerklärungen im Online-Geschäft selten zu. Der Nutzer liest Datenschutzerklärungen kaum und macht von Wahlmöglichkeiten wenig Gebrauch – sofern diese überhaupt bestehen. Gleichzeitig wünschen sich Nutzer mehr Kontrolle über ihre Daten. Dies scheitert oft an der mangelnden Benutzerfreundlichkeit, aber auch am fehlenden Wissen. Innovative Unternehmen können diese Bedürfnisse über die Unternehmenskommunikation bedienen und als Wettbewerbsvorteil nutzen.

Inhalt der Kommunikation zum Datenschutz

Bei der Information der Nutzer über die Datenbeschaffung und -bearbeitung («notice») ist Transparenz entscheidend. Datenschutzerklärungen, die selbst die Expertin nach der Lektüre nicht versteht, sind ohne Mehrwert für die Kundin und die Reputation. Die EU verlangt eine leicht zugängliche und verständliche Erklärung in einer klaren und einfachen Sprache. Versprechen hat der Anbieter einzuhalten, z. B. dass Chat-Mitteilungen nach Ablauf einer gewissen Dauer tatsächlich verschwinden wie zugesichert und nicht im Log gespeichert und für Dritte zugänglich bleiben wie bei Snapchat. Das Einholen der Einwilligung («consent») nach erfolgter Information ist ein Muss für die Beschaffung und Bearbeitung von Nutzerdaten. Ein ideales Produktedesign erlaubt es den Nutzern einfach und unkompliziert, Präferenzen zu definieren und Daten zu löschen. Dies erhöht die Rechtssicherheit für den Anbieter und die Qualität der Datenanalyse, z. B. wenn Nutzer die nicht mehr relevanten Daten entfernen. Der Verzicht auf die Datennutzung («opt-out») eines Nutzers ist schon aus Reputationsgründen zu befolgen. Regulatorische Anforderungen an die Sicherheit der Daten durch organisatorische und technische Massnahmen nehmen zu. Zugesicherte Sicherheitsniveaus sind einzuhalten.

Datenschutzerklärungen im neuen Design

Datenschutzerklärungen sind selten ähnlich attraktiv gestaltet wie Werbung. Es gibt jedoch Design-Alternativen zu seitenlangen Fliesstexten in Juristensprache. Bereits kleine Änderungen erhöhen die Leserfreundlichkeit; so z. B. die Verwendung von «layered notices», bei der eine kurz gehaltene Übersichtsseite mit aussagekräftigen Überschriften und Erklärungen in Alltagssprache der Leserin

einen ersten Eindruck vermittelt (z. B. IBM und Microsoft). Dem Interessierten stehen verlinkte rechtliche Erläuterungen zur Vertiefung zur Verfügung. Zusammenfassende Überschriften oder Tabellen verbessern die Lesbarkeit. Symbole oder «Icons» schaffen auch in textbasierten Erklärungen Übersicht. Grafiken dienen als Zusammenfassung für die Leserin, unabhängig vom Sprachniveau der Adressatin (z. B. eBay International AG für www.ebay.ch). Die Möglichkeiten effektiver Datenschutzkommunikation als Mittel zur Abgrenzung von der Konkurrenz sind längst nicht ausgeschöpft.

IT-Sicherheitslücken als neue Bedrohung für Unternehmen

Die bekannte Zahl der Konsumenten, die in der Schweiz von einem Datenmissbrauch («data breach») betroffen sind, ist relativ gering. Auch die Kosten für Unternehmen im Falle eines «data breachs» sind tief, gemessen am Aufwand für umfassende präventive Massnahmen. Reputationsschäden oder Auswirkungen auf den Unternehmenswert bleiben allerdings meist unberücksichtigt.

Unternehmen schaffen zur Prävention teils finanzielle Anreize in Form von «bug bounties», damit Sicherheitslücken gemeldet und nicht ausgenutzt werden. Selbst mehrere hunderttausend US-Dollar reichten z. B. bei Apple aber nicht aus zur Meldung einer Sicherheitslücke in iOS anstelle der Nutzung für Schadsoftware («malware»). Mängel in der Datensicherheit können aber auch ohne «malware» direkt den Unternehmenswert negativ beeinflussen: Der Vorwurf angeblich festgestellter Sicherheitsmängel der Produkte, z. B. Herzschrittmacher der St. Jude Medical, belasten den Aktienwert. Für eine Zielgesellschaft in Übernahmeverhandlungen kann dieser Vorwurf den Verkaufspreis drücken oder den Verkauf verunmöglichen. Die (angebliche) Identifikation von Sicherheitsrisiken durch Dritte, z. B. Konkurrenten, hat bei technologieintensiven Branchen enormes Schädigungspotenzial.

Markt für Sicherheitslösungen

Vor allem KMU können es sich selten leisten, im Bereich Datensicherheit intern die notwendige Fachkompetenz aufzubringen. Auch die öffentliche Verwaltung ist zudem immer öfter Ziel von Angriffen. Eine Zusammenführung von Wissen und Fähigkeiten in diesem Bereich bietet ein Betätigungsfeld für innovative private Anbieter, aber auch für «public private partnerships».

Prävention vs. Cyberinsurance

Geschäftsleitungen behandeln Datensicherheit oft als reines «compliance»-Thema. Die meiste Aktivität erfolgt nach Bekanntwerden eines «data breach». Die zunehmende Digitalisierung und Vernetzung, z. B. in Form des Internet of Things (IoT), multipliziert das Risiko für Unternehmen. Da Unsicherheit der grösste Feind der Unternehmensentwicklung ist, investieren Unternehmen mit der notwendigen Finanzkraft in Versicherungslösungen (sog. «cyberinsurances»), um die direkten finanziellen Risiken abzufedern. Abstufungen der Prämien je nach ergriffenen Massnahmen und Ratings zur Evaluation von Sicherheitslevels sollen notwendige Anreize zur Prävention schaffen. Anbieter von cybersecurity-Lösungen setzen Anreize zur Investition in die Prävention anstelle von rein nachgelagerten Versicherungslösungen, indem sie selbst Garantien für die Sicherheit ihrer Produkte abgeben. Ob Garantie oder Versicherung – Reputationsschäden lassen sich nur durch direkte Massnahmen zur Prävention im Unternehmen vermeiden.

Server-Lösungen in der Schweiz

Das Schweizer Datenschutzrecht erlaubt den Transfer von Personendaten ins Ausland. Sofern das Zielland gemäss Liste des Eidgenössischen Datenschutzbeauftragten (EDÖB) keinen adäquaten Datenschutz bietet, bedarf es für die Bekanntgabe der Daten eines anderen Rechtfertigungsgrundes. Vor allem sicherheitssensitive Branchen wie das Gesundheits-, Banken- oder Rechtswesen sind gehalten, Sicherheitsrisiken zu vermeiden. Mit steigenden Anforderungen in der Schweiz und in der EU sowie den Rechtsunsicherheiten im Verhältnis mit den USA bieten sich Chancen für Unternehmen mit Schweizer Cloud-Angeboten (z. B. Webhosting von Hostpoint AG oder Swisscom myCloud mit dem claim «Security in the heart of Switzerland»). Die Vermarktung muss auch einem Geschäftsführer, der möglicherweise über keine vertieften IT-Kenntnisse verfügt, die Vorzüge einer verlässlichen Schweizer Lösung aufzeigen.

Marketing und Vertrieb im digitalen Umbruch

7 Branding in Social Media: Schutz des Brands auf dem Online-Marktplatz

Delia Fehr-Bosshard, LL.M.

Social Media bieten einen internationalen Marktplatz mit tiefen Eintrittsbarrieren. Sie erlauben die Interaktion mit Nutzern, Kunden, Fans und solchen, die es noch vom Brand, d. h. dem Angebot, der Marke und der Reputation, zu überzeugen gilt. Online Branding birgt aber aufgrund der Internationalität und raschen Verbreitung rechtliche Fallstricke, die in der Branding-Strategie zu adressieren sind.

Gefährdung des Brands in Social Media

Der internationale Zugang zu sozialen Medien erhöht den Druck auf den eigenen Brand. Rechtliche Gefahren für den Brand beim Einsatz in sozialen Medien sind bspw. die folgenden:

- Unberechtigte Dritte können den Brand für ihre eigenen Zwecke verwenden, z. B. als Profilnamen. Wenn auf einer Plattform «first come, first served» gilt, kann ein Dritter den Brandauftritt verhindern. Einige Plattformen vergeben identische Profilnamen mehrmals, wodurch konkurrierende Profile existieren können.
- Dritte können ein geschütztes Zeichen informativ verwenden, ohne Markenrechte zu verletzen. Die Abgrenzung vom unerlaubten Gebrauch als Kennzeichen ist in sozialen Medien noch schwieriger zu ziehen als z. B. in Printmedien.
- Eine Domainregistrierung mit dem Brand in der URL kann markenrechtlich zulässig sein, wenn Dritte über die Webseite keine gleichartigen Leistungen anbieten.
- Die Verwendung fremder Brands in Parodien ist weitgehend erlaubt. Die Verbreitung falscher oder irreführender Angaben ist aber persönlichkeits- und/oder lauterkeitsrechtlich problematisch.
- Erlaubt der Brand-Inhaber die Nutzung des Zeichens durch Dritte, besteht online die Gefahr der Verwässerung, z. B. durch Kombinationen oder Abänderungen der Marke. Im Extremfall droht on- und offline der Verlust des Markenschutzes. Ab 2017 können Dritte ohne vorgängiges Gerichtsverfahren die Löschung der Marke wegen Nichtgebrauchs beim Eidgenössischen Institut für Geistiges Eigentum verlangen.
- Für den Werbetreibenden ist es aufwändig, den Überblick über kollidierende Rechte zu behalten. Auch Plattformbetreiber stellen Bedingungen auf für die Integration ihrer eigenen Marken und urheberrechtlich geschützter Icons in der Werbung Dritter, sichern sich selbst aber umfangreiche Nutzungsrechte an Inhalten der Nutzer zu.

Nationales Werberecht für Online-Branding

Nationales Werberecht gilt auch online und kann eine Lokalisierung des Online-Branding notwendig machen. Die Schweiz kennt insbesondere folgende werberechtlichen Anforderungen:

- Werbung in der Schweiz darf unabhängig vom verwendeten Kanal nicht zu Täuschung oder Irreführung Anlass geben. Werbeangaben müssen wahr und klar sein. Schleichwerbung stellt ein lauterkeitsrechtliches Risiko dar und schadet der Glaubwürdigkeit. Hinweise wie «promoted by» oder «paid content» erhöhen die Transparenz und trennen den redaktionellen Inhalt von der Werbung.
- Versuche zur Attraktivitätssteigerung durch gekaufte «likes» oder «friends» sind intransparent. Es existiert keine Gerichtspraxis dazu in der Schweiz. In Deutschland gelten solche Praktiken als irreführend.
- Die Impressumspflicht, bekannt aus der EU, existiert in abgeschwächter Form auch in der Schweiz: Wer seine Leistungen elektronisch

anbietet, muss klare und vollständige Angaben zu Identität und Kontaktadresse machen.
- Spezialbestimmungen für bestimmte Produkte und Werbeformen (z. B. Heilmittel, Lebensmittel, Alkohol, Tabakprodukte, Lotterien, Preisausschreiben und Wettbewerbe) sowie private Regelwerke (z. B. die Grundsätze der Lauterkeitskommission, Empfehlungen des Verbandes IAB Schweiz, Standesregeln/Richtlinien für Personen in Medizinalberufen und Anwälte) gelten auch online.

Rechtlicher und faktischer Schutz für Online-Branding-Elemente

Der Schutz von Online-Branding-Elementen richtet sich nach lokalem Recht. In der Schweiz sind viele Fragen (noch) nicht gerichtlich geklärt. Zentral sind folgende Schutzmassnahmen:
- Nach der Festlegung von Kernmärkten sind nationale Marken zu registrieren. Zeichen (z. B. Begriffe, Grafiken) sind als Marken schutzfähig, wenn sie eine betriebliche Herkunft von Waren oder Dienstleistungen bezeichnen. Das gilt z. B. für Blog-Titel nicht, wenn der Blogger damit den Inhalt des Beitrags beschreibt. Die Schweiz kennt, anders als Deutschland, keinen Titelschutz. Nur im Einzelfall sind Titel urheberrechtlich und/oder lauterkeitsrechtlich geschützt.
- Die Registrierung auf Social Media bewirkt einen faktischen Schutz, da Plattformen teils eine Verifizierung von Profilen anbieten. Die Profile sind aktiv zu bewirtschaften.
- Der eigene Brand bleibt nur stark, wenn der Inhaber ihn gegen Dritte verteidigt. Zentrale Instrumente sind Markenüberwachungen, Firmen- und Domainrecherchen sowie die Überwachung der relevanten Social-Media-Kanäle. Die Benutzung des Schutzvermerks ® für registrierte Marken signalisiert eine konsequente Verteidigung.
- Die scheinbare Anonymität des Internets macht es aufwändiger, Verletzer zu identifizieren. Abmahnungen erzielen aber gute Erfolge, da die Rechtsverletzung häufig aus Unwissenheit erfolgt. Für Rechtsverletzungen im Internet besteht in der Regel schweizweit eine gerichtliche Zuständigkeit gegen den Verletzer.
- Viele Betreiber bieten Hand zur Beseitigung rechtsverletzender Inhalte. Betreiber regeln die Instrumente zum Rechtsschutz für Brand-Inhaber in den Nutzungsbedingungen, teils gestützt auf Selbstregulierung (z. B. den simsa code-of-conduct hosting).

Branding-Strategie adressiert Risiken und Unsicherheiten

Zum Schutz des Brands und der Reputation gehört auch die Kontrolle der Produkte und Leistungen, für welche eine Marke on- und offline durch den Inhaber und Dritte verwendet werden darf und soll. Regeln für Dritte haben mehr Gewicht, wenn der Brand-Inhaber selbst eine schlüssige Strategie verfolgt. Dazu gehört die Schulung der eigenen Mitarbeitenden zum Verhalten in Social Media. Die (interne) Branding-Strategie soll die Toleranzgrenze für Rechtsverletzungen definieren. Ein verhältnismässiger Ansatz ist aus Kostengründen zentral, aber auch deshalb, weil überschiessende Aktionen online zum Bumerang mit Reputationsrisiken werden können. Die eigene Strategie ist regelmässig zu evaluieren. Eine klar definierte und gelebte Branding-Strategie unterstützt auch den Rechtsberater darin, die geeigneten Schritte zu ergreifen und den Brand-Inhaber effizient zu beraten.

8 Personalisierte Werbung

Dr. Rolf Auf der Maur

Persönlichkeitsverletzung oder Garant für Medienvielfalt?

Online-Werbung lässt sich präzis auf die Bedürfnisse der Nutzer abstimmen – sofern diese bekannt sind. Der Erhebung und Verarbeitung von Personendaten zwecks Targeting sind aber enge datenschutzrechtliche Grenzen gesetzt. Diese Grenzen könnten bald noch enger werden, wenn die Schweiz ihr Recht der ab Mai 2018 in allen EU-Staaten verbindlichen Datenschutz-Grundverordnung (DSGVO) anpasst. Es bleibt zu hoffen, dass die Schweiz der Personalisierung von Werbung nicht unnötig grosse Steine in den Weg legt. Immerhin sind Werbeeinnahmen auch in Zukunft unabdingbare Voraussetzungen für den Erhalt der Medienvielfalt.

Medien unter Druck

Der Konsum von Werbung gilt vielen Mediennutzern eher als Zwang denn als Vergnügen. Die Zunahme von Ad-Blockern bei Online-Werbung sowie die Möglichkeit, bei zeitversetzter TV-Nutzung Werbung zu überspringen, führen zu messbaren Umsatzeinbussen bei Online-Plattformen und TV-Sendern. Dies geht einher mit einer schwindenden Zahlungsbereitschaft für Medieninhalte, weil diese über zahlreiche Multiplikatoren wie etwa LinkedIn und Facebook oder über Aggregatoren wie Google News, Newsvine, Daily Beast oder Upday auch kostenlos zugänglich sind. Von den gebührenfinanzierten öffentlichrechtlichen TV-Sendern abgesehen, können diese Entwicklungen existenzbedrohende Auswirkungen annehmen und die Medienvielfalt gefährden.

Hinzu tritt, dass Online-Werbung immer weniger in einem bestimmten Umfeld platziert wird (beispielsweise in der NZZ im Vertrauen auf eine wirtschaftsaffine Leserschaft), sondern über Netzwerke, welche Konsumenten über verschiedene Plattformen hinweg identifizieren und ihnen Werbung ausliefern, die ihren vermuteten Interessen entspricht. Targeting, Auslieferung und Auswertung laufen weitgehend automatisiert ab (sog. «Programmatic Advertising»). Die Kontrolle über Werbeinventar und Preise verlagert sich immer mehr weg von den Plattformbetreibern und hin zu grossen Werbenetzwerken. Nur grosse Netzwerke können den Werbeauftraggebern eine relevante Reichweite bieten. Diese Entwicklung setzt national oder regional tätige Medien unter Druck.

Verschärfung des Datenschutzes in der EU

Internet und Big Data haben ganz neue Dimensionen für die Erhebung und Verarbeitung von (Personen-)Daten erschlossen. Die Datenschutzgesetze europäischer Prägung stammen aus den 80er-Jahren und sind nicht für die digitale Netzgesellschaft gedacht. Stand früher der Schutz der Persönlichkeit des einzelnen vor Missbrauch seiner Daten durch den Staat im Vordergrund, geht es heute vermehrt um Themen wie Datensicherheit oder den Schutz vor automatisierten Entscheiden und vor Filtern, die Medieninhalte aussortieren. Ausserdem findet Datenaustausch über Internet meist

grenzüberschreitend statt, weshalb gerade die EU die in ihrem Binnenmarkt geltenden Regeln vereinheitlichen wollte. Das Vorhaben war über Jahre heftig umstritten. Bei der im Dezember 2015 verabschiedeten Endfassung der EU-Datenschutz-Grundverordnung (DS-GVO) blieben zahlreiche Anliegen der Medien und der Werbeindustrie auf der Strecke.

Online-Plattformen müssen künftig für Portabilität der Nutzerdaten sorgen, diese aber auf Verlangen des Nutzers oder nach einer bestimmten Zeit wieder vollständig löschen («Recht auf Vergessen»). Ausserdem gelten künftig detaillierte Informationspflichten. Betroffene müssen vorab informiert werden, ob sich die Bearbeitung ihrer Daten auf Gesetz, Einwilligung oder auf ein berechtigtes Geschäftsinteresse stützt. Dabei ist bereits heute umstritten, ob Werbung als Geschäftsinteresse anerkannt sein soll. Im Zweifelsfall ist eine ausdrückliche, freiwillige und informierte Einwilligung der Betroffenen einzuholen. Datenschutzerklärungen werden infolge der strengeren Informationspflichten noch länger. Bereits heute liest diese kaum jemand. Wer es trotzdem tut und beispielsweise mit der Bearbeitung seiner Daten im Ausland nicht einverstanden ist, hat wenig Handlungsoptionen: faktisch kann er bloss auf die Inanspruchnahme des Dienstes verzichten. Die neuen Regeln sind ab dem 25. Mai 2018 in allen EU-Ländern direkt anwendbar. Für Aufmerksamkeit in den Chefetagen sorgt die dem Kartellgesetz nachempfundene Bussenregelung von bis zu 4 % des weltweiten Umsatzes.

Parallel dazu bleibt die sog. Cookie-Richtlinie unverändert in Kraft. Dieser Richtlinie ist es zu verdanken, dass Nutzer von in der EU betriebenen Online-Plattformen zuerst Hinweise zu Cookies zu sehen und deren Einsatz zuzustimmen haben, bevor sich der gesuchte Inhalt nutzen lässt. Alle diese Einschränkungen behindern Innovation und Schlagkraft europäischer Plattformen und stärken indirekt die grossen globalen Plattformen, die sich mit weniger formalistischen Einschränkungen auf die Bedürfnisse ihrer Nutzer ausrichten können.

Chance für medienfreundliche Regulierung in der Schweiz

Die Schweiz ist auf ungehinderten Austausch von Personendaten mit den umliegenden Ländern angewiesen. Sie muss ihr Datenschutzgesetz anpassen, um die Anerkennung eines gleichwertigen Datenschutzes gegenüber der EU nicht zu verlieren. Die Vernehmlassung zu einer Totalrevision des Datenschutzgesetzes sollte bereits seit September 2016 laufen, ist aber infolge von Differenzen bei der Ämterkonsultation verspätet. Das geltende Gesetz stammt aus dem Jahr 1992. Es statuiert bewährte Grundsätze wie die Zweckbindung und das Verhältnismässigkeitsprinzip, ohne sich in detaillierten Regelungen zu verlieren. Solche finden sich in Spezialgesetzen mit besonderer Risikolage (Energie, Finanzwesen, Gesundheitswesen).

Es ist zu hoffen, dass der Schweizer Gesetzgeber auf detaillierte Anforderungen an eine ausdrückliche und informierte Zustimmung zu Datennutzungen verzichtet. Im Zeitalter von Big Data bleibt die informierte Zustimmung des einzelnen Nutzers eine Fiktion. Die wahren Risiken liegen bei unbeabsichtigter oder unerlaubter Offenlegung von Daten (infolge von Hacking und Data Breaches) sowie bei automatisierten Entscheiden und Filtern, die für den Einzelnen gravierende Folgen haben können. Hier weist das Gesetz aus dem Jahr 1992 Lücken auf, die durch Anforderungen an Transparenz und Offenlegung von Fehlern (insb. bei Data Breaches) zu schliessen sind.

In der Praxis werden sich viele Schweizer Unternehmen der Anwendbarkeit der DS-GVO nicht entziehen können. Denn diese greift unabhängig vom Standort eines Unternehmens immer dann, wenn Daten von EU-Bürgern verarbeitet werden oder wenn die Bearbeitung in der EU stattfindet. Diese Umstände sind bei nationalen und regionalen Schweizer Online-Medien allerdings nicht gegeben, weshalb sich zumindest für diese eine liberalere Regulierung treffen liesse. So wäre etwa in Betracht zu ziehen, im Schweizer Recht einen expliziten Rechtfertigungsgrund für die Bearbeitung von Personendaten durch Medienunternehmen zu schaffen. Dies wäre ein Beitrag zur Erhaltung der Medienvielfalt in der Schweiz.

Bessere Werbung für erhöhte Akzeptanz

Werbeauftraggeber und Online-Plattformbetreiber tun aber gut daran, sich nicht auf die Zurückhaltung des Gesetzgebers zu verlassen. Letztlich hängt die Wirksamkeit von Werbeformaten von der Akzeptanz beim Publikum ab. Am 15. September 2016 haben sich die wichtigen internationalen Verbände und Betreiber von Online-Plattformen zur «Coalition for better ads» zusammengeschlossen. Sie wollen in gemeinsamer Selbstregulierung dafür sorgen, dass die als besonders störend empfundenen Werbeformen (etwa Pop-ups und Layovers) von den Bildschirmen der Medienplattformen verschwinden. Noch steht der Tatbeweis aus, dass dieses Vorhaben gelingt und Werbung beim Publikum künftig vermehrt Akzeptanz findet.

9 Native Advertising: Todesstoss für Publizistik oder Rettungsring für Medien?

Dr. Rolf Auf der Maur

Dr. Thomas Steiner, LL.M.

Werbeinhalte lassen sich bei digitaler Nutzung von Medien zunehmend vermeiden: Ad Blocker unterdrücken die gängigen Werbeformate auf Websites und Smartphones. Angesichts dieser Entwicklung ist es naheliegend, dass Werbeauftraggeber ihre Botschaften am liebsten in redaktionelle Inhalte verpacken: «Native Advertising» oder «Sponsored Content» erzielen hohe Zuwachsraten und generieren damit willkommene Zusatzeinnahmen für Medienanbieter. Aus rechtlicher Sicht ist eine transparente Information der Nutzer erforderlich, wobei ein grosser Ermessensspielraum für die Umsetzung besteht.

Formen von Native Advertising

Immer mehr Nutzer lassen digitale Werbung mit *Ad-Blocker-Software* unterbinden – auch auf Smartphones und Tablets. Die Plattformbetreiber versuchen, mit technischen Massnahmen dagegenzuhalten. Doch die Anbieter von Ad-Blocker-Software blockieren Gegenmassnahmen umgehend. Auch TV-Werbung steht unter Druck: TV-Verbreiter bieten ihren Kunden bei zeitversetzter Nutzung von Programmen die Möglichkeit, Werbung zu überspringen. Davon machen immer mehr Zuschauer Gebrauch, weshalb die Reichweite der Werbeblöcke zurückgeht.

Ein weiterer Grund für das Aufkommen von Native Advertising ist die steigende mobile Nutzung von Medieninhalten aller Art. Nutzer akzeptieren Online-Werbung auf mobilen Geräten weniger als auf grösseren Bildschirmen. Viele traditionelle Online-Werbeformate wie Banner oder Skyscraper sind für mobile Bildschirme gar nicht verfügbar. Um die physikalischen Grenzen des Mobile Marketings zu überwinden, verpacken Werbeauftraggeber und ihre Agenturen Werbung so, dass sie vom Aussehen und der Wirkung her redaktionellen Inhalten (oder Inhalten von anderen Nutzern) gleicht.

Beispiele von Native Advertising sind:

- Advertorials (eine Mischung aus den englischen Wörtern «Advertising» und «Editorial»)
- Gesponserte Beiträge auf Newsportalen oder in sozialen Medien
- Endorsements (z. B. in Tweets oder Facebook-Posts von Sportlern oder Musikern)

Erlaubt ist, was nicht irreführt

Native Advertising ist unter Schweizer Recht erlaubt. Explizite gesetzliche Einschränkungen finden sich einzig für lineare TV- und Radio-Programme. Das Bundesgesetz über Radio und Fernsehen (RTVG) verlangt, dass Werbeinhalte innerhalb von klar abgegrenzten Werbeblöcken ausgestrahlt werden. Sponsoring und Product Placements sind am Anfang und am Ende einer Sendung sowie nach jeder Werbeunterbrechung zu deklarieren. Sponsoren dürfen keinen Einfluss auf den Inhalt von Sendungen nehmen, und Product Placements dürfen keinerlei Werbewirkung entfalten. Bei (interaktiven) Online-Plattformen gelten die weniger spezifischen Grundsätze des Gesetzes gegen den unlauteren Wettbewerb (UWG). Ausserdem haben die Selbstregulierungsorgane Schweizerische Lauterkeitskommission (SLK) und Presserat gewisse Grenzen und Standards gesetzt.

Das *UWG* bezweckt die Gewährleistung fairen Wettbewerbs. Eine Verschleierung des Werbezwecks eines Inhalts verstösst nicht in jedem Fall gegen das UWG. Unlauter ist die Verschleierung aber dann, wenn sie unterschwellig bzw. schleichend den Kaufentscheid des Konsumenten beeinflusst oder zur Täuschung Anlass gibt.

Die *Grundsätze der SLK* erlauben die Integration von bezahlten Inhalten wie Publireportagen und anderen gesponserten Beiträgen, solange die

bezahlten Inhalte mit geeigneten Hinweisen vom Redaktionsteil abgegrenzt werden. Auch gemäss dem von der SLK angewandten *ICC Code of Advertising and Marketing Communication Practices (ICC Code)* gilt, dass Werbung und andere Formen kommerzieller Kommunikation klar als solche erkennbar sein müssen.

Die *Erklärung der Pflichten und Rechte der Journalistinnen und Journalisten* schreibt vor, bezahlte Inhalte erkennbar von redaktionellen Inhalten abzugrenzen. Zudem untersagen die Grundsätze der SLK und des Presserats sogenannte Koppelungsgeschäfte: Die Akquisition von Werbung darf nicht mit der Verpflichtung des Journalisten oder Herausgebers verbunden werden, ein bestimmtes Thema zu wählen oder positiv über das Produkt oder die Dienstleistung eines Werbeauftraggebers zu schreiben.

Transparenzhinweise als Lösung

Es liegt in der Natur von Native Advertising, die Grenzen zwischen Werbung und redaktionellem Inhalt zu vermischen. Umso wichtiger sind die *Herstellung von Transparenz und die Abgrenzung vom eigentlichen Redaktionsteil.* Gemäss den allgemeinen Grundsätzen des UWG müssen Transparenzhinweise wahr und klar sein. Es gibt keine besonderen Vorschriften hinsichtlich der Wortwahl oder der Grösse und Darstellung der Hinweise. Wichtig ist jedoch, dass Konsumenten die Transparenzhinweise unabhängig vom verwendeten Gerät erkennen, lesen und verstehen können.

Webseiten werden auf mobilen Geräten anders dargestellt als auf Laptops oder Desktops. «Responsive» gestaltete Online-Plattformen müssen auf kleinen Bildschirmen mit sehr wenig Text auskommen. Nutzer sollten nicht bis zum Ende eines Beitrags scrollen müssen, um die Transparenzhinweise zu sehen. Sie erwarten, dass bei gesponserten Beiträgen bzw. Advertorials Hinweise wie «gesponsert» oder «Werbung» unmittelbar *über oder unter* dem Beitrag angezeigt sind.

Social Media mit eigenen Regeln

Kreativere Lösungen sind bei Endorsements gefragt. Sportler, Musiker oder Schauspieler mit *Endorser-Funktion* werden zu Werbebotschaftern der jeweiligen Markenhersteller. Twittert oder postet ein Sportler z. B., dass er gerade im Testcenter der Firma X ist, um sein neues Rennrad zu testen, kann ein Transparenzhinweis notwendig sein. Dies gilt zumindest dann, wenn der Sportler in seiner Funktion als Endorser postet und seine positive Beschreibung des getesteten Rennrads der Verkaufsförderung dienen soll. Auf seine Endorser-Funktion kann der Sportler z. B. mit dem Zusatz «#XBotschafter» hinweisen.

Allerdings löschen Social-Media-Plattformen Werbeinhalte umgehend, wenn sie nicht im Rahmen eines der vom Betreiber der Plattform zur Verfügung gestellten Formate verbreitet werden. Die grossen Social-Media-Plattformen wie Facebook und Youtube stellen dabei ihre eigenen Regeln auf und sind auch in der Lage, innerhalb ihres Auftritts Werbeblocker auszuschalten. Auch haben sie ihre eigenen Sanktionsmöglichkeiten, wenn Werbeauftraggeber die Regeln nicht einhalten: oftmals droht nicht nur die Unterdrückung der Werbeinhalte, sondern gar die Löschung des gesamten Accounts.

10 Growth Hacking: So funktioniert das Marketing der Zukunft

Gastbeitrag von Michel Kaufmann, JobCloud AG

Haben Sie jemals Werbung für Uber, Dropbox oder Airbnb gesehen? Und trotzdem kennen und nutzen viele Konsumenten diese Dienstleistungen. Es ist interessant sich zu überlegen, woher man diese modernen Produkte kennt und weshalb man sie nutzt. Viele erfahren über ihre Freunde von diesen Services, lesen in Online-Medien darüber oder sehen auf Facebook und Co. Beiträge von begeisterten Kunden. Diese Marken wurden nie auf Werbeformaten in Online-, TV- oder Printmedien angepriesen: Die Vermarktung funktioniert anders und «Growth Hacking» spielt dabei eine wichtige Rolle.

Ein überzeugendes Produkt verkauft sich fast selber

Die Kunden von Uber und Co. haben oft ein überraschendes oder gar begeisterndes Kundenerlebnis, wenn sie die Dienstleistung das erste Mal nutzen. Davon berichten sie den Kolleginnen und tragen so die Botschaft weiter. Die Kunden agieren als Botschafter; so funktioniert das virale Marketing. Sie sprechen darüber, weil das Produkt- und Kundenerlebnis einzigartig ist. Der sog. «Product/Market fit» (PMF) ist optimal. Sean Ellis – VC Investor, Berater und CEO von Growthhackers.com, der die Begriffe Growth Hacking und Product/Market fit seit 2013 wesentlich geprägt und allgemein bekannt gemacht hat – definiert den Begriff so: «PMF ist die Voraussetzung dafür, um Marketing effektiv skalieren zu können.»

Growth Hacking beginnt mit diesem Product/Market fit und beschäftigt sich iterativ damit. Ein erfolgreiches Produkt oder Kundenerlebnis ist nicht statisch, es soll sich entlang der dynamischen Bedürfnisse und Verhaltensweisen der Kunden laufend verbessern. Zu Beginn wurde die Uber-Rechnung durch einen einzigen Kunden bezahlt. Heute kann eine Fahrt unter Freunden einfach über die App aufgeteilt werden. Das ist praktisch und fördert die Viralität.

Die Viralität einer Dienstleistung kann durch ein enges Verzahnen von Produktmerkmalen und Marketingfunktionen gefördert werden. Konkret: Wenn ich einen neuen Dropbox-Kunden vermittle, bekommen wir beide ein Guthaben für gratis Speicherplatz. Uber vergibt Gutscheine für Freifahrten. Selbst Tesla nutzt diese Incentivierung der Kunden für den Verkauf von Neuwagen und investiert kein Geld für konventionelle Werbung. Die Kunden berichten als Evangelisten auf den sozialen Medien über ihre positiven Erlebnisse und bewerben das Produkt.

Der Growth Hacker ist ein interdisziplinärer Macher

Growth Hacker sind unternehmerisch denkende Product Manager/Online Marketeers/Verkäufer. Sie nutzen die verschiedenen digitalen Möglichkeiten zur laufenden Verbesserung und Inszenierung der Produkte. Sie erstellen Inhalte, sind Spezialisten in Suchmaschinenoptimierung und -marketing (SEO, SEM) und fördern die Viralität auch über Social Media Marketing (Facebook Ads etc.). Die Arbeitsmethodik im Growth Hacking ist agil und Entscheide werden nach A/B-Tests faktenbasiert getroffen. Mit diesen Tests werden Varianten von E-Mails, Webpages oder digitalen Werbemitteln laufend miteinander verglichen. In der digitalen Welt ist alles messbar.

«Der Growth Hacker hat das Ziel, durch analytisches Denken und Fokus auf den Kunden das Wachstum des Unternehmens zu steigern, Conversions oder Verkäufe zu erhöhen.»
Stefan Steiner, Managing Director venturelab (IFJ)

Es ist besonders interessant, wenn man klassisch organisierte Marketing-/Produkt- und Verkaufs-

Teams mit dem Ansatz des Growth Hacking vergleicht. Während die meisten Firmen nach Fachgebieten organisiert sind, agiert ein Growth-Team interdisziplinär. Klassisch erarbeitet man Konzepte, Briefings und delegiert die Umsetzung von Werbe- oder Marketingmitteln häufig an Agenturen – das alles dauert seine Zeit und kostet viel Geld. Entscheide werden aufgrund von Meinungen und persönlichen Präferenzen oder vagen Erfahrungswerten getroffen. Aussagen wie: «Das gefällt mir aber gar nicht» oder «Diese Werbeidee hat einigen Kunden gefallen» hört man oft in klassischen Marketingmeetings. Es wird selten experimentiert und mit Daten argumentiert. Ein interdisziplinär arbeitendes Growth-Team generiert Ideen, setzt diese möglichst zügig und wenn immer möglich selbstständig um und sammelt Daten. Viele Experimente misslingen und so werden diese Ideen schnell verworfen. Man konzentriert sich auf die funktionierenden Ideen und optimiert diese mit A/B-Tests laufend weiter. Man arbeitet unentwegt daran, den besten «Hack» zu finden, um das Wachstum exponentiell zu beschleunigen.

Ein Growth Hacker ist bestrebt, Produkte und das Marketing mit digitalen Mitteln zu optimieren, ineinander zu verzahnen und soweit möglich zu automatisieren. Das Ziel besteht darin, eine Wachstumsmaschine zu bauen und diese laufend zu verbessern. Die Bezeichnung «Hacker» steht für sehr gute technische Kenntnisse bis hin zum Programmieren. Der Growth Marketeer ist bestrebt, kreative «Hacks» zu finden, mit welchen Wachstum generiert werden kann. Das kann bedeuten, dass im Web verfügbare Daten aggregiert, ausgewertet und für die Marketing-Automatisierung genutzt werden. Dies darf natürlich nur im gesetzlichen Rahmen des Datenschutzes und der Privatsphäre passieren.

Ist Growth Hacking bloss ein Modebegriff?

Kritische Meinungen gibt es noch wenige zu diesem Thema zu lesen. Ben Harmanus – Community Manager des Landingpage-Tools Unbounce.com – schrieb kürzlich einen Blogartikel zum Thema und erklärt darin, dass nur die wenigsten Personen die Fähigkeiten haben, um mit guten Programmierkenntnissen, Kreativität und unternehmerischem Denken tatsächlich Growth Hacks mit explosionsartigem Wachstum zu schaffen. Die meisten sogenannten Growth Hacker sind Community-, Content- oder Online-Marketing-Manager, die sich mit diesem modischen Jobtitel schmücken. Ich bin der Ansicht, dass es beim «Growth Hacking» um die altbekannten Mechanismen des Marketings geht, gepaart mit den digitalen Werkzeugen und einer agilen Arbeitsweise, die in der Software-Entwicklung schon seit Jahren angewandt wird. Es ist also doch mehrheitlich alter Wein in neuen Schläuchen. Trotzdem ist es meiner Meinung nach angebracht, mit einem neuen, frechmutigen Namen die gewohnte Arbeitsweise infrage zu stellen und sich wieder auf die Kernidee des Marketings zu besinnen.

In den USA gibt es bereits zahlreiche Firmen, die Growth-Teams beschäftigen. Dies erkennt man an den zahlreichen Jobangeboten in diesem Bereich. Auch in der Schweiz suchen Unternehmen vermehrt Growth Hacker, allen voran Start-ups, welche kosteneffizient einen globalen Absatzmarkt adressieren und entsprechend ihrer Firmengrösse und DNA agil arbeiten möchten.

Mehr zu diesem spannenden Thema erfahren Sie mit einer Suche nach «Growth Hacking» auf Google oder Youtube. Growthhackers.com von Sean Ellis ist eine wertvolle Quelle für Informationen. Auf Refind.com, einem Schweizer Start-up von Gründer Dominik Grolimund, findet man laufend lesenswerte Beiträge unter den Tags «Growth», «Growth Hacking» oder «Growth Marketing».

11 Digitaler Vertrieb: Kartellrecht als Wegbereiter

Klaus Neff, LL.M.

Digitaler Vertrieb bedeutet, dass die Vermarktung und der Absatz von Produkten oder Dienstleistungen über digitale Vertriebswege erfolgen. Sowohl für die Kommunikation mit dem Kunden, für die Bereitstellung von Leistungen als auch für die Abwicklung der Geschäfte wird also in erster Linie das Internet als Vertriebskanal benutzt.

Insbesondere Hersteller von Markenartikeln oder komplexeren und beratungsintensiveren Produkten nehmen die Digitalisierung als Bedrohung wahr. Ihre Bemühungen zur Kontrolle oder gar Behinderung des digitalen Vertriebs stösst aber zunehmend auf Widerstand von Kartellbehörden. Aufgrund der damit verbundenen Risiken empfiehlt es sich, rechtzeitig angemessene Rechtsberatung beizuziehen.

Veränderte Rahmenbedingungen

Das Fundament jeder geschäftlichen Transaktion ist zwischenmenschliche *Kommunikation.* An diesem banalen Umstand hat die rasante Entwicklung insbesondere der Informationstechnologie zwar nichts geändert. Kommunikation ist heute aber praktisch jederzeit und überall möglich. Und allerlei produkt- oder dienstleistungsrelevante *Informationen* (Herkunft, Beschaffenheit, Qualität, Preis, Lebensdauer etc.) sind ständig und überall verfügbar. Zugleich eröffnet namentlich bei Konsumgütern die dauernde Rückkoppelung zwischen Nachfrage und Produktion eine laufende Verkürzung von Produktionszyklen, gefolgt von entsprechend kürzeren Angebotszyklen. Das Kauf- und das Nutzungsverhalten wie auch Marktbedingungen ändern sich also mit rasanter Geschwindigkeit.

Digitaler Vertrieb als Chance

Herkömmliche Vertriebsstrukturen sind diesen veränderten Umständen nur bedingt gewachsen. Um *längerfristig konkurrenzfähig zu bleiben,* müssen daher insbesondere für Konsumgüter bestehende Vertriebssysteme angepasst und neue Vertriebswege erschlossen werden. Die Ergänzung bestehender Vertriebsstrukturen durch digitalen Vertrieb erscheint dabei nicht nur unvermeidbar, sondern geradezu geboten. Dies gilt vorab für Unternehmen, die ihre Vertriebsreichweiten vergrössern, ihre Besucher- und Verkaufszahlen erhöhen und zeitnah im Markt agieren möchten. Digitaler Vertrieb ist aber auch für Unternehmen sinnvoll, die sich neu am Markt positionieren möchten und sich noch keinen traditionellen Vertrieb leisten können oder wollen.

Digitaler Vertrieb als Bedrohung

Nicht wenige Branchen nehmen digitalen Vertrieb heute aber als Gefahr wahr. Insbesondere *Markenartikelhersteller oder Hersteller von komplexeren Produkten* sehen v. a. aufgrund der daraus resultie-

renden Transparenz die Reputation und die korrekte Handhabung ihrer Produkte beeinträchtigt. Produktspezifischer, bisweilen auch beratungsintensiver (meist sog. selektiver) Verkauf über Fachhändler hat diesen Produkten in der Vergangenheit nicht nur eine gewisse Exklusivität garantiert, sondern über enge Händlerbindungen oft auch überdurchschnittliche Preise. Für den schweizerischen Kunden war und ist Letzteres von bisweilen schmerzhafter Relevanz: Die hohe inländische Kaufkraft veranlasst solche Hersteller noch heute häufig dazu, für solche Produkte in der Schweiz signifikant höhere Preise als im europäischen Ausland geltend zu machen.

Vertragliche Rahmenbedingungen

Jedenfalls soweit ein Hersteller kein eigenes Vertriebsnetz aufbauen will oder sich dies aus finanziellen und logistischen Gründen nicht leisten kann, ist er auf vertragliche Bindungen mit unabhängigen Partnern angewiesen. Er und seine Partner haben dabei die Wahl zwischen zahlreichen Möglichkeiten, sich gegenseitig mehr oder weniger umfangreiche Rechte und Pflichten zu gewähren bzw. aufzuerlegen. Die wichtigsten Klauseln betreffen: *Exklusivität, Wettbewerbsverbot, Mindestumsatzziele, Verkaufsbedingungen und Werbetätigkeiten,* wobei die letzten vier Bestimmungen (in der Regel zulasten des Distributors) das vertragliche Gegengewicht zur Exklusivität (in der Regel zugunsten des Distributors) bilden. Exklusivität bedeutet dabei in aller Regel räumliche Exklusivität. Dem Distributor wird also ein spezifisches Gebiet zugewiesen, das er ausschliesslich bearbeiten soll/darf. Ausschliesslichkeit bedeutet dabei, dass der Distributor im Vertragsgebiet nach Möglichkeit vor der Konkurrenzierung durch Vertragsprodukte geschützt wird.

Exklusivitätsabreden und Kartellrecht

Vereinbarungen zwischen voneinander unabhängigen Parteien, die den Wettbewerb beschränken, werden vom Kartellrecht erfasst. Je nach Wirkung auf den Wettbewerb können sie *unzulässig bzw. nichtig* sein und in besonders stossenden Fällen auch eine *Sanktionierung* der Vertragsparteien zur Folge haben. Als besonders unerwünscht werden sowohl im schweizerischen wie auch im europäischen Kartellrecht sog. absolute Gebietsschutzabreden gewürdigt. Konkret sind solche Exklusivitätsabreden nur dann zulässig, wenn der Distributor vor Direktvertrieb bzw. -marketing durch gebietsfremde Distributoren geschützt ist (sog. Aktivvertrieb), Lieferungen durch gebietsfremde Distributoren in sein Vertragsgebiet auf Anfrage hin aber dulden muss (sog. Passivvertrieb).

Kartellrecht fördert digitalen Vertrieb

Digitaler Vertrieb gilt seit geraumer Zeit sowohl in der Schweiz als auch in der EU als Passivvertrieb. Konkret bedeutet dies, dass der Hersteller/Lieferant seine *Distributoren nicht daran hindern darf, das Internet als Vertriebskanal zu benutzen.* Umgekehrt sind Distributoren berechtigt, eine Internetpräsenz aufzubauen und ihre Produkte über diesen Verkaufskanal ohne geografische Einschränkungen zu vertreiben. Interventionen von Kartellrechtsbehörden gegen vertragliche Beschränkungen des digitalen Vertriebs müssen somit (nebst anderem) als *Wegbereiter für diese Vertriebsart* gewürdigt werden. In der aktuelleren Fallpraxis wurden etwa folgende Klauseln zulasten des Distributors als unzulässig angesehen:

- Verbote, Markenzeichen auf Internetseiten Dritter zu verwenden.
- Verbote, Preisvergleichsmaschinen einzusetzen.
- Plattformverbote, d. h. die Untersagung des Vertriebs über Internetplattformen, die für den Kunden erkennbar oder nicht erkennbar von Dritten verwaltet werden.

Digitaler Vertrieb hat für den herkömmlichen Handel disruptive Wirkungen. Und dies gilt aufgrund der *Interventionsbereitschaft von Kartellbehörden* zunehmend auch für den (meist selektiven) Vertrieb von Markenartikeln und komplexeren Produkten. Aufgrund der Risiken tut sowohl lieferanten- wie distributorenseitig angemessene Rechtsberatung not.

12 Softwarebezogene Analysepatente: Ist das Patentieren von «Analytics»-Methoden erlaubt?

Sarah Zurmühle

Bereits zum sechsten Mal in Folge belegte die Schweiz im diesjährigen Global Innovation Index der World Intellectual Property Organization den ersten Platz. Sie gehört mit jährlichen Investitionen von knapp 20 Milliarden Euro im R&D-Bereich zusammen mit Schweden, dem Vereinigten Königreich und den USA zu den innovativsten Wirtschaften der Welt. Ein grosser Anteil dieser Investitionen erfolgt im Bereich der ICT-Technologien wie bspw. den softwarebezogenen Analysemethoden. Die Patentierbarkeit solcher Methoden ist in der Schweiz jedoch umstritten, schliesst bspw. das Europäische Patentübereinkommen sog. Programme für Datenverarbeitungsanlagen und Businessmethoden explizit von seinem Anwendungsbereich aus. Analysemethoden sind dennoch auch in der Schweiz patentierfähig, sofern der Erfinder eine minimale Technizität aufzeigt und die Innovation in einer konkreten, anwendbaren technischen Lehre beschreibt.

Was sind softwarebezogene Analysemethoden?

Softwarebezogene Analysemethoden dienen zur Untersuchung eines bestimmten Problems oder Sachverhalts und werden weder manuell noch maschinell, sondern mithilfe von Computern bedient. Diese Methoden können entweder rein digital ausgestaltet oder als Software in Hardwareprodukten implementiert sein. Besonders begehrt sind momentan computerimplementierte Analysemethoden im Bereich von Risikomanagement und Big Data Analytics.

«Erweiterter technischer Charakter» als massgebliche Voraussetzung

Das Schweizer Patentgesetz (PatG; SR 232.14) selbst macht weder eine Referenz zu Computerprogrammen und Geschäftsmethoden, noch stellt es explizit Voraussetzungen an die Technizität von Innovationen. Das Europäische Patentübereinkommen (EPÜ; SR 232.142.2) andererseits führt in Art. 52 Abs. 2 lit. c EPÜ sowohl Businessmethoden als auch Computerprogramme exemplarisch als «nicht erfinderisch» auf. Entgegen des ausdrücklichen Wortlautes des EPÜ erlauben aber sowohl das Europäische Patentamt als auch die beurteilenden Gerichte das Patentieren von Computerprogrammen und Businessmethoden, sofern die innovativen Verfahren und Erfindungsgegenstände über einen «zusätzlichen technischen Charakter» verfügen.

Was genau unter einem solch zusätzlichen technischen Charakter zu verstehen ist, hängt von einer Gesamtbetrachtung des Einzelfalls ab und kann an dieser Stelle nur summarisch umschrieben werden. Erwartet wird, dass eine Erfindung einen erweiterten technischen Beitrag leistet, welcher über die reine Anwendbarkeit auf einem technischen Gerät hinausgeht. Regelmässig ungenügend ist eine Erfindung dann, wenn sie zwar auf einem Computer einsetzbar ist, der Erfinder aber nicht aufzeigt, dass diese daneben noch eine weitere technische

Leistung erbringen oder einen nachweisbaren technischen Effekt bewirken kann. Ein Musterbeispiel hierfür sind in Quellcode verfasste Softwarebefehle, welche zwar auf einem Computer einsetzbar sind, überdies aber keine technische Qualifikation bieten. Den patentrechtlichen Anforderungen genügen also nur Erfindungen, welche aufgrund ihrer Aufgabenstellung, in der Art und Weise ihrer Problemlösung oder in ihrer funktionalen Wirkungsweise einen zusätzlichen technischen Charakter aufweisen. Unbestritten ist die Patentierbarkeit von softwarebezogenen Erfindungen, welche über eine maschinelle Komponente verfügen, also bspw. mit einem Hardware-Gerät verbunden oder darin implementiert sind. Auch Verfahren und Mittel zur Steuerung von mechanischen Anlagen und Netzwerken sind regelmässig patentierbar, so etwa im Bereich der Weichenstellung von Bahnanlagen oder in der Kontrolle von Energieträgern. Schwierig bleibt die Bewertung einer rein computerimplementierten Erfindung, wenn die erfinderische Leistung im Transferieren oder Verarbeiten von Datensignalen liegt, ohne dass ein kontrollierender oder steuernder Einfluss auf die Daten ausgeübt wird. Dies im Gegensatz zur Manipulation von Datensignalen, welche regelmässig einen technischen Effekt bewirken und folglich ihre zusätzliche Technizität erkennbar zum Ausdruck bringen. Die in der Schweiz patenterteilende Behörde, das Institut für Geistiges Eigentum, erachtete bspw. ein Computersystem zur Verwaltung von digitalen Benutzungsrechten nicht als patentierbar, während sie ein Verfahren zur Kontrolle der Qualität von digitalen Farbbildaufzeichnungen zuliess.

Keine abstrakte Umschreibung der technischen Lehre

Überdies ist es für jede Patentanmeldung erforderlich, die technische Lehre, welche zur Lösung eines bestimmten Problems verwendet wird, verständlich darzulegen. Die entsprechende technische Lehre darf nicht abstrakt umschrieben werden, da das Patentrecht keine abstrakten, generischen Verfahrensmethoden schützt. Experten aus dem Fachgebiet der beanspruchten Erfindung müssen imstande sein, eine Erfindung aufgrund des Beschriebs der technischen Lehre umzusetzen. Analysemethoden, welche ohne Nennung einer konkreten Anwendungsmöglichkeit nur ein Verfahren beschreiben, genügen diesen Anforderungen regelmässig nicht.

Analysepatente also auch im Softwarebereich patentierbar

Das Schweizer Patentrecht orientiert sich folglich weitgehend an der europäischen Interpretation von softwarebezogenen Erfindungen. Die patenterteilende Behörde hat faktisch zwei weitere Schutzvoraussetzungen geschaffen, welche bei der Bewertung von computerimplementierten Erfindungen und Geschäftsmethoden zu berücksichtigen sind. Analysemethoden, welche zu ihrer Umsetzung Computer benötigen, sind entgegen des ausdrücklichen Wortlautes des Europäischen Patentübereinkommens also dennoch patentierbar, sofern sie 1) einen zusätzlichen technischen Charakter aufzeigen und 2) die zur Anwendung kommende technische Lehre konkrete Anwendungsmöglichkeiten benennt. Trotz erhöhter Hürden sind also auch softwarebezogene Analysemethoden dem Patentschutz zugänglich.

13 Werbeblocker: Gibt es ein Recht auf werbelosen Medienkonsum?

Katharina Henz

Werbeblocker erfreuen sich bei Nutzern immer grösserer Beliebtheit. Damit stellen sie Medienanbieter sowie die Werbeindustrie vor grosse Herausforderungen. In Rechtsprechung und Praxis stellen sich Fragen nach dem Umgang mit dem sogenannten «Adblocking». Eine Schweizer Rechtsprechung dazu gibt es bisher nicht, jedoch haben deutsche Gerichte entschieden, dass Werbeblocker grundsätzlich rechtmässig sind. Ein deutsches Landesgericht hat sich allerdings dieses Jahr gegen die «Whitelist»-Funktion ausgesprochen, mittels derer sich Unternehmen vom Adblocking freikaufen können. Es bleibt abzuwarten, ob hierzulande bald ähnliche Urteile fallen oder ob sich die Schweizer Gerichte «werbefreundlicher» zeigen.

Was sind Werbeblocker?

Werbeblocker sind ein immer weiter verbreitetes Phänomen mit grossen Auswirkungen auf die Werbeindustrie. Es handelt sich dabei um im Hintergrund ablaufende Filterprogramme, mit denen auf Webseiten enthaltene Werbeanzeigen ausgefiltert werden, sodass sie für den Nutzer nicht mehr sichtbar sind. Neben Webseiten werden Werbeblocker auch bei Fernsehern eingesetzt. Einerseits gibt es Werbeblocker, die für die Dauer der Werbepause auf ein anderes (von Werbung freies) Programm umschalten oder aber den Fernseher ganz abschalten, andererseits gibt es solche, die bei der Video-Aufzeichnung Werbeanzeigen herausfiltern.

Werbeblocker filtern inzwischen nicht mehr jegliche Werbung heraus, sondern erstellen sogenannte weisse Listen für Werbeeinblendungen, die als unaufdringlich bewertet werden («acceptable ads»), auf die sich Webseiten teilweise kostenpflichtig eintragen lassen können, wenn sie Kriterien wie Platzierung oder Grösse erfüllen. In der Folge werden Werbeeinblendungen auf diesen Webseiten nicht blockiert. Der deutsche Online-Werbeblocker «Adblock Plus» geht inzwischen sogar noch einen Schritt weiter und zeigt dort, wo der Webseiten-Betreiber vorher Werbung eingeblendet hat, ersatzweise Anzeigen, an denen Adblock Plus sich selber einen Werbeerlös sichert.

Übersicht über die bisherige Rechtsprechung zu Werbeblockern

In der Schweiz fehlen bisher einschlägige (publizierte) Urteile zur Zulässigkeit von Werbeblockern. Verschiedene deutsche Gerichte haben jedoch bereits Entscheide zum Thema gefällt, die sich zwar nicht direkt auf die Schweiz übertragen lassen, denen aber für die Schweizer Praxis Anhaltspunkte entnommen werden können.

Sowohl der deutsche Bundesgerichtshof (BGH) als auch verschiedene deutsche Landgerichte haben bereits zugunsten von TV- sowie Online-Werbeblockern entschieden, dass die Bewerbung und der Vertrieb von Werbeblockern nicht als wettbewerbswidriges Verhalten i.S. des deutschen UWG anzusehen sei (Urteil des BHG v. 24.06.2004, Az.: I ZR 26/02). Grundlage der Klagen war jeweils das deutsche UWG und die daraus abgeleiteten Verbote der produktbezogenen Behinderung, der Werbebehinderung sowie der unzulässigen allgemeinen Marktbehinderung. Nach Ansicht der Gerichte besteht zwischen einem Fernsehunternehmen bzw. einer Webseite und einem Werbeblocker zwar ein konkretes Wettbewerbsverhältnis, jedoch stelle der Werbeblocker lediglich eine technische Hilfe zur Verfügung und die Entscheidung zur «Umgehung» liege bei den Nutzern. Die Werbung erreiche nur diejenigen Nutzer nicht, die sich bewusst dafür entschieden hätten, keine Werbung sehen zu wollen und die geschäftliche Tätigkeit der Unternehmen sei durch die Werbeblocker nicht existenziell bedroht. Es liege auch keine gezielte Behinderung i. S. einer Verdrängungsabsicht vor.

Das Oberlandesgericht Köln entschied im Juni diesen Jahres, dass Adblocking zwar rechtmässig sei, da letztlich der Nutzer über das Blockieren von Werbung entscheide, nicht jedoch die Whitelist-Funktion (Urteil des OLG Köln v. 24.06.2016, Az.: 6 U 149/15). Diese sei wettbewerbswidrig, weil die Werbung beim Betrieb des Werbeblockers nur bei der Einhaltung vorgegebener Kriterien und gegen Zahlung eines Entgelts nicht unterdrückt werde, denn es handle sich dabei um eine «aggressive geschäftliche Handlung […], die geeignet ist, den Verbraucher oder sonstigen Marktteilnehmer zu einer geschäftlichen Entscheidung zu veranlassen, die dieser andernfalls nicht getroffen hätte». Adblock Plus darf in Deutschland kein Entgelt mehr für die Aufnahme von «acceptable ads» auf die Whitelist erheben, sofern dies Webseiten der Klägerin Axel Springer AG betrifft. Das Urteil wurde an den BGH weitergezogen.

Reaktionen auf Werbeblocker in der Praxis

Von Werbeblockern betroffene Unternehmen haben unterschiedlich auf diese reagiert. Für grössere Unternehmen besteht die Möglichkeit, sich gegen eine Gebühr «freizukaufen», sodass als «akzeptabel» eingestufte Werbeanzeigen trotz aktiviertem Werbeblocker (in der Standardeinstellung) angezeigt werden. Google, Microsoft und Amazon haben entsprechende Abkommen mit Eyeo, dem Hersteller von Adblock Plus, abgeschlossen. Kleinere Unternehmen müssen kein Entgelt bezahlen für die Aufnahme in die Whitelist – welche Unternehmen dafür zahlen müssen und welche nicht, dazu äussert sich Eyeo aber nicht. Gemäss Eyeo muss allerdings jedes Unternehmen dieselben Kriterien hinsichtlich Werbung erfüllen, unabhängig davon ob zahlend oder nicht zahlend.

Facebook hat Anfang August diesen Jahres bekannt gegeben, dass es künftig selbstständig gegen das Unterdrücken von Werbeanzeigen vorgehen werde. Man werde auch denjenigen Nutzern, die einen Werbeblocker installiert haben, Werbeanzeigen zeigen. Eine weitere Möglichkeit besteht für Betreiber von Webseiten darin, sogenannte «Anti-Adblocker» zu verwenden und damit Nutzer, die einen Adblocker installiert haben, zu sperren.

Kommentar und Fazit

Die deutsche Rechtsprechung bejaht die Frage, ob ein Recht auf werbelosen Medienkonsum bestehe. Es könne keine gezielte Behinderung der Provider festgestellt werden und es gebe auch kein faktisches Vertragsverhältnis, welches den Leser verpflichte, sich Werbung anzuschauen. Dem lässt sich entgegnen, dass Leser mit dem Konsum von Medien wie Webseiten eine kostenfreie Leistung beziehen, die sie mit Werbung, die ihnen auf Webseiten angezeigt wird, gewissermassen bezahlen. Werden die Werbeanzeigen ausgeblendet, so bedroht das die wirtschaftliche Existenz von Providern.

Benutzer-Umfragen zeigen, dass die Konsumenten keine Werbeeinblendungen sehen möchten, die für sie irrelevant sind oder die ihr Online-Erlebnis beeinträchtigen. Zudem möchten sie einen Einfluss darauf haben, welche Art von Werbung ihnen gezeigt wird. Die Betreiber können folglich mit der Art der Werbung, die sie ihren Nutzern zeigen, deren Erlebnis beim Konsum der Medien beeinflussen und sie können dafür sorgen, dass diese sich gar nicht veranlasst sehen, einen Werbeblocker einzusetzen. Eine weitere Möglichkeit bestände darin, eine «werbefreie Option» kostenpflichtig anzubieten.

Werbeblocker bieten den Benutzern eine Dienstleistung an, die diese erst deshalb beanspruchen, weil sie mit der Dienstleistung der Betreiber so nicht zufrieden sind. Diese haben es in der Hand, ihr Angebot entsprechend anzupassen.

E-Finance

14 FinTech – InsurTech – RegTech

Dr. Jana Essebier

Angela Oppliger

Neue Begriffe prägen die Diskussion über den Finanzmarkt. Immer häufiger hört man Ausdrücke wie FinTech, InsurTech und RegTech. Die Rede ist von der digitalen Revolution im Finanzsektor. Auch der Bundesrat hat sich bereits mit FinTech befasst. Am 20. April 2016 beauftragte er das Eidgenössische Finanzdepartment (EFD) mit der Prüfung, ob eine Anpassung der regulatorischen Rahmenbedingungen notwendig wird, um die Markteintrittsschranken im Bereich FinTech zu senken. Zudem hat der Nationalrat am 22. September 2016 ein Postulat seiner Wirtschaftskommission angenommen, welches eine Verbesserung der Wettbewerbsfähigkeit des Finanzplatzes bei neuen Finanztechnologien anstrebt. Aber worum geht es eigentlich? Läuft die Schweiz Gefahr, den Anschluss zu verpassen?

FinTech

FinTech steht für die Verbindung von Finanzdienstleistungen und Technologie. Der Begriff wird für Produkte und Dienstleistungen verwendet, welche durch neue Technologien die Erbringung von Finanzdienstleistungen verändern oder erleichtern. Er umfasst innovative Applikationen, Software etc., welche die Digitalisierung im Bereich von Finanzdienstleistungen vorantreiben, global stark vernetzt und rund um die Uhr verfügbar sind. Dies führt zu einer schnelleren und effizienteren Abwicklung von Transaktionen. Zurzeit werden FinTechs vor allem im Bereich Robo-Advice (Anlageempfehlungen, die durch automatisierte Analyseprozesse generiert werden) sowie mobiler Bezahlung, Blockchain-Technologie (ein virtuelles öffentliches Verzeichnis, das von einem Netzwerk von Computern unterhalten und unverändert abgespeichert wird) und automatisierten Kreditentscheiden aufgebaut.

InsurTech

InsurTech setzt sich aus Insurance, d. h. aus Versicherungen, und Technologie zusammen. Es handelt sich um einen Teilbereich von FinTech-Produkten, der sich spezifisch mit Versicherungen befasst. Ziel der neu entwickelten Applikationen ist es, alle Bereiche rund um das Thema Versicherungen zu zentralisieren und so eine bessere Übersicht zu schaffen. Bisher sind im Markt vor allem Start-ups aktiv, die Versicherungen vermitteln und die Kunden bei der Verwaltung dieser Versicherungen unterstützen.

RegTech

RegTech steht für die Kombination von Regulierung und Technologie. Dabei werden neue Technologien entwickelt, um es Unternehmen, insbesondere auch Finanzdienstleistern, zu erleichtern, regulatorische Anforderungen zu überprüfen und einzuhalten. RegTech-Applikationen sollen die Effektivität und Effizienz im Bereich der Regulierung steigern. Daher ist RegTech ein wichtiges Hilfsmittel in der Compliance und trägt zu deren Automatisierung bei. Die Entwicklung von RegTech-Applikationen und die damit einhergehende Digitalisierung fördern ebenso die Transparenz in Regulierungsfragen. RegTech-Innovationen erleichtern insbesondere das Datenmanagement von Finanzdienstleistern und die regulatorische Berichterstattung an die zuständige Behörde.

Bewilligung oder Registrierung gemäss Finanzmarktgesetzen

Häufig erbringen diese Unternehmen Dienstleistungen oder entwickeln Technologien, ohne selbst den Finanzmarktgesetzen zu unterstehen. Dies ist jedoch im Einzelfall zu prüfen. Als Grundregel gilt Folgendes:

- Wer fremde Gelder von einem Konto auf ein anderes transferiert oder Versicherungen vermittelt, muss die notwendigen Registrierungen als Finanzintermediär nach dem Geldwäschereigesetz oder als Versicherungsvermittler im Blick behalten.
- Unternehmen, welche Gelder entgegennehmen, sollten vor der Aufnahme der Geschäftstätigkeit prüfen, ob sie eine Bewilligung benötigen oder ob sie sich auf eine Ausnahme stützen können.
- Wer beabsichtigt, Risiken anderer Personen zu versichern, sollte vorab prüfen, ob eine Bewilligung nach dem Versicherungsaufsichtsgesetz erforderlich ist.

Regulierung bremst Entwicklung in der Schweiz

Die Registrierung als Finanzintermediär oder Versicherungsvermittler ist in der Regel auch für kleinere Unternehmen möglich, jedoch stellt der administrative Aufwand operationelle Anforderungen. Zudem hat sie Auswirkungen auf die erzielte Marge.

Anders ist dies, wenn eine Bankenbewilligung notwendig wäre. Findet keine Ausnahme Anwendung, dann muss das Unternehmen prüfen, ob und zu welchen Kosten die Tätigkeit mit Unterstützung von Banken ausgeübt werden kann. Ist dies nicht oder nicht zu vertretbaren Kosten möglich, muss das Geschäftsmodell angepasst werden. Ein Antrag auf Erteilung einer Bankenbewilligung ist in der Regel keine Alternative, da der Aufwand und damit die Kosten sehr hoch sind. In diesem Bereich ist das Schweizer Recht im Vergleich zum Recht in vielen anderen Staaten weiterhin relativ restriktiv. Dies kann dazu führen, dass Geschäftsmodelle nicht oder jedenfalls nicht in der Schweiz umgesetzt werden. Die Entwicklung im Bereich FinTech wird damit gebremst.

Bankenlizenz Light als Ausweg

Als Ausweg wird eine neue Bewilligungskategorie diskutiert. Diese steht unter dem Titel «Bankenlizenz Light». Noch hat das EFD jedoch keine entsprechenden Vorschläge publiziert. Die Eigenkapital- und sonstigen Anforderungen müssten indessen erheblich tiefer als bei der gegenwärtigen Bankenbewilligung sein, damit diese Variante überhaupt als Alternative für kleinere Unternehmen in Betracht kommt. Für viele Start-up-Unternehmen dürfte wohl nur eine Ausweitung der Ausnahmen vom Einlagenbegriff und damit vom Anwendungsbereich des Bankengesetzes den für das Geschäftsmodell notwendigen Entwicklungsspielraum schaffen.

Die Schweiz steht unter Zeitdruck

Es bleibt zu hoffen, dass diese Vorschläge bald publiziert und Erleichterungen für FinTech zeitnah umgesetzt werden. Anderenfalls besteht das Risiko, dass ausländische Anbieter den Schweizer Markt erobern, bevor sich Schweizer FinTechs entfalten können. In der Zwischenzeit profitieren ausländische Anbieter davon, dass das Schweizer Recht üblicherweise die grenzüberschreitende Ttigkeit ausländischer Anbieter weniger streng reguliert als die vergleichbare Tätigkeit von Schweizer Anbietern.

15 Crowdfunding als Finanzierungsquelle für Schweizer Start-ups


Dr. Stefan Grieder


Dr. Jana Essebier


Florian Fuhrimann

Crowdfunding kann eine alternative Finanzierungsquelle für Start-up-Unternehmen sein. Noch bremst das Schweizer Bankengesetz die Entwicklung, jedoch zeichnet sich der Abbau von Hürden am Horizont ab.

Was ist Crowdfunding?

Die Digitalisierung und das Internet haben die Gemeinschaftsfinanzierung zu einem Massenphänomen werden lassen. Beinahe jeden Tag kann man von einem Projekt lesen, welches durch Crowdfunding finanziert wird. Als Crowdfunding (auch Schwarmfinanzierung) werden Formen der Finanzierung über Internetplattformen mithilfe einer Vielzahl von Investoren bezeichnet. Dabei investieren die einzelnen Investoren häufig jeweils vergleichsweise geringe Beträge. Etabliert hat sich Crowdfunding vor allem im kulturellen Bereich und bei der Finanzierung von Start-up-Unternehmen.

Crowdfunding nimmt unterschiedliche Formen an. Das gemeinsame Kennzeichen aller Formen des Crowdfunding ist, dass keine Bank in die Finanzierung einbezogen wird, sondern vielmehr die Investoren und Kapitalnehmer über das Internet direkt miteinander in Kontakt treten. Im Grundsatz können folgende vier Finanzierungsformen unterschieden werden:

- Crowddonating (Unterstützung via Spenden);
- Crowdsupporting (Unterstützung durch Sponsoring, d. h. Erhalt von Sachgegenleistungen wie CDs, Konzerttickets, personalisierten Produkten etc.);
- Crowdinvesting (zur Verfügung stellen von Eigenkapital);
- Crowdlending (zur Verfügung stellen von Fremdkapital).

Verbreitung und Bedeutung in der Schweiz

Der Crowdfunding-Markt in der Schweiz ist in den letzten Jahren rasant gewachsen. Gemäss dem von der Hochschule Luzern publizierten «Crowdfunding-Monitoring 2016» hat sich das Volumen der vermittelten Gelder seit 2011 fast verneunfacht und betrug im Jahr 2015 rund 27.3 Millionen CHF. Die eindrücklichen Wachstumszahlen dürfen jedoch nicht darüber hinwegtäuschen, dass die absoluten Beträge weiterhin sehr tief sind.

Plattformen für Crowdsupporting wie z. B. www.100-days.net und www.wemakeit.com sind in der Schweiz bereits seit Jahren etabliert. Spendenplattformen erleben in neuerer Zeit einen Aufschwung. So ist z. B. die Raiffeisengruppe mit www.lokalhelden.ch in diesem Bereich aktiv geworden. Hingegen steckt das eigentliche Crowdlending in der Schweiz immer noch in den Kinderschuhen.

Bankengesetz als Hürde

Dass die Volumina der Schweizer Crowdlending-Plattformen im internationalen Vergleich noch gering sind, ist nicht nur den kleineren Marktverhältnissen geschuldet, sondern auch eine direkte Folge der Finanzmarktregulierung in der Schweiz. Als Hürde erweist sich dabei insbesondere das Bankengesetz.

Wer Darlehen von mehr als 20 Darlehensgebern entgegennimmt, ohne einen Prospekt erstellt zu haben, macht sich strafbar. Da das Erstellen eines Prospekts erhebliche Kosten verursacht, ist dies gerade für Privatpersonen und kleinere Unternehmen keine Option. Die typische Finanzierung durch eine Vielzahl von Personen – der Crowd – ist somit gerade nicht zulässig.

Auch die Plattformbetreiber sind mit dem Bankengesetz konfrontiert: Bei der Entgegennahme der Gelder aus der Crowd zwecks Weiterleitung an die Projektinitianten stellt sich die Frage, wann die Schwelle der bewilligungsfreien Tätigkeit überschritten wird. Weiter sind in diesem Zusammenhang auch steuerliche Aspekte zu berücksichtigen.

Politik hat Handlungsbedarf erkannt

Positiv ist festzuhalten, dass die Politik den Handlungsbedarf erkannt hat.

Am 20. April 2016 gab der Bundesrat im Rahmen einer Stellungnahme bekannt, dass er das Eidgenössische Finanzdepartement (EFD) beauftragt habe, den regulatorischen Handlungsbedarf im Bereich innovativer Finanztechnologien zu prüfen. Gleichzeitig machte er auf einen Beschluss aufmerksam, wonach FinTech-Unternehmen unter folgenden Voraussetzungen von der Bankenverordnung ausgenommen werden können: Sie dürfen 1) Gelder allein zum Zweck der Weiterleitung entgegennehmen, 2) keinen Zins dafür verlangen und 3) die Abwicklung solcher Gelder muss vorgängig bestimmt sein. Diese Ausnahme ist insbesondere für Plattformbetreiber von grosser Bedeutung.

Die Zeitspanne, innert welcher die Gelder nun weitergeleitet werden müssen, um unter den Ausnahmetatbestand zu fallen, ist damit jedoch noch nicht bestimmt. Die Rechtsunsicherheit in diesem Bereich dauert daher fort.

Laut der Stellungnahme des Bundesrates vom 17. August 2016 zur Motion 16.3472 im Schweizer Parlament sollen die Ergebnisse der Prüfung des EFD im Herbst 2016 vorliegen. Es dürfte wohl Anfang 2017 werden, bis konkrete Vorschläge für eine Änderung der Regulierung publiziert werden.

Abschaffung der 20er-Regel

Besonderes Augenmerk sollte der Abschaffung der 20er-Regel gelten.

Crowdlending wird erst dann eine ernst zu nehmende Alternative sein, wenn diese Einschränkung dahinfällt und tatsächlich die «Crowd» als Darlehensgeberin zur Verfügung steht.

Die regulierungsbedingten Kosten müssen auf das notwendige Mass gesenkt werden. Der Gesetzgeber sollte sich daher folgende Fragen stellen:

- Wie risikofähig ist der durchschnittliche Anleger in der Schweiz? In welchem Umfang ist Anlegerschutz daher tatsächlich nötig?
- Wie kann der Anlegerschutz verwirklicht werden, ohne dass die daraus resultierenden Kosten das Geschäftsmodell von vornherein unrentabel machen?
- Wie kann der technische Fortschritt dabei helfen?

De-Minimis-Ausnahmen als Lösung

Möglich wäre beispielsweise die Anhebung der Anzahl von Darlehensgebern von 20 auf 150. Denkbar wäre auch die Schaffung von Ausnahmen für geringe Darlehensvolumina, z. B. wenn ein Unternehmen ein Darlehen im Gesamtbetrag bis zu 500 000 CHF aufnimmt oder die Darlehenssumme pro Darlehensnehmer einen bestimmten Höchstbetrag wie z. B. 10 000 CHF nicht übersteigt.

Anstelle des Prospektes, den die Anleger ohnehin nur selten lesen, könnten die Plattformen zudem verpflichtet werden, bei jedem Log-in eines Anlegers auf die fehlende Regulierung und die Risiken aufmerksam zu machen.

16 Mobile Payment

Dr. Rolf Auf der Maur

Dr. Jana Essebier

Umbruch des Zahlungswesens oder nur ein Hype?

Warum haben sich Zahlungen per Mobiltelefon in Afrika rasant verbreitet, während der Umbruch in der Schweiz zaghaft voranschreitet? Stehen bei uns regulatorische Hürden und eine Überversorgung mit traditionellen Zahlungsoptionen den neuen Technologien im Wege? Eines ist jedenfalls klar: Obwohl noch wenig verbreitet, gibt Mobile Payment auch in der Schweiz viel zu reden.

Sind uns Entwicklungsländer voraus?

In Entwicklungsländern hat bisher nur ein kleiner Teil der Bevölkerung Zugang zu Bankdienstleistungen. Hingegen verfügt fast jedermann auch in abgelegenen Landstrichen über ein Mobiltelefon. Mobilfunkbetreiber haben schon vor zehn Jahren die Chance erkannt und sind in die Bresche gesprungen: Mit dem von Vodafone/Safaricom betriebenen Dienst M-PESA lassen sich per SMS von Abonnent zu Abonnent Beträge überweisen, die bei Agenten des Betreibers in Bargeld umgetauscht werden können. Das Modell basiert auf Vorauszahlung und war ursprünglich keinerlei Regulierung unterworfen. Inzwischen verfügt Vodafon/Safaricom für M-PESA zwar über eine Lizenz der Zentralbank im jeweiligen Land, doch gelten dabei weniger strenge Regulierungen als für Banken.

Wettstreit um Standards und Schnittstellen

Ganz anders ist das Bild in Europa und insbesondere in der Schweiz: Hier verfügt jedermann über ein Bankkonto oder zumindest über ein Zahlungskonto bei der Post. Kredit- und Debit-Karten haben breite Akzeptanz gefunden. Das dominierende Zahlungsmittel im Detailhandel bleibt bisher allerdings Bargeld, denn es lässt sich im dichten Netz von Bankomaten jederzeit beschaffen und gewährleistet Anonymität. Banken und Herausgeber von Kreditkarten haben in diesem Marktumfeld den Zahlungsverkehr unter Kontrolle und verdienen mit Gebühren aufseiten der Händler und Kunden gutes Geld. Diese Marktposition wollen sie auch beim Mobile Payment nicht an Telekommunikationsunternehmen oder Technologieunternehmen verlieren. Seit mit dem Markteintritt von Apple Pay zu rechnen war, ist Bewegung in den Markt gekommen. Die Marktteilnehmer stecken ihre Territorien ab: Twint und Paymit fusionieren ihre Angebote mit Wirkung ab Anfang 2017. Mit Swiss Wallet steht eine Lösung in den Startlöchern, die technisch ähnlich funktioniert wie Apple Pay.

Grundlegend neu sind die bei uns gebräuchlichen Mobile-Payment-Systeme allerdings nicht: Sämtliche Angebote basieren auf einer Kontobeziehung mit einer Bank (Debit Systeme) oder auf einer Kreditkarte innerhalb der bei dieser hinterlegten Limite. Die Innovation beschränkt sich auf die Art des Informationsaustausches zwischen dem Smartphone des Nutzers und dem Terminal des Händlers. Dies ist zwar auch auf regulatorische Hindernisse, wie dem Fehlen einer sogenannten Bankenlizenz Light für Zahlungsdienstleister, zurückzuführen. Wesentlicher dürften jedoch das Vertrauen sein, welches die traditionellen Anbieter geniessen, und Zweifel der Kunden an der Sicherheit bei neuen Lösungen. Ausserdem haben auch die traditionellen Anbieter das Bedürfnis der Kunden nach einfach zu bedienenden Lösungen erkannt. So bietet etwa Mastercard mit Masterpass eine tokenbasierte Online Zahlungsoption, die ohne die umständliche (und unsichere) Eingabe der Kartennummer auskommt und als Antwort auf Paypal zu verstehen ist.

Der drahtlose Informationsaustausch bei Mobile Payment erfolgt entweder über den offenen und weitverbreiteten Bluetooth-Standard (Twint) oder – bei neueren Geräten – über den Near-Field-Com-

munication-Standard (Apple Pay und Android Pay). Entscheidend ist, ob ein Zahlungsdiensteanbieter Zugriff auf diese Kommunikationsschnittstellen hat und ob er über Schnittstellen für die Kommunikation mit einer genügend grossen Anzahl von Zahlungsterminals verfügt. Andernfalls muss er sich einem Anbieter anschliessen, der Zugang zu diesen Schnittstellen hat. So lässt beispielsweise Apple den Zugriff auf die in iPhones integrierten NFC-Schnittstellen nur über ihr eigenes Wallet zu. Anbieter anderer Wallets (beispielsweise das vor der Lancierung stehende Swiss Wallet) können sich entweder auf Geräte mit anderen Betriebssystemen (insbesondere das von Google betriebene offene System Android) beschränken oder aber ihr Wallet unter dasjenige von Apple legen und ihre Transaktionen indirekt mit dem Terminal des Händlers abwickeln.

alle möglichen Objekte der sogenannten «Sharing Economy»). Auch Kundenbindungsprogramme haben damit begonnen, sich die neuen Möglichkeiten zunutze zu machen.

Entscheidend wird die Frage sein, welcher der involvierten Dienstleister (Händler, Terminalbetreiber, Issuer einer Kreditkarte, Bank oder Betreiber eines Wallet) am Ende über welche Daten verfügt und was er damit aus regulatorischer Sicht anstellen kann. Nur wer die Bedürfnisse des Kunden kennt, kann diesem längerfristig relevante Dienstleistungen bieten und von einem entsprechenden Wettbewerbsvorteil profitieren. Die Fülle der im Smartphone zusammenlaufenden Informationen stellt überdies ein wachsendes Sicherheitsrisiko dar.

Kundendaten als Wettbewerbsfaktor

Ist ein Wallet auf dem Smartphone einmal installiert, lassen sich Zahlungen durch einfachen Fingerabdruck auf dem Home Button autorisieren und ausführen. Die im Gerät hinterlegten und im Wallet konfigurierten Karten kann der Nutzer zuhause lassen. Dieser Zuwachs an Bedienungsfreundlichkeit ist gegenwärtig der entscheidende Vorteil von Mobile Payment. Darüber hinaus ermöglichen die neuen Mobile-Payment-Systeme erleichterte Zahlungen von Privatperson zu Privatperson. Ob diese Vorteile für den Siegeszug von Mobile Payment ausreichen, wird sich weisen. Allerdings dürfte die Entwicklung nicht stehen bleiben. So lassen sich auf der Kombination von Smartphone und Zahlungsdienst etwa neue automatisierte Zugangssysteme entwickeln (etwa für Hotels, Mietwohnungen, Veranstaltungen, den öffentlichen Verkehr oder

Beim Umgang mit Daten zeichnen sich bereits unterschiedliche Philosophien ab: Apple verzichtet auf die Übermittlung der Informationen zum Warenkorb, den ein Kunde erworben hat. Bei Android Pay hingegen ist vorgesehen, dass Google als Betreiberin des Systems die Informationen zum Warenkorb bekommt und auswerten kann. Für alle involvierten Dienstleister stellt sich daher die Frage, inwieweit sie kooperieren wollen und müssen.

Eine wichtige Rolle wird dabei neben dem Wettbewerbsrecht auch das Datenschutzrecht spielen. In der EU werden die Anforderungen mit Wirkung ab 2018 verschärft. Auch in der Schweiz steht eine Totalrevision des Datenschutzgesetzes an. Der Wettbewerb um die Daten der Kunden wird spannend bleiben.

17 Wie sicher sind meine mobilen Finanzdaten?

Christian Wyss, LL.M.

Führende Anbieter von mobilen Finanz-Apps sorgen für ein gutes Sicherheitsniveau. Die grössten Risiken sind nicht Sicherheitslücken im System, sondern Unachtsamkeit und Fehler beim Benutzen mobiler Finanzapplikationen. Trotzdem besteht auch für erfahrene und vorsichtige Nutzer von Finanz-Apps eine gewisse Gefahr eines unerwünschten Zugriffs. Die strenger werdende Datenschutzgesetzgebung wird helfen, diese Gefahr zu verringern.

FinTech: Neue Möglichkeiten für Anbieter und Kunden, aber auch für Kriminelle

Die Digitalisierung und neue technologische Innovationen verändern unseren Alltag. Neue Lösungen von etablierten Banken und neuen FinTech-Anbietern ermöglichen dem Kunden, jederzeit auf Finanzdaten zuzugreifen, Finanztransaktionen mühelos durchzuführen und einen besseren Überblick zu gewinnen.

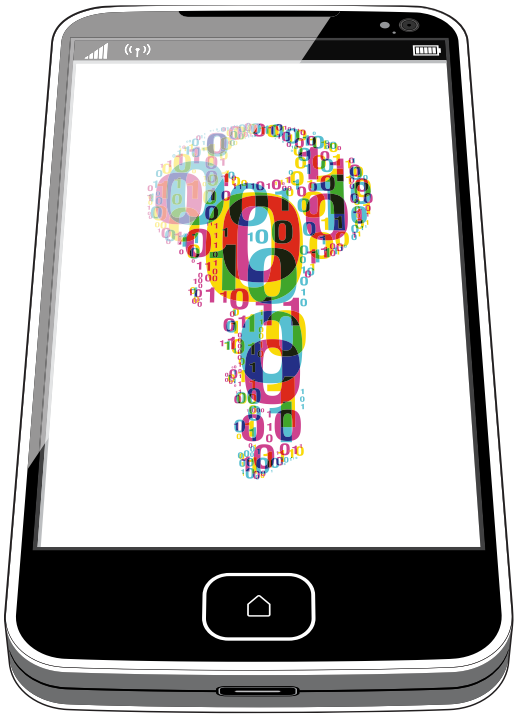
Gutes Sicherheitsniveau

Das Bankgeheimnis, die Finanzmarktregulierung mit den Vorgaben der FINMA und die in der Datenschutzgesetzgebung geforderten technischen und organisatorischen Massnahmen zur Verhinderung eines unbefugten Zugriffs haben zu einem hohen Stand der Datensicherheit geführt. Die so etablierten Qualitätsstandards gelten auch für Schweizer Anbieter mobiler Finanzdienstleistungen. Die FINMA hat in den letzten Jahren gezielte Zusatzprüfungen zum Thema IT-Sicherheit durchgeführt. Die FINMA ist zudem dabei, das für den Bereich der IT-Sicherheit wesentliche Rundschreiben 2008/7 Outsourcing Banken zu überarbeiten und auf Versicherungen auszuweiten. Nicht zu vergessen ist schliesslich auch, dass mit E-Banking die früher oft vorkommende Manipulation von aus Briefeinwürfen entwendeten schriftlichen Zahlungsaufträgen ein Ende gefunden hat.

Finanz-Apps: Das sind die Risiken

Das Verwenden von Finanz-Apps auf mobilen Geräten birgt jedoch auch einige spezifische Risiken:

- Die Anbieter von Finanz-Apps sind auf Plattformen wie Apple AppStore, GooglePlay oder den Windows-Store angewiesen. Auf jeder Plattform gelten unterschiedliche Nutzungsbedingungen, die sich je nach Land unterscheiden.
- Das Logo der Hausbank prangt jetzt stolz auf dem Homescreen des Mobiltelefons. Auf Desktop oder Laptop wurde den Kunden zuvor während Jahren eingeschärft, nach dem E-Banking die temporären Internetdateien



und damit die Spuren einer Bankbeziehung zu löschen.
- Mobile Geräte gehen aufgrund ihrer geringen Grösse eher verloren oder werden gestohlen. Sind diese schlecht gesichert, können Dritte Zugang auf die Finanz-App erhalten.
- Finanz-Apps sind eine interessante Zielscheibe: Je beliebter eine App und je sensibler die Daten, desto mehr lohnt sich der Versuch, unbefugt ins System einzudringen.

Daneben gibt es eine Reihe von Risiken, die sich durch vorsichtiges Verhalten der Nutzer vermindern lassen:
- Betrügerische Apps können sich als offizielle Angebote von Finanzdienstleistern tarnen und so Zugangsdaten ausspähen. Vor allem in alternativen App Stores tauchen ab und zu betrügerische Apps auf.
- Viele Nachrichten werden auf dem Mobiltelefon auch bei gesperrtem Bildschirm als Vorschau angezeigt. Wer eine Finanz-App nutzt und zum Beispiel mTAN-Codes per SMS empfängt, sollte diese Einstellung ändern.
- Fehlende oder einfach zu erratende Passwörter machen es Kriminellen einfach, ein mobiles Gerät zu missbrauchen.
- Heute ist offen, welche digitalen Dienstleistungen und Geschäftsmodelle sich mittelfristig durchsetzen werden. Viele Nutzer probieren neue Apps aus. Wichtig ist zu verhindern, dass in nicht mehr genutzten Apps und mobilen Geräten Datenfriedhöfe zurückbleiben, über die der Nutzer keine Kontrolle mehr hat.

Neues Datenschutzrecht fördert Transparenz und Sicherheit

Gemäss der im Mai 2018 in Kraft tretenden EU-Datenschutz-Grundverordnung müssen Anbieter von Finanz-Apps unbefugte Zugriffe auf personenbezogene Daten umgehend an die zuständige Datenschutzaufsichtsbehörde melden. Die EU verlangt zudem eine Benachrichtigung der Betroffenen, wenn voraussichtlich ein hohes Risiko für deren Rechte und Freiheiten besteht. Es ist davon auszugehen, dass der Vorentwurf des revidierten Schweizer Datenschutzgesetzes analoge Pflichten zur Meldung und Mitteilung von Datenschutzverletzungen enthalten wird. Bisher war die Finanzbranche mit Informationen über sicherheitsrelevante Vorfälle im Bereich E-Banking und Mobile Banking eher zurückhaltend, um ihre Kunden nicht zu verunsichern. Informationen über solche Vorfälle sind aber entscheidend, weil Hacker die erbeuteten Daten auch dazu verwenden, zukünftige Angriffe zielgerichteter und effizienter durchzuführen. Gesteigerte Transparenz in diesem Bereich wird der Informatiksicherheitsbranche erlauben, Lücken rascher zu schliessen und den allgemeinen Sicherheitsstandard kontinuierlich zu erhöhen.

E-Health

18 Sicherheit von Patientendaten: Meldepflichten am Horizont

Dr. Thomas Steiner, LL.M.

Hackerangriffe auf Patientendaten nehmen in den USA und in Europa zu. Die Gefahr besteht auch in der Schweiz. Zusätzlich bedrohen Unachtsamkeit mit IT-Sicherheit und ungenügende Zugangskontrollen die Sicherheit von Patientendaten. Das Schweizer Datenschutzrecht verpflichtet Ärzte und Spitäler bisher nicht, Entwendungen personenbezogener Gesundheitsdaten (Patientendaten) an die Datenschutzaufsichtsbehörde oder an die betroffenen Patienten zu melden. Das könnte sich bald ändern.

Unerlaubte Entwendung von Patientendaten

Im letzten Jahr betrafen die beiden grössten in Kalifornien an den Attorney General gemeldeten Entwendungen nicht verschlüsselter Personendaten (sog. Data Breach) einen Krankenversicherer (Anthem) und eine Gruppe von Spitälern (UCLA Health). Es waren personenbezogene Daten von 10,4 Millionen Versicherten bzw. 4,5 Millionen Patienten betroffen. Entwendete Daten werden typischerweise für Identitätsdiebstähle oder zur Erpressung betroffener Personen missbraucht.

Andere, ebenfalls häufige Ursachen für Data Breaches sind: 1) Verlust oder Diebstahl (physisch); 2) Unachtsamkeit von Mitarbeitern beim Umgang mit IT-Systemen sowie 3) der Missbrauch bzw. die unautorisierte Nutzung von Zugangsrechten (intern).

Diese Gefahren bestehen auch für in der Schweiz gespeicherte und verarbeitete Patientendaten.

Datensicherheit beim elektronischen Patientendossier

Im nächsten Jahr wird in der Schweiz das elektronische Patientendossier eingeführt. Patientendaten werden dann weiterhin primär auf den Servern der jeweiligen Spitäler und Praxen gespeichert (sog. Primärsystem). Künftig besteht aber die Möglichkeit, dass Ärzte direkt auf bei anderen Ärzten oder bei Spitälern bzw. sog. Gemeinschaften oder Stammgemeinschaften gespeicherte Patientendaten zugreifen können, vorausgesetzt Arzt und Patient beteiligen sich am elektronischen Patientendossier (für Spitäler ist die Teilnahme obligatorisch).

Man spricht von einem dezentralen bzw. virtuellen Patientendossier. Sogenannte Gemeinschaften und Stammgemeinschaften ermöglichen und koordinieren den Zugriff auf die dezentral gespeicherten Daten (sog. Sekundärsystem). Sie müssen sich zertifizieren lassen und ein System zur Erkennung sicherheitsrelevanter Vorfälle implementieren. Sicherheitsrelevante Vorgänge müssen sie der Zertifizierungsstelle und dem Bundesamt für Gesundheit (BAG) melden. Für Spitäler und Ärzte gelten derzeit keine vergleichbaren gesetzlichen Meldepflichten.

Handlungsbedarf im Gesundheitswesen

Kürzlich hat sich der Bundesrat in einer Stellungnahme (Antwort auf Interpellation Graf-Litscher) zur Sicherheit der elektronischen Patientendaten geäussert. Er hat festgestellt, dass «das allgemeine Sicherheitsniveau im Gesundheitswesen leider noch nicht demjenigen anderer Branchen (z. B. Finanzen, Versicherungen, Verwaltung)» entspricht und deshalb Handlungsbedarf bestehe. Was genau getan werden müsste, hat der Bundesrat aber nicht gesagt. Er hat auf die Zertifizierungsvoraussetzungen für Gemeinschaften und Stammgemeinschaften sowie auf die Datenschutzgesetze von Bund und Kantonen verwiesen. Bisher enthalten aber weder das Datenschutzgesetz des Bundes (DSG) noch die kantonalen Datenschutzgesetze Data-Breach-Meldepflichten. Auf Bundesebene könnte sich das bald ändern.

Data-Breach-Meldepflichten am Horizont

Das DSG wird derzeit revidiert. Der Vorentwurf liegt noch nicht vor. Die Grundzüge der Revision sind aber bereits bekannt. Geplant ist unter anderem die Pflicht, Verletzungen der Datensicherheit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) zu melden. Wenn ein hohes Risiko für die Persönlichkeit der betroffenen Personen besteht, müssen (so die geplante Regelung) diese ebenfalls informiert werden. Inspiriert ist die Regelung von der Meldepflicht, die in der EU ab dem 25. Mai 2018 gilt.

Meldung an die Datenschutzaufsichtsbehörde: EU

Wer Leistungen auf dem EU-Binnenmarkt erbringt, muss sich bei der Bearbeitung von Personendaten ab dem 25. Mai 2018 an die EU-Datenschutzgrundverordnung (DS-GVO) halten. Diese verpflichtet die für die Bearbeitung Verantwortlichen, unbefugte Zugriffe auf personenbezogene Daten an die zuständige Datenschutzaufsichtsbehörde zu melden. Die Meldung muss innert 72 Stunden erfolgen. Bei unterlassener Meldung droht eine Busse von bis zu 10 000 000 EUR oder von bis zu 2 % des im vorangegangenen Geschäftsjahr weltweit erzielten Umsatzes (je nachdem, welcher der Beträge höher ist).

Meldung an die betroffenen Personen: EU

Gemäss EU-DS-GVO muss die Verletzung der Datensicherheit zusätzlich den betroffenen Personen gemeldet werden, wenn voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Dies ist dann der Fall, wenn Daten entwendet, offengelegt, vernichtet oder verändert wurden.

Die DS-GVO regelt nebst der Meldepflicht auch konkrete für die Meldung an die betroffenen Personen geltende Ausnahmen. Diese müssen in den folgenden Fällen nicht zusätzlich zur Aufsichtsbehörde informiert werden: 1) wenn der für die Bearbeitung Verantwortliche angemessene technische oder organisatorische Sicherheitsmassnahmen (z. B. Pseudonymisierung oder Verschlüsselung) getroffen hat und diese auf die vom Data Breach betroffenen Daten angewendet hat; 2) wenn er nach Entdeckung des Vorfalls durch Massnahmen sichergestellt hat, dass für die betroffenen Personen aller Wahrscheinlichkeit nach kein hohes Risiko mehr besteht; oder 3) wenn der Aufwand für eine individuelle Benachrichtigung der betroffenen Personen unverhältnismässig wäre und eine öffentliche Bekanntgabe vergleichbar wirksam wäre.

Transparenz fördert Sicherheit

Im Bereich der Luftfahrt bestehen extensive Meldepflichten zu sicherheitsrelevanten Vorfällen. Sie tragen dazu bei, dass selbst kleinere Vorfälle untersucht und Sicherheitslücken geschlossen werden. Im Gesundheitsbereich hingegen fehlt diese Transparenz bisher. Wenn Leistungserbringer im Gesundheitswesen unerlaubte Zugriffe auf oder Entwendungen von personenbezogenen Gesundheitsdaten künftig – ähnlich wie in der EU – der Datenschutzaufsichtsbehörde melden müssten, könnte dies für mehr Transparenz sorgen.

Hierfür müssten aber nebst dem DSG auch die kantonalen Datenschutzgesetze angepasst werden. Denn Spitäler unterstehen bei der Bearbeitung personenbezogener Daten in vielen Bereichen dem kantonalen Datenschutzrecht. Zu diesen Bereichen gehören insbesondere stationäre Leistungen, die Spitäler ganz oder teilweise zulasten der obligatorischen Krankenpflegeversicherung erbringen, sowie unter einem kantonalen Leistungsauftrag erbrachte ambulante Leistungen.

Der EDÖB und die Aufsichtsbehörden des Bundes müssten in ihren jeweiligen Tätigkeitsberichten zumindest anonymisiert über gemeldete Data Breaches informieren. Zudem steht eine Meldung jeweils am Anfang einer internen Untersuchung des Vorfalls in Kooperation mit der Aufsichtsbehörde. Diese dient letztlich der Eruierung von Fehlerquellen und der Schliessung von Sicherheitslücken.

19 Der lange Weg zum elektronischen Patientendossier: Der Basler E-Health-Modellversuch

Dr. David Jenny, LL.M.

Was ist E-Health?

Elektronische Daten-Kommunikation im Gesundheitswesen wird als E-Health bezeichnet. Ein Teilbereich ist das elektronische Patientendossier. Geregelt wird es im Bundesgesetz über das elektronische Patientendossier (EPDG) vom 19. Juni 2015, das 2017 in Kraft treten soll. Gemäss Art. 2 lit. a EPDG ist ein elektronisches Patientendossier ein «virtuelles Dossier, über das dezentral abgelegte behandlungsrelevante Daten aus der Krankengeschichte einer Patientin oder eines Patienten oder ihre oder seine selber erfassten Daten in einem Abrufverfahren in einem konkreten Behandlungsfall zugänglich gemacht werden können». Zugriffsrechte haben nebst dem Patienten auch die Gesundheitsfachpersonen, denen der Patient diese Rechte erteilt. In medizinischen Notfallsituationen können auch Gesundheitsfachpersonen ohne Zugriffsrechte zugreifen, soweit dies nicht ausdrücklich ausgeschlossen wurde.

Nur mit Einwilligung

Erstellt werden kann ein elektronisches Patientendossier nur mit schriftlicher Einwilligung des Patienten. Gültig ist die Einwilligung nur, «sofern die betroffene Person sie nach angemessener Information über die Art und Weise der Datenbearbeitung und deren Auswirkungen freiwillig erteilt» (Art. 3 Abs. 1 EPDG). Wer einwilligt, ist vermutungsweise einverstanden, dass im Behandlungsfall Daten im elektronischen Patientendossier erfasst werden. Die Einwilligung ist jederzeit widerrufbar.

Basler Modellversuch

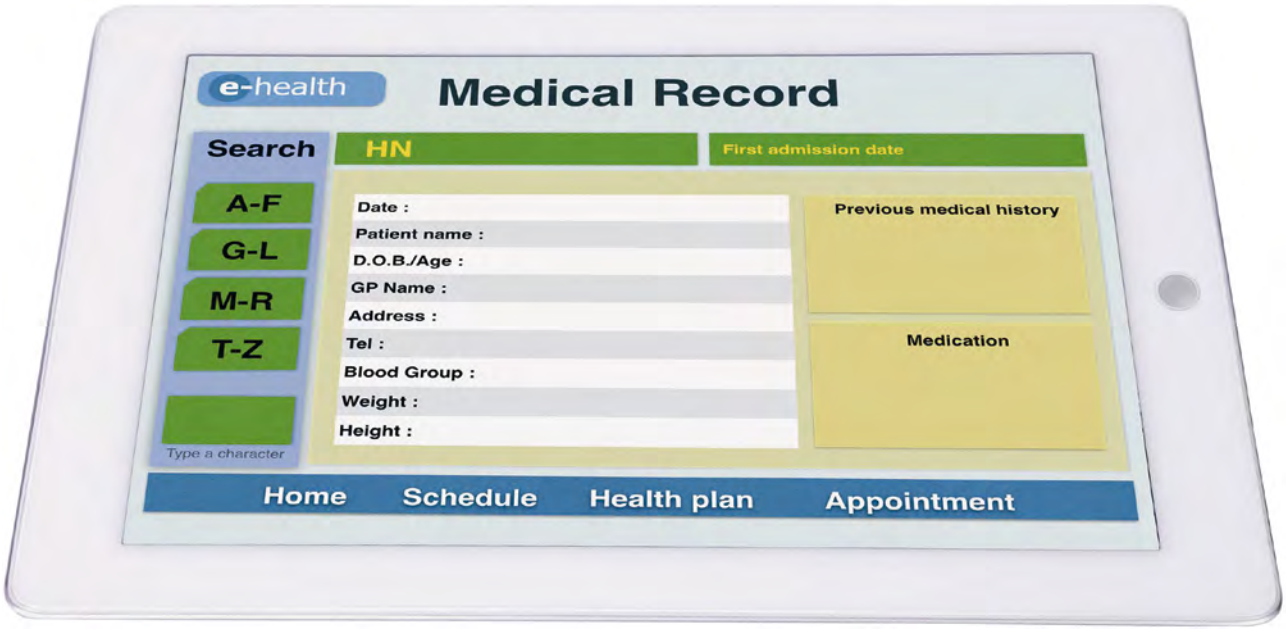
In Basel-Stadt wurden die Arbeiten zur Einführung des elektronischen Patientendossiers einige Zeit vor Inkrafttreten des EPDG in Angriff genommen. Einerseits wurden 2013 Ausgaben für die Realisierung des E-Health-Modellversuchs Regio Basel bewilligt, andererseits wurden die für den Modellversuch notwendigen gesetzlichen Änderungen geschaffen.

Besondere Personendaten

§ 59 des kantonalen Gesundheitsgesetzes erlaubt die Durchführung von E-Health-Modellversuchen und ermächtigt den Regierungsrat zur Regelung der zur bearbeitenden Personendaten und Zugriffsrechte. Gesundheitsdaten sind jedoch Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung (beispielsweise des Grundrechts auf Schutz der Privatsphäre) besteht. Notwendig ist daher eine spezielle formellgesetzliche Grundlage, die dem Referendum untersteht. Eine nicht referendumsfähige regierungsrätliche Verordnung genügt diesen Anforderungen nicht.

Vom Gesetz …

Um den E-Health-Modellversuch im Kanton Basel-Stadt zu ermöglichen, musste daher das kantonale Gesetz über die Information und den Datenschutz (IDG) geändert werden. Das Datenschutzgesetz des Bundes (DSG) kommt nicht zur Anwendung, da dieses nur die Bearbeitung von Daten durch private Personen und Bundesorgane regelt. Die 2013 neu geschaffene kantonale Bestimmung regelt allgemein die Voraussetzungen für das Bearbeiten von Personendaten im Rahmen von Pilotversuchen.



Bewilligt werden kann die Bearbeitung von besonderen Personendaten, wenn die fragliche Aufgabe in einem Gesetz geregelt ist (für das Patientendossier im Gesundheitsgesetz), ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden und eine Testphase vor dem Wirksamwerden des fraglichen Gesetzes zwingend erforderlich ist. Dies liegt vor, wenn:

a) die Erfüllung einer Aufgabe technische Neuerungen erfordert, deren Auswirkungen zunächst evaluiert werden müssen,

b) die Erfüllung einer Aufgabe bedeutende organisatorische oder technische Massnahmen erfordert, deren Wirksamkeit zunächst geprüft werden muss, insbesondere bei der Zusammenarbeit mit öffentlichen Organen des Bundes und anderer Kantone und Privaten oder

c) sie die Übermittlung von besonderen Personendaten an Dritte mittels eines Abrufverfahrens erfordert.

Pilotprojekte wie der E-Health-Modellversuch sind auf maximal fünf Jahre zu befristen und zu evaluieren.

… zur Verordnung …

Damit der Basler Modellversuch starten durfte, mussten schliesslich die Details in der Verordnung über den E-Health-Modellversuch geregelt werden. Darin finden sich u. a. Bestimmungen zur Teilnahmeberechtigung am Versuch, zur Einwilligung zur Datenbearbeitung im elektronischen Patientendossier, zum Zugriff zum Dossier durch den Patienten oder die Fachperson und weitere Personen. Datenverantwortlich mit Gesamtverantwortung ist das Gesundheitsdepartement, das insbesondere das Risikomanagement übernimmt und die Sicherheitsmassnahmen bestimmt. Ein Trägerverein E-Health soll sodann Leistungserbringer und Patienten in den Modellversuch einbinden.

… zum konkreten Nutzen

Bis Neuerungen wie das elektronische Patientendossier für den einzelnen Patienten und die Fachpersonen im Gesundheitswesen Alltag sind, müssen in unserem föderalistischen Gemeinwesen einige Hürden überwunden werden. Die Bereitstellung der entsprechenden technischen Infrastruktur und deren Finanzierung reichen bei Weitem nicht aus. Auf Bundes- und kantonaler Ebene müssen die rechtlichen Voraussetzungen geschaffen werden. Das mit dem elektronischen Patientendossier verfolgte Ziel der Qualitätssteigerung der medizinischen Behandlung kann erst dann erreicht werden, wenn Patienten ihre Einwilligung geben und die Gesundheitsfachpersonen das elektronische Patientendossier nutzen werden. Ob der erwartete volkswirtschaftliche Nutzen erzielt werden wird, wird sich erst in einiger Zeit weisen.

20 Lifestyle- oder Medizinprodukt? Regulatorische Anforderungen an Medical Apps

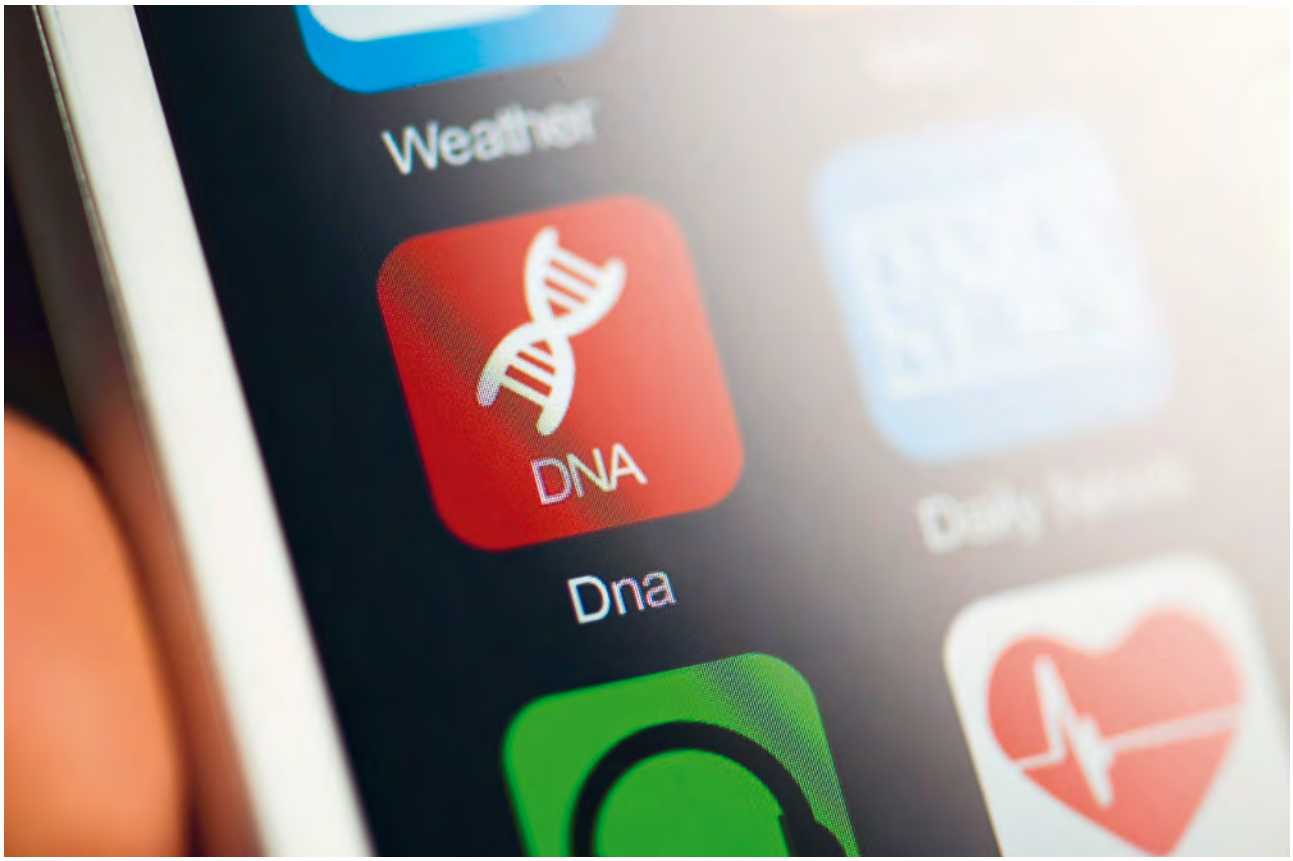
Christian Wyss, LL.M.

Heutige mobile Geräte verfügen über viele Funktionen, die auch für medizinische Zwecke genutzt werden können: Apps messen, wie oft wir uns bewegen, zählen Kalorien, geben Gesundheitstipps, analysieren Daten oder helfen bei der Dosierung von Medikamenten. Apps im Bereich Lifestyle, Fitness, Wohlbefinden und Ernährung bleiben ausserhalb der Medizinprodukteregulierung und können auch von kleinen Softwareentwicklern rasch und kostengünstig erstellt werden. Zur medizinischen Verwendung bestimmte oder angepriesene Apps unterliegen dagegen den strengen Anforderungen der Medizinprodukteregulierung. Im Einzelfall kann diese Grenze schwierig zu ziehen sein.

Wellnessanwendung oder Medizinprodukt?

Das wichtigste Abgrenzungskriterium ist die Zweckbestimmung, die der App mit ihrem Namen, in der Werbung und in der Gebrauchsanweisung gegeben wird. Folgende Apps gelten beispielsweise als Medizinprodukte:

- Diabetes-Management-App zur Erfassung der Blutzuckerwerte und Ermittlung der nötigen Insulinmenge
- Sehtest-App
- Herzmassage-App, die mit Bewegungssensor und Stoppuhr prüft, ob die Herzmassage richtig ausgeführt wird
- Pulsmessung für Patienten



- App, die einem Blutspender Gesundheitsfragen stellt, um zu ermitteln, ob das Blutspendezentrum sein Blut verwenden kann
- Menstruationskalender, um die fruchtbaren Tage des Monats zu bestimmen
- App, die stillenden Müttern sagt, ob sie ein bestimmtes Medikament nehmen dürfen
- App, die hilft, mit dem Rauchen aufzuhören
- App, die überwacht, ob verschriebene Medikamente regelmässig eingenommen werden

Dagegen gelten beispielsweise folgende Apps nicht als Medizinprodukte:

- Schrittzähler
- Pulsmessung für Sportler
- App, die beim Sport an Nahrungs- und Flüssigkeitszufuhr erinnert
- Kalorienzähler für Linienbewusste
- App mit Fitnessübungen

Zubehör und Nachschlagewerke

Als Medizinprodukte gelten Apps, die ein Mobiltelefon oder Tablet zum Zubehör eines medizinischen Geräts machen: Eine App macht das iPhone zur Fernbedienung für die Insulinpumpe oder das Hörgerät, oder ein Tablet dient als Bildschirm für eine Magnetresonanztomographie.

Nicht als Medizinprodukte gelten Apps, die den Inhalt von medizinischen Büchern oder Zeitschriften auf dem Mobiltelefon verfügbar machen, z. B. ein medizinisches Wörterbuch oder Ausbildungsvideos. Geht die App über die reine Wissensbereitstellung hinaus und bietet Entscheidungsunterstützung oder berechnet eine Medikamentendosis, liegt ein Medizinprodukt vor.

Warum ist diese Abgrenzung wichtig?

Nicht alle Softwareentwickler sind vertraut mit den umfangreichen regulatorischen Anforderungen im Gesundheitswesen. Fällt eine App unter die Medizinprodukteregulierung, gelten erhöhte Anforderungen an Qualitätsmanagement und Dokumentation bei Entwicklung, Programmierung, Validierung, Testing und Versionenmanagement. Die Markteinführung erfordert ein CE-Kennzeichen und muss in den meisten Fällen der Swissmedic gemeldet werden.

Swissmedic kann nachträglich kostenpflichtige Kontrollen durchführen, um zu bestimmen, ob eine App als Medizinprodukt gilt und ob die Voraussetzungen für das Inverkehrbringen erfüllt sind. Sind diese nicht erfüllt, kann Swissmedic die App vom Markt nehmen und das weitere Inverkehrbringen in der Schweiz und in der EU unter Strafandrohung verbieten.

21 E-Commerce mit Arzneimitteln: Gefahr für die Gesundheit oder Geschäftsmodell der Zukunft?

Barbara Schroeder de Castro Lopes, LL.M.

Arzneimittel sind kein unbedenkliches Konsumgut, sondern enthalten Wirkstoffe mit Gefahrenpotenzial. Entsprechend restriktiv hat der Gesetzgeber auch die Bestimmungen zum Versandhandel ausgestaltet. Demnach ist E-Commerce mit Medikamenten, welcher als eine Spezialform des Versandhandels gilt, grundsätzlich untersagt. Bewilligungen werden nur ausnahmsweise und unter strengsten Sicherheits- und Qualitätsanforderungen erteilt.

Dennoch stehen international die Zeichen beim Geschäft mit der «Online-Pille» auf Wachstum. Sollen die Arzneimittelhersteller daher auch hierzulande ihre Marketing-Aktivitäten mehr in Richtung Versandapotheken verlagern? Inwiefern ist ein Strukturwandel bei einer derart strengen Regulierung und einer starken Apothekerlobby überhaupt möglich?

Leitprinzipien bei der Abgabe von Arzneimitteln

Die vom Gesetzgeber verfolgte Regel-Ausnahme-Struktur für den Versandhandel (Verbot mit Erlaubnisvorbehalt) widerspiegelt die Leitprinzipien bei der Abgabe von Arzneimitteln in der Schweiz. Demnach soll eine Abgabe nur nach persönlicher, sachgerechter Fachberatung durch Apotheker bzw. Drogisten sowie unter ärztlicher Überwachung möglich sein. Ein Anspruch auf Erteilung einer Versandhandelsbewilligung besteht nach dieser Konzeption also nicht. Auch nicht rezeptpflichtige Arzneimittel (OTC-Arzneien) benötigen eine ärztliche Verschreibung, wenn das Medikament online bestellt wird. Daneben muss ein entsprechendes Qualitätsmanagement sicherstellen, dass eine ausreichende persönliche Beratung und Überwachung der Patienten durch eine Fachperson erfolgt und dass die versendeten Arzneimittel nur an die Personen ausgeliefert werden, auf deren Namen das Rezept ausgestellt wurde. Lagerung und Transport dürfen die Sicherheit und Wirksamkeit der Medikamente nicht beeinträchtigen.

Rein virtuelle Apotheke nicht zulässig

Eine rein virtuelle Apotheke ohne Betrieb einer realen Präsenzapotheke ist zudem nicht möglich. Der Grund: um im Bewilligungsdickicht der schweizerischen Arzneimittelgesetzgebung Chancen auf eine Ausnahmebewilligung für den Versandhandel zu haben, wird zunächst eine kantonale Detailhandelsbewilligung benötigt. Diese wird nur denjenigen erteilt, die eine Präsenzapotheke führen.

Vorteile von Versandapotheken im Wettbewerb

Versandapotheken profitieren insbesondere vom Diskretionsbedürfnis der Patienten sowie vom 24/7-Service. Auch das Einsparen des Abholungsaufwands wird von einem bestimmten Kundensegment als Vorteil angesehen. Daneben erheben Versandapotheken grundsätzlich keinen Bezugs- und Medikamentencheck (Gebühren für Rezeptkontrolle, Patientenberatung und Dossiereröffnung). Da nur eine einzige reale Apotheke erforderlich ist, fallen auch für den schweizweit flächendeckenden Vertrieb die Miet- und Personalkosten für eine Ladenkette weg und auch die Kosten für die Logistik können flexibler strukturiert werden. Eine Fokussierung auf ein bestimmtes Kundensegment ist im Versandhandel eher möglich.

Ein Blick über die Grenze

Während gesundheitliche Gefahren beim illegalen Vertrieb mit gefälschten und/oder nicht zugelassenen Arzneimitteln nicht von der Hand zu weisen

sind, ist andererseits ebenso offensichtlich, dass weder der legale noch der illegale Internethandel mit Medikamenten an der Grenze halt machen.

Der europäische Gerichtshof hatte bereits im Jahre 2003 einen Fall zu beurteilen, in dem sich der deutsche Apothekerverband e. V. und die Online Apotheke DocMorris – nun eine Tochterfirma der schweizerischen Versandapotheke «Zur Rose» – gegenüberstanden. In diesem Urteil hielt er fest, dass ein nationales Verbot des Versandhandels für OTC-Arzneien nicht gerechtfertigt und eine mit dem freien Warenverkehr im EU-Binnenmarkt nicht vereinbare Beschränkung sei. Zur Verbesserung der Sicherheit ist seit Mitte 2015 ein EU-Versandhandelslogo für den Internethandel mit Humanarzneimitteln vorgeschrieben. Das Versandhandelslogo soll den Konsumenten zeigen, dass ein Versandhändler nach seinem jeweiligen nationalen Recht zum Versandhandel über das Internet mit Arzneimitteln berechtigt ist. Zudem lässt sich zukünftig auf den ersten Blick der Mitgliedstaat erkennen, in dem der Versandhändler niedergelassen ist.

Im jüngsten Urteil des EuGH vom Oktober 2016 ging es um die Frage, ob die deutsche Preisbindung für Arzneimittel auch für ausländische Versandapotheken gilt, wenn diese rezeptpflichtige Medikamente an Kunden in Deutschland verkaufen. Das Gericht hat nun entschieden, dass die deutsche Preisbindung in diesem Fall für ausländische Versender nicht bindend ist. Ob dies tatsächlich zu sinkenden Preisen führt, bleibt abzuwarten. Am deutschen Apothekertag wurde bereits laut über ein generelles Verbot des Versandhandels mit rezeptpflichtigen Medikamenten nachgedacht.

In der Schweiz sind Online-Bestellungen von Arzneimitteln aus dem Ausland für Private in begrenztem Umfang möglich. Eine Privatperson darf für sich selber Arzneimittel in der Menge eines Monatsbedarfs importieren. Für die Berechnung des Monatsbedarfs sind die Angaben des Herstellers massgebend.

Hat das Bundesgericht den Versandapotheken «den Stecker gezogen»?

Nach einem Bundesgerichtsurteil im September 2015 sagte das SRF das «Aus für den Versandhandel mit Medikamenten» voraus.

Das vom Gericht beurteilte Geschäftsmodell der Versandapotheke «Zur Rose» sah vor, dass das im Versandhandel erforderliche ärztliche Rezept auch für nicht verschreibungspflichtige Medikamente von einem von der Apotheke delegierten Arzt erst nach Bestelleingang ausgestellt wurde. Auf der Basis eines vom Kunden auszufüllenden Online-Fragebogens machte sich der Arzt jeweils ein Bild vom Gesundheitszustand des Patienten und konnte bei Bedarf persönlich mit ihm Kontakt aufnehmen.

Das Bundesgericht erachtete die Modalitäten dieses Bestellvorgangs als nicht vereinbar mit dem klaren Wortlaut des Gesetzes, da kein persönlicher Kontakt zwischen Arzt und Patient stattfand und untersagte der Versandapotheke «Zur Rose» den weiteren Vertrieb von nicht rezeptpflichtigen Medikamenten auf diesem Weg. Dies, obwohl erfahrungsgemäss OTC-Arzneien in Präsenzapotheken oftmals ohne jede Beratung erhältlich sind.

Dennoch wurde den Versandapotheken mit dem Bundesgerichtsurteil nicht wie prophezeit «der Stecker gezogen». Dies belegt die auch für das Jahr 2016 bis anhin positive Umsatz- und Ergebnisentwicklung der betroffenen Versandapotheke «Zur Rose», welche aber wohl zum Teil im liberaleren Ausland erwirtschaftet wurde. Demnach besteht auch in einem anspruchsvollen regulatorischen Umfeld noch Raum für innovative Geschäftsmodelle. Der E-Commerce lässt sich auch in diesem Wirtschaftszweig kaum aufhalten und die Präsenzapotheken werden sich mittel- und langfristig nicht mit der Bekämpfung des Onlinehandels begnügen können. Eine vorausschauende Vorbereitung aller Beteiligten erweist sich deshalb als unabdingbar.

Energie

22 Smart Grids und Datenschutz

Dr. Stefan Rechsteiner

Manuel Blättler

Die Zukunft gehört den intelligenten Systemen. Dies gilt auch für Stromnetze. Doch mit dem Austausch von Daten zwischen den Komponenten eines intelligenten elektrischen Netzes kommen datenschutzrechtliche Fragestellungen. Welche dies sind, wird nachfolgend skizziert.

Smart Grids sind intelligente elektrische Netze

Smart Grids verdanken ihren Namen der Vernetzung neuer Technologien mithilfe von Informations- und Kommunikationstechnologie. Mit Smart Meters – intelligenten Messsystemen – werden Verbrauchsdaten von Haushalten und Unternehmen generiert und gesammelt. Diese Daten können wiederum im Rahmen eines Smart-Grid-Systems von den verschiedenen Marktteilnehmern genutzt werden, um den intelligenten Austausch der Energie aus verschiedenen Quellen sicherzustellen. Die bestehenden Stromnetze können dadurch besser genutzt und die Netzstabilität gewährleistet werden. So kann z. B. die schwankende Elektrizitätserzeugung aus erneuerbaren Energien mit intelligenten Steuerungen und der Einbindung von Stromspeichern, wie Batterien oder Elektroautos, besser ausbalanciert werden.

Energiestrategie 2050 – neue Regelungen zu den intelligenten Systemen

Am 30. September 2016 verabschiedete das Parlament das erste Massnahmenpaket der Energiestrategie 2050. Darin enthalten sind auch Bestimmungen zum Thema Smart Grid; namentlich im Zusammenhang mit der Einführung und Weiterentwicklung von intelligenten Messsystemen beim Endverbraucher sowie intelligenten Steuer- und Regelsystemen bei Endverbrauchern und Erzeugern. Eine dieser Bestimmungen beschäftigt sich mit dem Datenschutz im Smart Grid. Aus gutem Grund. Es stellen sich heute nämlich drängende Fragen zu dieser Thematik.

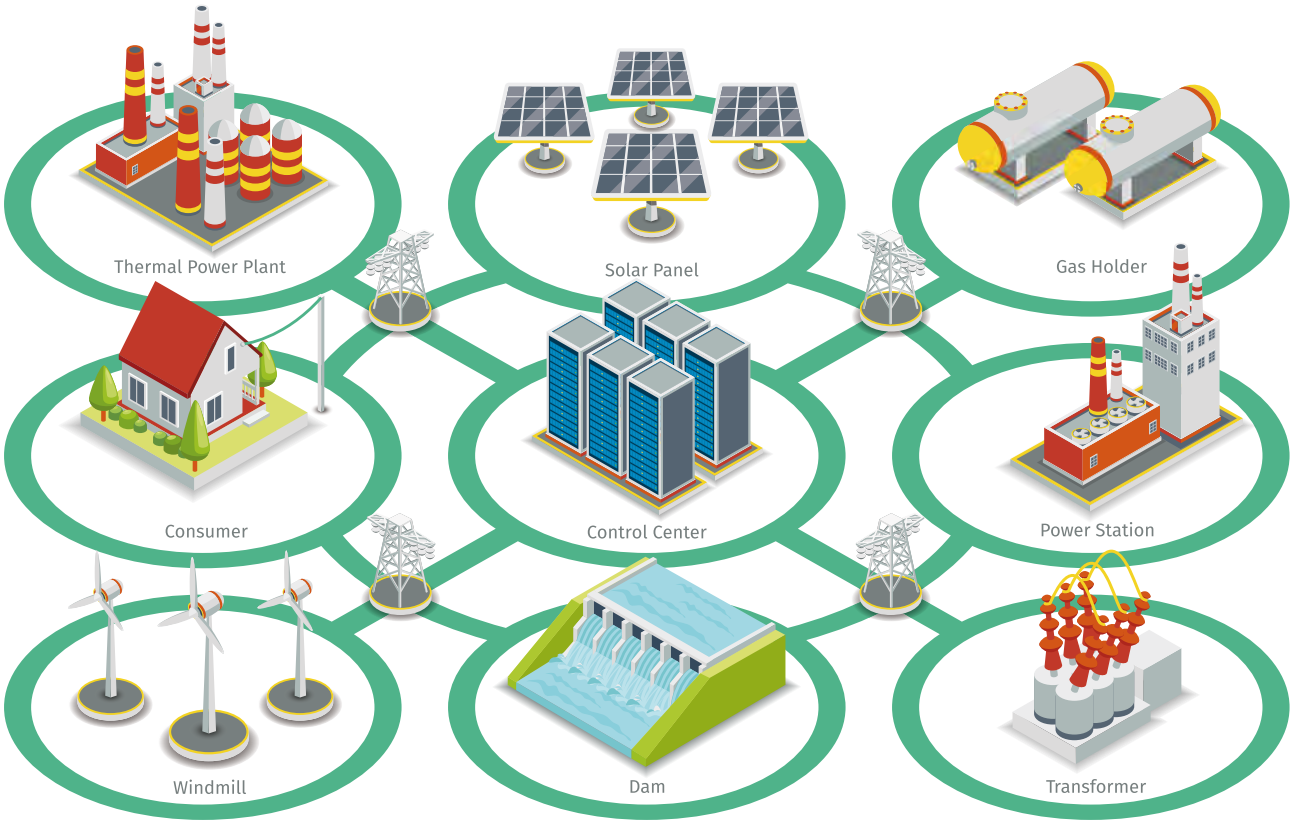
Einhaltung des Datenschutzes – viele Datenströme umfassen Personendaten

Bei einem grossen Teil der im Smart-Grid-System fliessenden Datenströme, wie z. B. Abrechnungsdaten, Kundendaten und Meter-Daten, handelt es sich um Personendaten, also Daten, die einer bestimmten Person zugeordnet werden können. Beim Umgang mit Personendaten sind die datenschutzrechtlichen Vorgaben – im Sinne des Schutzes von Personendaten vor Missbrauch – zu beachten. Dies geht soweit, dass wenn ein Datensatz Personendaten enthält, hinsichtlich des ganzen Datensatzes die datenschutzrechtlichen Vorgaben zu beachten sind.

Rechtszersplitterung und Rechtsunsicherheit – Datenschutzgesetze von Bund und Kantonen existieren nebeneinander

Das bundesrechtliche Datenschutzgesetz gilt zwischen Privaten und gegenüber Bundesbehörden. Parallel dazu haben aber auch die Kantone eigene Datenschutzgesetze. Diese gelten im Umgang mit kantonalen Behörden. Viele Netzbetreiber können im weiteren Sinne zur kantonalen Verwaltung gezählt werden (Kantonswerke). Auf diese finden deshalb die kantonalen Datenschutzbestimmungen Anwendung.

Das Smart-Grid-System besteht aus privaten und öffentlichen, staatlichen und kantonalen Marktteilnehmern. Es droht deshalb eine Rechtszersplitterung innerhalb eines Smart-Grid-Systems. Der Gesetzgeber adressiert diese Problematik im Rahmen des soeben verabschiedeten ersten Massnahmenpakets zur Energiestrategie 2050. Dies geht auf die



entsprechende Empfehlung der VISCHER AG in der im Auftrag des Bundesamtes für Energie durchgeführten Studie zum Thema Datenschutz für Smart Grids zurück. So wird das Stromversorgungsgesetz nach Inkrafttreten des Massnahmenpakets explizit festlegen, dass auf die Datenbearbeitung im Zusammenhang mit intelligenten Mess-, Steuer- oder Regelsystemen das Datenschutzgesetz des Bundes Anwendung findet. In der Zukunft werden somit auch kantonale Betriebe und Anstalten im Bereich der Smart Meters datenschutzrechtlich dem Bundesrecht unterstellt sein.

Diese zukünftige Regelung über den Datenschutz verspricht eine Verbesserung im Zusammenhang mit der drohenden Rechtszersplitterung. Damit sind aber noch nicht alle Quellen von Rechtsunsicherheit beseitigt. Weder das Datenschutzgesetz des Bundes noch die Datenschutzgesetze der Kantone enthalten sektorspezifische Regelungen. Die allgemeinen Regeln können im konkreten Anwendungsfall in Bezug auf die Datenströme in Smart Grids erhebliche Interpretationsspielräume offen lassen. So kann es für den einzelnen Marktteilnehmer beispielsweise schwierig sein abzuschätzen, wann ein überwiegendes privates oder öffentliches Interesse vorliegt, das die Bearbeitung von Personendaten rechtfertigt und wann deren Bearbeitung folglich rechtmässig ist.

Im Rahmen des ersten Massnahmenpaketes zur Energiestrategie 2050 wird dem Bundesrat daher die Kompetenz eingeräumt, Ausführungsbestimmungen über die Bearbeitung von Daten in diesem Zusammenhang zu erlassen. Es ist zu hoffen, dass sich der Bundesrat den beschriebenen Problemen im Rahmen dieser Ausführungsbestimmungen annehmen wird.

Der Bund verfügt über die notwendigen Kompetenzen, hat diese aber noch nicht ausreichend genutzt

Der Bund verfügt über eine in der Verfassung verankerte Kompetenz zur Regelung des Betriebs von Smart Grids unter Einsatz von Smart-Meter-Geräten. Diese Kompetenz umfasst auch die Regelung der Nutzung und Bearbeitung von Meter-Daten.

Das Stromversorgungsgesetz des Bundes enthält bereits heute bestimmte Regelungen betreffend die Bearbeitung von Messdaten. Im Zusammenhang mit der Bearbeitung von Messdaten der Endverbraucher gilt: Wirtschaftlich sensible Informationen, die aus dem Betrieb der Elektrizitätsnetze gewonnen werden, müssen von den Elektrizitätsversorgungsunternehmen vertraulich behandelt werden und dürfen nicht für andere Tätigkeitsbereiche genutzt werden.

Die Stromversorgungsverordnung enthält auch schon Regeln zum Zugang zu Messdaten. Die Umschreibung des Zwecks, zu welchem Informationen weiteregegeben werden dürfen, ist jedoch für einige Anwendungen in Smart-Grid-Systemen zu eng. So wird z. B. die Gebäudeautomatisierung nicht von der besagten Regelung erfasst. Ausserdem stellt sich die Frage des Datenschutzes in den meisten der in der Stromversorgungsverordnung beschriebenen Fälle gar nicht erst. Dies weil für diese Fälle aggregierte Daten ohne Personenbezug (z. B. Bilanzmanagement) oder Daten, welche in längeren Zeitabständen (ein- oder zweimal jährlich) erhoben werden, genügen.

Die Kompetenzen des Bundes werden im Rahmen der Energiestrategie 2050 gerade im Bereich des Datenschutzes im Zusammenhang mit intelligenten Systemen explizit bestätigt und konkretisiert. Da die Frage des Datenschutzes im heutigen Gesetz eine untergeordnete Rolle spielt und der Gesetzgeber die drängenden Fragen noch nicht beantwortet hat, ist der Bundesrat gefordert. In der Zwischenzeit stehen wir Ihnen gerne beratend zur Seite.

Hinweis

Dieser Artikel basiert weitgehend auf dem Beitrag der VISCHER AG und der Forschungsstelle für Informationsrecht der Universität St. Gallen (FIR-HSG) zur Studie «Datenschutz für Smart Grids: Offene Fragen und mögliche Lösungsansätze» vom 30. Juni 2014 im Auftrag des Bundesamtes für Energie BFE, S. 71 ff. sowie dem Beitrag von Prof. Dr. Hettich und Dr. Stefan Rechsteiner: Datensicherheit und Datenschutz im Smart Grid, in: Jusletter next: 27. Oktober 2014 – Energierecht.

Vgl. zum Ganzen auch: Bundesamt für Energie: Smart Grid Roadmap Schweiz <*http://www.bfe.admin.ch/smartgrids/index.html?lang=de&dossier_id=06308*> (besucht am 22. September 2016), S. 3 und 20 f.

Rechtsschutz im digitalen Umfeld

23 Aufbewahrung elektronischer Dokumente: Minenfeld für international tätige Unternehmen

Dr. Reto Marghitola

Die Aufbewahrung elektronischer Dokumente ist für internationale Unternehmen doppelt wichtig: Erstens müssen sie an allen Standorten die nationalen Gesetzesbestimmungen einhalten. Zweitens kann eine geschickte Strategie helfen, wichtige Gerichtsverfahren zu gewinnen.

Im heutigen Geschäftsverkehr explodiert die Datenmenge. Gemäss Schätzungen verdoppelt sich das Datenvolumen alle 1,2 Jahre. Bei vielen Unternehmen stellt die Aufbewahrung elektronischer Daten einen signifikanten Kostenfaktor dar.

Aus rechtlicher Sicht stellen sich zwei Fragen:

1 Was muss ein Unternehmen tun, um bei der Aufbewahrung elektronischer Dokumente die gesetzlichen Vorschriften einzuhalten?
2 Sollen Dokumente, die keiner gesetzlichen Aufbewahrungspflicht unterstehen, aufbewahrt oder gelöscht werden?

Auch E-Mails betroffen

International tätige Unternehmen sind gut beraten, die Aufbewahrung von elektronischen Dokumenten nicht auf die leichte Schulter zu nehmen. Jedes Land hat eigene Vorschriften zur Aufbewahrung von Dokumenten. Werden diese nicht beachtet, drohen den fehlbaren Mitarbeitern strafrechtliche Sanktionen.

Unter Schweizer Recht müssen zum Beispiel per E-Mail erfolgte Bestellungen und Auftragsbestätigungen zehn Jahre lang aufbewahrt werden. Bereits die fahrlässige Verletzung dieser Vorschrift kann strafrechtliche Sanktionen nach sich ziehen.

Wie lange müssen Dokumente aufbewahrt werden?

Ein international tätiges Unternehmen steht auf den ersten Blick vor einer riesigen Herausforderung. Wie kann ein in hundert Ländern tätiges Unternehmen sicherstellen, dass die Aufbewahrungsvorschriften in all diesen Ländern erfüllt werden?

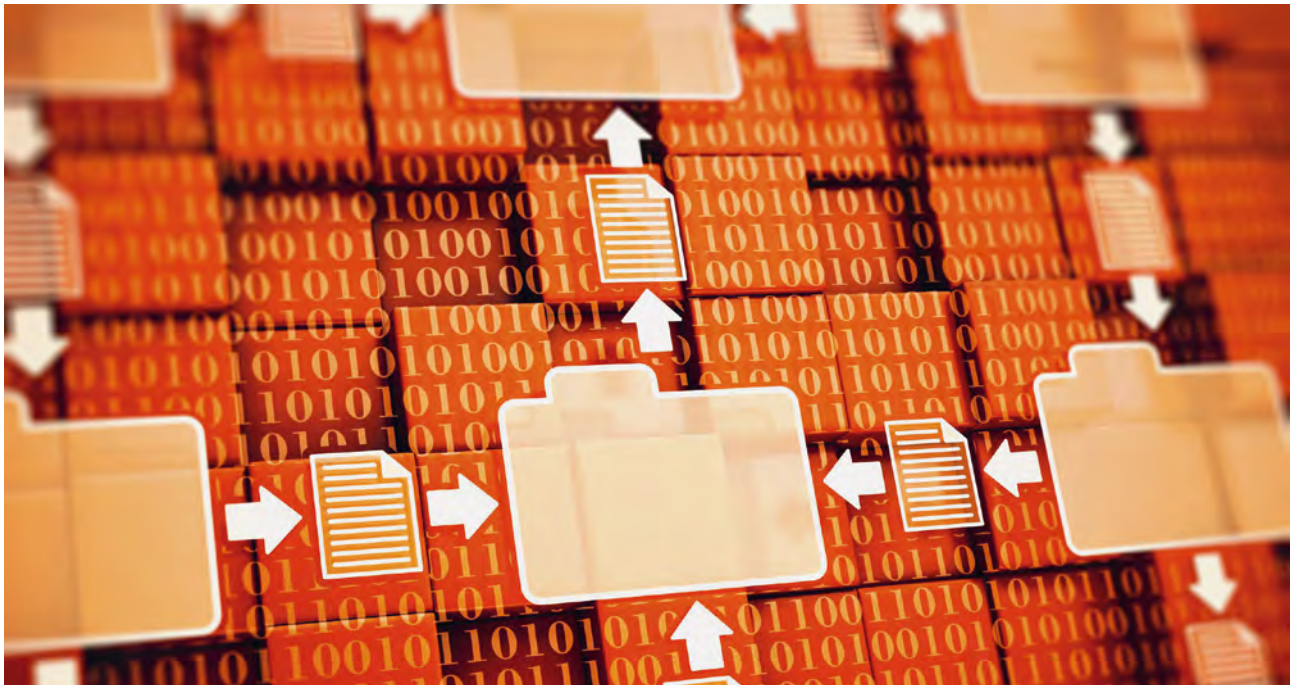
Als ersten Schritt hat es für jedes Land Folgendes zu erfassen:

- Voraussetzungen der Anwendbarkeit des nationalen Rechts (z. B. Standort im Land);
- Kategorien aufzubewahrender Dokumente (z. B. Bilanz, Geschäftskorrespondenz, etc.);
- Form der Aufbewahrung (Original, Kopie, in elektronischer Form);
- Dauer der vorgeschriebenen Aufbewahrung.

Die richtige Strategie wählen

In einem zweiten Schritt stellt sich die Frage, ob das Unternehmen freiwillig mehr Dokumente aufbewahren will als gesetzlich vorgeschrieben. Einerseits kann dies bereits aus betrieblichen Gründen nützlich sein. Andererseits ist es in späteren Gerichtsverfahren oft entscheidend, ob das Unternehmen relevante Dokumente aufbewahrt hat oder nicht.

In sogenannten «civil law»-Ländern, d. h. Ländern, welche nicht der englischen Rechtstradition folgen (u. a. kontinentaleuropäische Länder, Japan, Festland-China etc.), werden Prozesse hauptsächlich mit eigenen Dokumenten geführt. Eine Pflicht der Gegenseite, im Prozessfall Dokumente herauszugegeben, besteht – soweit nicht anders vereinbart – meist nur in sehr beschränktem Ausmass. In diesen Ländern kann es für den Prozesserfolg sehr vorteilhaft sein, wenn zum Beispiel Entwürfe aus Vertragsverhandlungen oder Berichte zur Umset-



zung von Projekten aufbewahrt werden. Dadurch kann das Unternehmen den eigenen Standpunkt im Streitfall besser beweisen.

«Document retention policy» reduziert US-Prozessrisiken

Für Grosskonzerne liegen die grössten Prozessrisiken aber meist nicht in «civil-law»-Ländern, sondern in den USA. Banken, Pharmaunternehmen und Automobilhersteller haben erlebt, was es bedeutet, in die Mühlen der US-Justiz zu geraten. Gefahr droht Unternehmen einerseits durch US-Strafverfahren und andererseits durch zivilrechtliche Sammelklagen. Exorbitante Bussen und sogenannte «punitive damages» können ganze Jahresgewinne grosser Unternehmen zunichtemachen.

In US-Zivilverfahren haben Unternehmen grundsätzlich alle relevanten Dokumente auf den Tisch zu legen. In US-Strafverfahren kann der Staatsanwalt – wenn ein Unternehmen nicht wie üblich kooperiert und relevante Dokumente «freiwillig» offenlegt – diese beschlagnahmen.

Grundsätzlich ist die Ausgangslage für US-Verfahren somit die folgende: Je mehr Dokumente ein Unternehmen freiwillig aufbewahrt, desto grösser das Risiko, dass aggressive Kläger- oder Staatsanwälte eine sogenannte «smoking gun» finden, welche ein (angebliches) Fehlverhalten des Unternehmens belegt. Für Unternehmen mit starkem US-Bezug ist daher eine «document retention policy», welche typischerweise eine kurze Dauer für das Aufbewahren von E-Mails und anderen elektronischen Dokumenten vorsieht, ein «must have».

Bei Unternehmen, welche eine separierte US-Einheit haben, kann es sinnvoll sein, eine «document retention policy» für diese und eine separate für die übrigen Einheiten zu erstellen.

Oft empfehlenswert: Automatisierte Dokumentenablage

Ist eine «document retention policy» einmal erstellt, hat das Unternehmen seine Ablage – elektronisch und in Papierform – entsprechend dieser zu organisieren. Für die elektronische Ablage empfiehlt sich ein automatisiertes System. Wird manuell abgelegt, führt dies in der Regel zu übermässig hohen Kosten. Schliesslich hat das Unternehmen seine Mitarbeiter darüber zu informieren, wie die automatische Ablage funktioniert und sie zu instruieren, welche Dokumente im Original (Bilanz, Geschäftsbericht, unterzeichnete Verträge etc.) abzulegen sind.

24 Die Bedeutung von E-Discovery in Prozessen mit Schweizer Bezug

Daniele Favalli, LL.M.

In vielen Bereichen der Wirtschaft stehen die Schweiz, Europa und auch andere Länder immer wieder unter dem Einfluss von Entwicklungen aus den USA. Im Wirtschaftsrecht sind die Unterschiede zwischen dem US-amerikanischen und dem kontinental-europäischen Rechtskreis vor allem im Prozessrecht deutlich. Während amerikanisches Vertragsrecht nicht diametral zum Vertragsrecht in der Schweiz, in Deutschland oder Frankreich steht, sind die Unterschiede im Prozessrecht signifikant. In den letzten Jahren ist jedoch ein Trend zur Amerikanisierung in diesem Bereich erkennbar. Im digitalisierten Umfeld sollten sich zudem Schweizer Unternehmen rechtzeitig damit bekannt machen.

Class Actions und E-Discovery als Beispiele aus dem US-Prozessrecht

Unterschiede im Prozessrecht lassen sich zum Beispiel an den US-amerikanischen Class-Action-Verfahren besonders eindrücklich darstellen. So kennt die Schweizer Prozessordnung kein Pendant zu US Class Actions (da z. B. die Parteien eines Prozessverfahrens bekannt sein müssen, während man in den USA nicht alle Beteiligten einer sog. Prozessklasse [class] kennen muss).

Ein weiterer diametraler Unterschied zwischen den beiden Systemen ist die Regel, dass die Parteien in einem Schweizer Zivilprozess nur in einem sehr beschränkten Umfang die Herausgabe von Dokumenten und/oder anderen Informationen von der Gegenseite verlangen können. Im Gegensatz dazu können Parteien in US-amerikanischen Prozessen grundsätzlich weitgehende Informationen von anderen Parteien verlangen (sog. Discovery-Verfahren).

Beweismittel sind meist nur digital vorhanden

In diesem Zusammenhang ist die zunehmende Digitalisierung von Informationen von grosser Bedeutung. Gemäss einer amerikanischen Institution (Advisory Committee on Civil Rules) werden 92 % aller Informationen heute in digitaler Form generiert. Etwa 70 % dieser digital generierten Informationen werden nie ausgedruckt, sondern bleiben digital:
http://www.uscourts.gov/RulesAndPolicies/rules/archives/advisory-committee-reports.aspx).

Dies bedeutet, dass z. B. Offerten überwiegend nur noch elektronisch gemacht und angenommen werden. Auf Allgemeine Geschäftsbedingungen wird meist durch Verweis auf Websites aufmerksam gemacht, die jederzeit geändert werden können. Postalisch versandte Post und Pakete können heute elektronisch verfolgt (getracked) werden. Eingekauft wird online, Zahlungen werden per E-Banking erledigt, Flugtickets werden per SMS oder E-Mail auf das Mobiltelefon gesandt und von dort geladen, Begriffe wie Clouds, Social Media und Smartphones sind heute allgemeiner Sprachgebrauch und werden von einer grossen Mehrheit privat und beruflich genutzt.

Weiter ist festzustellen, dass weltweit immer mehr E-Mails versandt werden, immer mehr E-Mail-Konten geführt werden und die Digitalisierung über soziale Netzwerke rasant voranschreitet, was an folgendem Beispiel verdeutlicht wird:
http://www.radicati.com/wp/wp-content/uploads/2012/08/Email-Statistics-Report-2012-2016-Executive-Summary.pdf.

	2012	Schätzung bis 2016
E-Mail-Konten weltweit	3,35 Mrd.	4,337 Mrd.
E-Mail-Konten von Unternehmen	850 Mio.	1,151 Mrd.
E-Mails pro Tag weltweit	144,8 Mrd.	192,2 Mrd.
E-Mails pro Tag weltweit von Unternehmen	89 Mrd.	143,8 Mrd.
Instant-Messages-(IM-)Konten	2,7 Mrd.	3,4 Mrd.
Social-Network-Konten weltweit	2,7 Mrd.	4,3 Mrd.
User von E-Mails über das Handy weltweit	730 Mio.	n/a

Die Verbreitung von digitalen Informationen ist unaufhaltsam und es ist unmöglich zu verhindern, dass eine in der Schweiz erstellte digitale Information nicht irgendwo auf der Welt gespeichert oder verbreitet wird.

Trend zu umfangreicher Datenherausgabe

Im US-amerikanischen Zivilprozess ist bereits seit Jahren ein Trend zu umfangreicher elektronischer Datenedition im Gange, dem sich auch die Schweiz nicht entziehen kann. Die Herausgabe von elektronischen Daten im amerikanischen Zivilprozess wird als E-Discovery bezeichnet. Auch in der Schweiz ist eine zunehmende Amerikanisierung festzustellen.

Dies gilt zunächst im Bereich des Schiedsverfahrensrechts. Während früher in den, zwischen den Parteien und dem Schiedsgericht, vereinbarten prozessualen Zeitplänen das Thema «Discovery» bzw. «E-Discovery» auf dem europäischen Kontinent schlicht kein Thema war, wird heute von Anfang an Zeit für die Edition von (elektronischen Informationen und) Dokumenten eingeplant (allerdings in beschränktem Umfang).

Im Rahmen der Vereinheitlichung des Schweizer Zivilprozesses im Jahre 2011 wurde zudem eine erleichterte Beweisabnahme eingeführt, wonach nicht mehr nur in dringlichen Fällen (wenn später der Beweis nicht mehr zur Verfügung stehen würde) Beweis abgenommen werden kann (Art. 158 ZPO), sondern auch vor oder während des Prozesses (z. B. zur Beurteilung der Prozessrisiken). Diese Neuerung sollte nach dem Willen des Gesetzgebers keine Einführung von Discovery darstellen. Eine Erleichterung der Beweiserhebung ist aber damit jedenfalls erfolgt.

Weiter ist festzustellen, dass schweizerische Unternehmen zunehmend global und digital tätig sind. Oft haben Schweizer Unternehmen Tochtergesellschaften, Filialen, Verkaufsstellen und dergleichen im Ausland. Damit erhöht sich das Risiko, dass z. B. Tochtergesellschaften in den USA unter Druck US-amerikanischer Gerichte verpflichtet werden können, an einer E-Discovery teilzunehmen – diese kann auch Informationen betreffen, die letztlich in der Schweiz liegen. Oder ein Tochterunternehmen einer Schweizer Gesellschaft befindet sich aufgrund von Vertragsbeziehungen mit einer amerikanischen Gruppe auf einmal in einem amerikani-

schen Prozess, wo auch Dokumente mit Schweizer Bezug gefordert werden. Selbst bei Zivilprozessen in den USA, wo keine Schweizer Partei beteiligt ist, kann es passieren, dass eine dieser Prozessparteien auf der Grundlage des Haager Beweisübereinkommens die Übermittlung von Informationen verlangt, wenn z. B. das Schweizer Unternehmen als Konkurrent (oder Zulieferer von Teilen) im Markt bekannt ist und eine Prozesspartei glaubt, dadurch wichtige Informationen für ihren Prozess erhalten zu können (selbst wenn es sich eigentlich nur um einen Ausforschungsbeweis handelt).

Was könnte alles herauszugeben sein?

Inhaltlich kann sich E-Discovery (wenigstens nach weitreichendem, US-amerikanischem Verständnis) auf folgende Informationen beziehen und es ist heute gerade für Schweizer Unternehmen sinnvoll, sich Gedanken zu machen, wie mit derartigen Forderungen in der Zukunft umzugehen sein wird:

- Unternehmensdaten; Finanzzahlen inkl. Steuer- und Buchhaltungsinformationen;
- Korrespondenz; Faxschreiben (gesendet und erhalten);
- Entwürfe von Dokumenten sowie auch nicht gespeicherte Änderungen in einem Dokument; Tabellen und Entwürfe von Tabellen;
- Telefonnachrichten (auch gelöschte);
- Instant-Mitteilungen / Chats (gesendet und erhalten); LinkedIn- und Facebook-Einträge sowie Kommunikationen, welche über Social Media erfolgt sind;
- E-Mails (Outlook bzw. auf Unternehmensservern), Anhänge zu E-Mails;
- Internet Service Provider (ISP) E-Mails wie Yahoo, Googlemail, AOL usw.;
- Ordnernamen / elektronische Pfade und Verzeichnisse, Hauptordnerverzeichnisse;
- Sämtliche Aktivitäten im Internet inklusive Verweildauer auf den jeweiligen Seiten; Bilder inklusive im Internet besuchte Bilder;
- Metadata (Metainformationen sind Daten, die Informationen über Merkmale anderer Daten enthalten, aber nicht diese Daten selbst; bei Büchern sind das z. B. der Autor, der Verlag, das Erscheinungsjahr, die Auflage, bei elektronischen Dokumenten geht es um Verfasser, Zeitpunkt der Erstellung und der vorgenommenen Änderungen, die Frage, wer wann eine Datei geändert hat etc.);
- Ephemeral-Data (temporäre Daten wie RAM oder Caches wie bei IM oder Voice over IP [VOiP]);
- Database-Dateien;
- Files access history von Servern und/oder dem Internet; Verlauf Internetsuchen und Suchkriterien;
- Kontaktlisten, Outlook-Kalender;
- Kreditkartennummern und Online-Transaktionen;
- Blogs;
- Inventarlisten von externen Hardwarekomponenten (am Computer angeschlossene Geräte wie Drucker, Back-up-Systeme sowie externe Media-Applikationen); Software-Inventarlisten;
- Gelöschte Daten und Files.

Dieser schier unbegrenzte Umfang an Daten, der zumindest nach amerikanischem Verständnis ohne Weiteres gefordert werden können soll, zeigt, dass es in Zukunft wichtig sein wird, dass sich auch Unternehmen in der Schweiz zu E-Discovery Gedanken machen (Wo werden Daten gespeichert? Wann und wie sollten Daten gelöscht werden? Wie ist vorzugehen, wenn Unternehmen in die USA liefern oder, sofern es Zulieferer sind, ob die Kunden Produkte in die USA verkaufen? Gibt es Wege, um die Herausgabe zu verhindern, z. B. durch geeignete Klassifizierung?). Nicht nur die Wahrscheinlichkeit von E-Discovery für Unternehmen in der Schweiz nimmt zu, auch die schiere Menge an potenziell herauszugebenden Daten.

Solche Verfahren können rasch kostenintensiv, zeitlich langwierig und potenziell schädlich sein.

25 «Lust auf Lunch?»: Beweiserhebung im Umfeld privater E-Mails

Dr. Thomas Steiner, LL.M.

In Untersuchungen von Wettbewerbsbehörden, branchenspezifischen Aufsichtsbehörden oder der Staatsanwaltschaft sind Unternehmen häufig dazu verpflichtet, bei der Ermittlung des Sachverhalts mitzuwirken. Dazu gehört auch die Beweiserhebung im Rahmen interner Untersuchungen. Auch im Vorfeld von Zivilprozessen, bei denen ein Unternehmen als Kläger oder Beklagter auftritt, muss dieses intern Beweise erheben.

Beweisrelevante elektronische Dokumente befinden sich regelmässig in E-Mail-Postfächern oder Archiven. Bei der Durchsuchung von E-Mails und anderen elektronischen Dokumenten zur Beweiserhebung müssen Unternehmen die Privatsphäre ihrer Mitarbeiter respektieren und schützen. Das hindert Unternehmen aber nicht daran, ihrer Mitwirkungspflicht nachzukommen. Obwohl eine Suche nach beweisrelevanten elektronischen Dokumenten auch private E-Mails und persönliche Dokumente von Mitarbeitern zutage fördern kann, ist diese – wenn sie verhältnismässig und schonend erfolgt – datenschutzrechtlich zulässig. Die gezielte Suche nach auf Geschäftsservern gespeicherten privaten E-Mails von Mitarbeiterinnen und Mitarbeitern ist hingegen nur in Ausnahmefällen (in erster Linie bei konkretem Missbrauchsverdacht) zulässig.

Ein Privatnutzungsverbot nützt nur bedingt

Einige Unternehmen verbieten es ihren Mitarbeitern, den geschäftlichen E-Mail Account für den Austausch privater E-Mails zu nutzen. Ist dies der Fall, darf das Unternehmen immerhin vermutungsweise davon ausgehen, dass alle durchsuchten E-Mails geschäftsrelevant und nicht privat sind.

Die meisten Unternehmen erlauben oder dulden aber den Austausch privater E-Mails über Geschäftsadressen. Mitarbeiter verabreden sich über Geschäfts-E-Mails zu Lunch oder Feierabendbier mit Kollegen oder Freunden. Sie organisieren private Networking-Events oder bauen mit Mitarbeitern von Kunden über Jahre ein freundschaftliches Verhältnis auf und fragen in separaten oder als Teil von geschäftlichen E-Mails auch nach deren Befinden.

Ob die Privatnutzung nun erlaubt oder verboten ist – ein Unternehmen muss immer damit rechnen, dass sich in durchsuchten Postfächern und elektronischen Archiven auch private E-Mails von Mitarbeitern befinden. Solche E-Mails darf das Unternehmen zumindest dann nicht hinter dem Rücken des Mitarbeiters durchforsten, wenn der Betroffene nicht am untersuchten Sachverhalt beteiligt war. Doch selbst wenn der Mitarbeiter z. B. unter jenen Personen ist, die die Geschäftsbeziehung mit der Gegenpartei abgewickelt haben, gehören allfällige private E-Mails dieses Mitarbeiters regelmässig nicht zu den beweisrelevanten E-Mails. Das Unternehmen muss sie bei der Untersuchung schonend aussondern. Dies gilt zumindest in typischen und häufigen Fällen, in denen die Einwilligung der betroffenen Mitarbeiter vorher nicht oder nicht rechtzeitig eingeholt werden kann oder darf (z. B. um die Untersuchung nicht zu vereiteln oder um die Prozessvorbereitung geheim zu halten).

Relevante Postfächer eruieren und kopieren

Im Rahmen interner Untersuchungen ist zunächst zu eruieren, welche Mitarbeiter beweisrelevante E-Mails gesendet oder empfangen haben könnten. Bei kartellrechtlichen Untersuchungen sind dies z. B. diejenigen Mitarbeiter, die am möglicherweise problematischen Informationsaustausch oder an möglicherweise problematischen Treffen mit Konkurrenten teilgenommen haben. Im Zusammenhang mit Zivilprozessen sind es diejenigen Mitarbeiter, die mit der Gegenpartei bzw. dem relevan-

ten Kunden Geschäfte abgewickelt haben. Deren Postfächer muss das Unternehmen kopieren und sichern, damit die Beweiserhebung nicht durch Löschen von E-Mails behindert oder vereitelt wird.

E-Discovery-Software vergisst

Die Durchsuchung erfolgt idealerweise mittels einer E-Discovery-Software. Diese durchsucht die zuvor kopierten elektronischen Archive und Postfächer automatisch. Anders als Menschen «vergisst» die Software, wenn sie auch private E-Mails scannt und diese gar nicht erst in den Suchresultaten aufführt.

Suchbegriffe definieren

Suchbegriffe sind so zu definieren, dass irrelevante E-Mails mit rein persönlichem Inhalt möglichst gar nicht in den Suchresultaten erscheinen. Die Begriffe sind so zu wählen, dass die Suche auf Informationen abzielt, die für die Untersuchung bzw. zur Prozessvorbereitung im konkreten Fall relevant und daher erforderlich sind. Es scheint eher unwahrscheinlich, dass Mitarbeiter in privaten E-Mails Offerten versenden oder sich darüber austauschen, ob der Kunde bereits bezahlt bzw. die Zahlung oder Abnahme der Lieferung verweigert hat. Nicht auf private E-Mails zielen z. B. Stichworte wie «Kaufvertrag», «bezahlt», «geschuldet», «Kunde X», «Verrechnung», «Verzug», «Mängel», «Preis», «Rabatt» oder «Menge». Zudem empfiehlt sich die Eingrenzung der Suche auf E-Mails von und an den relevanten Kunden bzw. die jeweilige Gegenpartei («@companyname.com»). Die Suche beginnt immer mit spezifischen Stichworten. Sie kann anschliessend schrittweise auf allgemeinere Stichworte ausgeweitet werden.

Suche und Triage durch Spezialisten

Das Unternehmen sollte ein Team interner oder externer Spezialisten mit der Durchführung der Suche und einer Triage betrauen. Bei der Triage werden Suchresultate weiter eingegrenzt und noch verbleibende E-Mails (und daran angehängte Dokumente) mit rein persönlichem oder irrelevantem Inhalt ausgesondert. Wenn das Unternehmen (interne oder externe) Spezialisten mit der Triage betraut, hält es einen allfälligen Eingriff in die Privatsphäre betroffener Mitarbeiter möglichst gering. Denn es ist unwahrscheinlich, dass die Spezialisten die betroffenen (Verkaufs-)Mitarbeiter oder andere beteiligte Personen (näher) kennen.

Restriktive Zugangsberechtigungen

Die IT-Systeme, auf denen die elektronischen Dokumente gespeichert und durchsucht werden, muss das Unternehmen mit angemessenen technischen und organisatorischen Massnahmen sichern. Dazu gehört auch, dass Zugangsberechtigungen restriktiv vergeben werden. Die Sicherheitsmassnahmen dienen einerseits dem Schutz der Privatsphäre betroffener Mitarbeiter und Dritter (z. B. eines Whistleblowers). Andererseits dienen sie der Geheimhaltung der Untersuchung bzw. der Prozessvorbereitung.

Dokumentation der Suche und Triage

Das Unternehmen muss dokumentieren, welche Suchbegriffe es verwendet hat und wie die Spezialisten bei der Triage vorgegangen sind. So lässt sich später bei Bedarf nachweisen, dass die Suche auf das Notwendige beschränkt worden und verhältnismässig erfolgt ist – die Privatsphäre betroffener Personen also respektiert und geschützt worden ist.

26 Digitale Arbeitszeiterfassung: Regulatorische Anforderungen und neue Erfassungsmethoden

Nicole Brauchli-Jageneau

Sarah Zurmühle

Seit dem 1. Januar 2016 gelten für Schweizer Unternehmen die angepassten Bestimmungen zur Arbeitszeiterfassung. Obwohl das SECO mit den Änderungen zwei Ausnahmen zur Arbeitszeiterfassungspflicht eingeführt hat, bleibt die strikte Pflicht zur Arbeitszeiterfassung für die Mehrheit der Unternehmen bestehen.

Was wird von den Schweizer Unternehmen genau erwartet? Inwiefern können die gesetzlichen Anforderungen mit neuen technischen Möglichkeiten zur Arbeitszeiterfassung erfüllt werden? Und inwiefern wird der Arbeitgeber bei der Zeiterfassung durch das Datenschutzrecht des Arbeitnehmers eingeschränkt?

Gesetzliche Anforderungen an die Arbeitszeiterfassung

Unter dem Begriff Arbeitszeit wird jene Zeit verstanden, während welcher der Arbeitnehmende sich zur Verfügung des Arbeitgebers halten muss. Gemäss Arbeitsgesetz und der Verordnung 1 zum Arbeitsgesetz hat der Arbeitgeber grundsätzlich von allen Arbeitnehmenden die Arbeitszeit so zu erfassen, dass er jederzeit Rechenschaft darüber ablegen kann, wie viel Arbeit jeder Arbeitnehmende täglich und wöchentlich wann geleistet hat. Aufzuzeichnen sind der Arbeitsanfang und das -ende, aber auch geleistete Überstunden, Ruhetage sowie die täglichen Pausen von mindestens 30 Minuten.

Vom Grundsatz der Zeiterfassung ausgenommen sind nur jene Mitarbeitenden, welche entweder vom Arbeitsgesetz nicht erfasst werden oder welche ein Jahressalär von mindestens 120 000 CHF erhalten und über 50 % ihrer Arbeitszeit frei verfügen können (also während dieser Zeit keine Pflichtanwesenheit haben), sofern dies in einem Gesamtarbeitsvertrag entsprechend geregelt ist. Weiter kann mit der Arbeitnehmervertretung einer Branche vereinbart werden, dass für Mitarbeitende, welche über mindestens 25 % ihrer Arbeitszeit autonom verfügen können, die vereinfachte Arbeitszeiterfassung eingeführt wird. Diese Mitarbeitenden müssen demnach nur noch die Gesamtdauer ihrer täglich geleisteten Arbeitszeit erfassen.

Diese Ausnahmen von der strikten Pflicht zur Arbeitszeiterfassung finden aufgrund der zahlreichen Voraussetzungen in der Praxis jedoch nur auf eine kleine Anzahl von Arbeitnehmenden Anwendung. Laut Bundesratsschätzung dürften weniger als 10 % der Arbeitnehmenden die Auflagen tatsächlich erfüllen. Für den Grossteil der Unternehmen bleibt somit der Grundsatz der Pflicht der Arbeitszeiterfassung bestehen. Es muss davon ausgegangen werden, dass die Einhaltung der Pflicht zur Erfassung der Arbeitszeiten künftig vermehrt geprüft werden wird.

Neue technische Möglichkeiten und die klassische Stempeluhr

Wie die Arbeitszeit durch die Unternehmen erfasst wird, ist den einzelnen Betrieben überlassen. Die Erfassung ist für ein Unternehmen oft mit erheblichem Aufwand verbunden. Eine Erfassung von Hand oder mittels der klassischen Stempeluhr ist heute mit den vermehrt flexibleren Arbeitsmodellen nicht mehr vereinbar. Unternehmen sind deshalb auf der Suche nach geeigneten technischen Möglichkeiten, welche diesen Prozess automatisieren oder zumindest vereinfachen.

Heute sind bereits verschiedene Produkte erhältlich, welche eine digitale Zeiterfassung ermöglichen und eine auf das jeweilige Arbeitsmodell angepasste Lösung bieten. Mittels Software wie bspw. TimeTac können Mitarbeitende die Arbeitszeit via PC oder Mobile-App jederzeit und überall per Mausklick live aufzeichnen. Der Mitarbeitende kann jederzeit sein persönliches Zeitkonto einsehen und die erfassten Stunden überprüfen. Eine ähnliche Dienstleistung bietet auch die Firma Xmatik an, wobei der Kunde hier zwischen manueller und automatisierter Zeiterfassung auswählen kann. Auch für Aussendienstmitarbeitende gibt es spezialisierte Produkte auf dem Markt. Die Firma TomTom bietet unter dem Namen Webfleet ein Zusatzangebot für das Navigationssystem an, womit der Standort von Mitarbeitenden unterwegs geortet und gleichzeitig ihre Arbeitszeit erfasst werden kann. Dank des Ortungsdienstes können zurückgelegte Kilometer ähnlich wie in einem Fahrtenbuch erfasst werden, was ein effizientes Flottenmanagement ermöglicht. Mittels Knopfdruck kann der Benutzer zudem zwischen den Modi «privat» und «geschäftlich» umschalten. Eine flexible und einfache Benutzung unterwegs verspricht auch die Anwendung LogMyTime.

Diese zahlreichen Angebote auf dem Markt illustrieren das grosse Bedürfnis, die regulatorischen Bestimmungen mittels technischer Möglichkeiten effizient umzusetzen. Zu beachten ist in jedem Fall: Auch wenn der Arbeitgeber die Pflicht zur Arbeitszeiterfassung auf die Arbeitnehmenden überträgt, bleibt die Verantwortung beim Arbeitgeber. Die korrekte Umsetzung ist deshalb vom Arbeitgeber laufend zu überprüfen und in einem Reglement zu regeln.

Keine Überwachung des Arbeitnehmenden – worauf beim Einsatz technischer Möglichkeiten zu achten ist

Die Aufzeichnungen der geleisteten Arbeitszeit von Mitarbeitenden stellen Personendaten im Sinne des Datenschutzgesetzes dar. Das Datenschutzrecht beschränkt deshalb die Sammlung und Verarbeitung von Zutritts- und Logdaten mittels technischer Anwendungen: Der Arbeitnehmende muss transparent darüber informiert sein, welche Daten von ihm wie aufgezeichnet werden. Eine ständige, aktive und flächendeckende Überwachung der Arbeitnehmenden wäre offensichtlich unverhältnismässig. Daten dürfen aufgrund des Zweckbindungsprinzips deshalb auch nur zu dem Zweck verwendet werden, für welchen sie gesammelt wurden. Gesetzlich geschützt und damit zulässig ist die Bearbeitung von Daten, soweit sie die Eignung des Arbeitnehmenden für seine Aufgabe betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Die erfassten Daten sind grundsätzlich vertraulicher Natur. Der Arbeitgeber muss sicherstellen, dass diese richtig und aktuell sind und nur soweit erforderlich Dritten zugänglich gemacht werden. Die gewählte Anwendung sollte deshalb sicherstellen, dass Privat- und Arbeitszeit technisch klar auseinandergehalten werden können und keine Daten in der Privatzeit des Arbeitnehmenden erfasst werden. Schliesslich sollte die Speicherung der Daten auf einen sinnvollen Zeitrahmen begrenzt werden.

Volle Fahrt voraus in die digitale Arbeitszeiterfassung

Ein breites Angebot technischer Anwendungen verspricht, die gesetzlich vorgeschriebene Erfassung von Arbeitszeit zu vereinfachen. Während das Arbeitsrecht eine möglichst detaillierte und genaue Arbeitszeiterfassung fordert, wird das Sammeln und Verarbeiten dieser Daten durch das Datenschutzrecht begrenzt. In der Praxis ist es deshalb wichtig, ein Auge auf mögliche Probleme zu haben. Der Arbeitgeber muss den Arbeitnehmenden zwingend über die Datenerfassung informieren und die zur Zeiterfassung gesammelten Daten dürfen nur zum vereinbarten Zweck verwendet werden. Eine aktive und breite Überwachung des Mitarbeitenden mittels elektronischen Stempel- oder Ortungsdiensten ist jedenfalls dann verboten, wenn sie durch den Verwendungszweck nicht mehr gerechtfertigt werden kann.

Steuern

27 Praxisänderung bei der Bewertung von Start-ups

Martin Dubach

Praxisänderung im Kanton Zürich: Seit 1. November 2016 ist für die Bewertung von nicht kotierten Aktien von Start-up-Gesellschaften während der Aufbauphase, d.h. bis zum Vorliegen von repräsentativen Geschäftsergebnissen, der Substanzwert massgebend. Diese neue Praxis verbessert die steuerliche Situation der entsprechenden Aktionäre erheblich.

Bisherige Praxis:
Substanz- *oder* Finanzierungsrundenwert

Für die Vermögenssteuer einer Privatperson ist grundsätzlich der Verkehrswert eines Wertpapiers per 31. Dezember massgebend. Die Ermittlung dieses Verkehrswertes stellt sich jedoch vor allem bei Beteiligungen an Start-ups als nicht ganz einfach heraus – sind diese doch kaum je kotiert und besteht damit kein wirklicher Verkehrswert. Gestützt auf eine entsprechende landesweit gültige Wegleitung bewerteten die schweizerischen Steuerbehörden nicht kotierte Aktien solcher Unternehmen für das Gründungsjahr und während der Zeit der Aufbauphase auf Basis des *Substanzwertes* bzw. – sofern bereits Finanzierungsrunden resp. Kapitalerhöhungen stattgefunden haben – nach ihrem *Finanzierungsrundenwert.* Letzterer repräsentiert den potenziellen Wert, welchen sich die Investoren vom Unternehmen in Zukunft versprechen, mit anderen Worten den erwarteten Cashflow des Unternehmens oder den zukünftigen Verkaufspreis.

Diese Praxis führt zur unbefriedigenden Situation, dass sich Jungunternehmer wegen diesen Bewertungen mit hohen Vermögenssteuern konfrontiert sehen. Hinzu kommt, dass Start-ups in den ersten Jahren kaum je Gewinne schreiben, weshalb die Vermögenssteuerbelastung in keinem Verhältnis zu den Vermögenserträgen aus diesen Beteiligungen steht. Auch ein Verkauf der Aktien kommt faktisch kaum infrage. Nicht zuletzt übersteigt die Vermögenssteuer teilweise das (bewusst tief gehaltene) Einkommen der betreffenden Jungunternehmer. Diese Praxis wird deshalb seit Längerem aus Wirtschaftskreisen als (zu) grosses Hindernis bei der Gründung von Unternehmen kritisiert.

Neue Praxis:
Substanz- *und* Finanzierungsrundenwert

Per 1. November 2016 hat der Kanton Zürich eine Praxisänderung bekannt gegeben, welche *für alle noch nicht veranlagten Steuerjahre gilt.* Mit seiner Praxisänderung schlägt der Kanton Zürich einen neuen Weg bei der Bewertung von Start-ups ein. Er will damit besser auf die wirtschaftlichen Besonderheiten von Start-ups während ihrer Aufbauphase Rücksicht nehmen. Inwieweit andere Kantone nachziehen werden, ist noch offen. Allerdings kennen bereits heute einige Kantone wie z. B. Basel-Stadt eine liberalere Praxis.

Neu bewerten die Steuerbehörden des Kantons Zürich nicht kotierte Aktien von Start-ups zwecks Festlegung des Vermögenssteuerwertes, wie eingangs erwähnt, nur noch nach dem Substanzwert bis repräsentative Geschäftsergebnisse vorliegen.

Bemerkenswert ist die Beschränkung dieser gelockerten Praxis auf sogenannte Start-up-Gesellschaften und deren Definition. So gelten gemäss der Weisung der Finanzdirektion des Kantons Zürich «Kapitalgesellschaften mit einem innovativen (üblicherweise technologiegetriebenen) und skalierbaren Geschäftsmodell, das sich im Aufbau befindet» als Start-ups. Diese Definition trifft für Unternehmen der Biotech- und Medtech-Branche gleichermassen zu wie für solche des IT-Sektors.

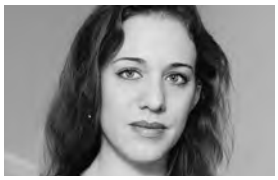
Was mit «repräsentativen Geschäftsergebnissen» gemeint ist, wird die Praxis noch zeigen müssen.

Ein Schritt in die richtige Richtung

Der Kanton Zürich kommt mit seiner Praxisänderung den verschiedentlichen Forderungen aus der Start-up-Szene deutlich entgegen und nähert die Bewertung den tatsächlichen Gegebenheiten von Start-ups an. Dieser Schritt ist insbesondere mit Blick auf die Transparenz im Standortwettbewerb zu begrüssen.

Im Zusammenhang mit der veränderten Praxis empfehlen wir betroffenen Start-ups, ihre Aktionäre über die Praxisänderung in Kenntnis zu setzen und auch bestehende Steuer-Rulings (z. B. betreffend Mitarbeiterbeteiligungen) zu überprüfen sowie gegebenenfalls anzupassen.

28 Steuern und Sozialabgaben beim Online-Verkauf



Beatrice Klaesi

Der Verkauf von Gegenständen übers Internet gehört heute zum Alltag. Nicht nur Unternehmen verkaufen ihre Ware über Online-Portale, sondern auch Privatpersonen nutzen die Möglichkeit, Gegenstände übers Internet zu veräussern – angefangen von Alltags- und Einrichtungsgegenständen, die nicht mehr benötigt werden, bis hin zum Handel mit Waren aller Art wie z. B. Kunstgegenständen, Konzerttickets, aber auch selbst hergestellten Waren.

Ab wann unterliegen solche Verkäufe der Mehrwertsteuer bzw. ab wann der Einkommenssteuer aus selbstständiger Erwerbstätigkeit und wann sind sie Gegenstand der Sozialversicherung?

Die folgenden Ausführungen stützen sich auf die gesetzlichen Regelungen in der Schweiz und es wird nur kurz auf allfällige Abgabepflichten im Ausland eingegangen.

Unternehmerische Tätigkeit

Die schweizerische Steuergesetzgebung verlangt für das Vorliegen einer Mehrwertsteuerpflicht wie auch einer selbstständigen Erwerbstätigkeit, welche Einkommenssteuer und Sozialversicherungsabgaben nach sich zieht, vor allem ein planmässiges auf Gewinnerzielung ausgerichtetes Vorgehen und einen Auftritt nach aussen.

Wer somit sein altes Auto oder andere persönliche Gebrauchsgegenstände, welche er nicht mehr benötigt, übers Internet verkauft, wird nicht abgabepflichtig – weder im Hinblick auf die Mehrwertsteuer noch auf die Einkommenssteuer und Sozialversicherungsabgaben.

Selbst wenn einmalig ein Gegenstand von hohem Wert, z. B. ein geerbtes Kunstgemälde im Wert von 200 000 CHF, verkauft wird, löst dies grundsätzlich keine Steuer- oder Sozialversicherungspflicht aus.

Kritisch wird es, wenn Verkäufe regelmässig stattfinden und dafür auch Waren eingekauft werden. Dabei ist nicht erforderlich, dass ein solcher Handel über längere Zeit aufrechterhalten wird, auch ein kurzzeitiger intensiver Handel mit Waren kann eine Steuerpflicht auslösen. Ebenfalls keine Rolle spielt, ob der Verkäufer diese Tätigkeit haupt- oder nebenberuflich ausübt.

Wer somit Waren übers Internet – z. B. über eBay oder Ricardo – systematisch zusammensucht und sie danach wieder veräussert, riskiert einkommenssteuer- wie auch mehrwertsteuerpflichtig zu werden und Sozialversicherungsabgaben leisten zu müssen.

Auch wer regelmässig selbst Waren herstellt – z. B. Töpferwaren, Taschen etc. – und danach übers Internet veräussert, um damit einen Gewinn zu erzielen, riskiert steuer- und sozialversicherungsabgabepflichtig zu werden.

Im Folgenden werden einige für die Mehrwertsteuer bzw. die Einkommenssteuer und Sozialversicherung relevanten Regelungen dargestellt.

Mehrwertsteuerpflicht

In der Schweiz

Sobald eine unternehmerische Tätigkeit vorliegt und der jährliche Umsatz – der Erlös aus den Verkäufen – mindestens 100 000 CHF beträgt, besteht eine Pflicht, sich im Schweizer Mehrwertsteuerregister eintragen zu lassen und Mehrwertsteuer auf den Umsätzen abzurechnen.

Zur Berechnung der Grenze von 100 000 CHF macht es keinen Unterschied, ob der Gegenstand an einen Empfänger mit (Wohn-)Sitz im In- oder im Ausland

verkauft wird. Mehrwertsteuerlich relevant ist, dass der Gegenstand dem Käufer in der Schweiz übergeben wird (Fall, dass der Käufer den Gegenstand beim Verkäufer abholt, sog. «Abhollieferung») bzw. von der Schweiz aus versandt wird (Fall, dass der Verkäufer den Gegenstand dem Käufer sendet, sog. «Versendungslieferung»).

In der Regel beträgt der Schweizer Mehrwertsteuersatz 8 % und wird auf dem Erlös aus denjenigen Verkäufen erhoben, bei welchen die Ware nicht direkt ins Ausland geliefert wird. Keine Mehrwertsteuer muss folglich auf denjenigen Verkäufen abgerechnet werden, bei welchen der Verkäufer den Gegenstand an den im Ausland ansässigen Käufer sendet.

Zusammenfassend heisst dies für den Verkäufer, dass er in der Schweiz mehrwertsteuerpflichtig wird, sobald er einen Jahresumsatz von mindestens 100 000 CHF aus Verkäufen erzielt, er aber unter Umständen die Mehrwertsteuer auf einem geringeren Umsatz abrechnen muss, da er auf den Verkäufen, bei denen er den Kaufgegenstand direkt an den Käufer ins Ausland versendet, keine Mehrwertsteuer abliefern muss.

Im Ausland

Je nach den gesetzlichen Bestimmungen, die im Ansässigkeitsstaat des Käufers gelten, muss sich der Verkäufer auch in diesem Land (Ausland) als mehrwertsteuerpflichtig registrieren lassen und Mehrwertsteuer entrichten, wenn er Gegenstände an Abnehmer in diesem Staat verkauft. Es ist dabei zu beachten, dass zahlreiche Länder keine oder eine Umsatzgrenze von weniger als 100 000 CHF vorsehen.

Wer somit einen internationalen Warenhandel übers Internet aufbauen will, tut gut daran, sich im Vorfeld über eine allfällige Mehrwertsteuerpflicht in den Ländern zu informieren, in welchen potenzielle Käufer ansässig sind.

Einkommenssteuer und Sozialversicherungsabgaben

In der Schweiz

Im Bereich der Einkommenssteuer und der Sozialversicherungsabgaben besteht keine Untergrenze, sodass, anders als bei der Mehrwertsteuer, der Verkäufer auch dann abgabepflichtig werden kann, wenn sich die jährlichen Erlöse aus den Verkäufen auf unter 100 000 CHF belaufen.

Ist der Verkauf der Waren übers Internet als unternehmerisch und damit als selbstständige Erwerbstätigkeit zu qualifizieren, unterliegt der Erlös aus den Verkäufen abzüglich der damit zusammenhän-

genden Aufwendungen (z. B. Anschaffungskosten der Waren, Transportkosten, Auktionsgebühren etc.) der Einkommenssteuer wie auch den Sozialversicherungsabgaben.

Anders als bei der Mehrwertsteuer fallen Einkommenssteuer und Sozialversicherungsabgaben somit nicht auf dem Umsatz aus den Verkäufen, sondern ‹nur› auf dem entsprechenden Gewinn an. Es unterliegt aber der Gewinn aus allen Verkäufen – unabhängig davon, wo der Käufer ansässig ist und wohin die Ware geliefert wird – der Besteuerung bzw. den Sozialversicherungsabgaben.

Im Ausland

Einkommenssteuer und Sozialversicherungsabgaben sind in der Regel in dem Staat zu leisten, in welchem die entsprechende Tätigkeit ausgeübt wird. Solange somit eine in der Schweiz wohnhafte Person ihren Internethandel von der Schweiz aus ausübt, entsteht weder eine Einkommenssteuernoch eine Sozialversicherungsabgabepflicht im Ausland, selbst wenn die Waren an Empfänger im Ausland geliefert werden.

Fazit

Der Verkauf von Waren übers Internet ist attraktiv, weil er mit einem verhältnismässig geringen Aufwand betrieben und eine grosse Anzahl von potenziellen Käufern erreicht werden kann.

Sobald jedoch nicht nur persönliche Gegenstände, die nicht mehr benötigt werden, verkauft werden, sondern ein eigentlicher Handel betrieben wird, indem systematisch Waren eingekauft und verkauft oder selbst gefertigte Waren angeboten werden, besteht das Risiko – unter Umständen in mehreren Ländern – mehrwertsteuerpflichtig sowie im Land, in welchem die Tätigkeit ausgeübt wird, einkommenssteuer- und sozialversicherungsabgabepflichtig zu werden.

Wer somit beabsichtigt, das Internet in dieser Weise als Verkaufsplattform zu nutzen, ist gut beraten, die rechtliche Situation im Vorfeld gründlich abzuklären, um allfällige Nacherhebungsverfahren und Bussen zu verhindern.

Immobilien

29 Der Grundstückskauf in Zukunft

Dr. Benedict F. Christ, LL.M.

Auch Digitalnomaden benötigen Oasen, um ihre Zelte aufzuschlagen. Diese Oasen sind Grundstücke. Heute wird ein Grundstückskauf meistenorts noch wie im Papierzeitalter abgewickelt. Wie werden wir in der digitalen Zukunft ein Grundstück erwerben?

Archaischer Papierprozess

Im heutigen Grundstücksgeschäft werden zwar elektronische Hilfsmittel verwendet. Im Wesentlichen handelt es sich aber um ein physisches Geschäft mit zahlreichen Medienbrüchen.

Gestützt auf die Instruktionen von Käufer und Verkäufer entwirft ein Notar den Grundstückskaufvertrag. Dazu nimmt er eine Vorlage aus einem früheren, ähnlichen Geschäft und passt sie manuell an das neue Geschäft an. Dieser Vertrag wird ausgedruckt, unterzeichnet, beurkundet, gestempelt, gebunden und dem Grundbuch geschickt. Der Grundbuchbeamte füttert sodann die Angaben aus dem Vertrag in das Grundbuch und schickt den Parteien wiederum in Papierform einen Grundbuchauszug. Für die Zahlungsabwicklung hat die alte Bank vorgängig auf Papier eine Pfandfreigabeerklärung, die neue Bank ein Zahlungsversprechen abgegeben. Für die Zahlungen, die über das Treuhandkonto des Notars laufen, muss jeder Schritt manuell angewiesen werden. Für diese archaische Welt wird das elektronische Grundstücksgeschäft eine Revolution sein.

Immerhin gibt es heute schon den Register-Schuldbrief, eine elektronische Hypothek. Noch sind allerdings die meisten Schuldbriefe als Wertpapiere verbrieft. Diese Wertpapiere müssen aufwendig herumgereicht werden und gehen – zusammen mit dem Pfandanspruch – selbst in den Kellern von Banken immer wieder verloren. Diese Probleme löst der Register-Schuldbrief, der nur als elektronischer Eintrag im Grundbuch besteht.

Elektronische Transaktionsplattform für Grundstücksgeschäfte

Wahrscheinlich schon in naher Zukunft werden Verfügungen über Grundeigentum über eine elektronische Transaktionsplattform erfolgen. Das Standardgeschäft Grundstückskauf wird man sich dabei etwa wie folgt vorstellen müssen.

Wer über sein Grundstück verfügen möchte, lässt sich als Verfügungsberechtigter identifizieren und erhält einen gesicherten Zugang zur Plattform. Der Verfügungsberechtigte kann dann seinerseits den weiteren Beteiligten (Käufer, Banken, Steuerverwaltung, Notar und Anwälten) Zugang zum Dossier geben.

Über die Plattform werden alle für die Transaktion erforderlichen Daten ausgetauscht und eingegeben. Dazu gehören automatisch abgegriffene Grundbuchdaten ebenso wie die Daten zur Finanzierung. Über eine Eingabemaske mit weiterführenden Erläuterungen können die Parteien ganz einfach die spezifischen Elemente des Kaufvertrags und die Modalitäten der Kaufpreisabwicklung festlegen. Aber auch den Austausch und das Verhandeln von komplexen Vertragsentwürfen wird die Plattform unterstützen. Widersprüchliche, unzulässige (etwa Verletzungen der Lex Koller oder der Zweitwohnungsregeln) oder unmögliche Vertragsinhalte erkennt die Plattform automatisch. Sind alle Elemente bereinigt, verhandelt und richtig erfasst, geben alle Beteiligten (einschliesslich Banken, Grundbuch, Steuerverwaltung und Notar) die finale Fassung frei. Damit ist die Transaktion bereit, beurkundet zu werden.

Medienbruch Notar

Trotz elektronischer Plattform werden die Verkäufer und Käufer den Kaufvertrag noch vor einem Notar abschliessen müssen. Denn ohne physische Präsenz beim Notar kann keine öffentliche Urkunde erstellt werden. Die Urkunde selber fertigt der Notar aber als elektronische Urkunde aus.

Zeitgleiche und automatische Abwicklung

Sind die Bedingungen für den Vollzug erfüllt, gibt der Notar die Transaktion elektronisch zum Vollzug frei. Damit werden zeitgleich die einzelnen Transaktionsschritte ausgelöst, die alle elektronisch erfolgen. Dazu gehören insbesondere die Überweisung des Kaufpreises, die Zahlung der Handänderungs- und Grundstücksgewinnsteuern, die Übertragung des Grundstücks samt Eintragung des neuen Eigentümers im Grundbuch sowie die Freigabe der alten Hypothek und deren Übertragung auf die neue Gläubigerbank. Auch in Zukunft könnte es bei einzelnen Schritten aus technischen Gründen zu kurzen Verzögerungen kommen. Das Geschäft ist erst abgeschlossen, wenn alle Schritte erfolgt sind. Ist dies innerhalb einer bestimmten Frist nicht der Fall, lässt die Transaktionsplattform automatisch den ursprünglichen Zustand wieder herstellen.

Stand der Umsetzung

Noch sind wesentliche Teile des elektronischen Grundstückskaufs Vision. Grundsätzlich wäre die elektronische Transaktionsplattform aber schon heute technisch möglich und rechtlich zulässig. So können etwa über die Plattform Terravis (terravis.ch) in gewissen Kantonen mit einzelnen Notaren einfache Grundbuchgeschäfte schon jetzt elektronisch abgewickelt werden. Diese Plattform wird laufend ausgebaut und auf weitere Gebiete ausgedehnt werden. In der Schweiz ist insbesondere das Notariat kantonal geregelt, aber auch für das Grundbuch gelten zusätzlich kantonale Regeln. Darum wird es unterschiedlich lange dauern, bis das elektronische Grundstücksgeschäft überall Realität sein wird.

Virtuelle Beurkundung

Selbst nach Einführung der elektronischen Plattform wird es einen Medienbruch geben, weil die notarielle Beurkundung eine physische Präsenz der Parteien erfordert. Aufgrund der geltenden Regeln zur Beurkundung ist dies nicht anders möglich. Möglicherweise wird aber auch dieser Schritt mittelfristig virtuell werden. Die öffentliche Urkunde soll die Parteien vor unüberlegten Verfügungen schützen. Dazu prüft der Notar, ob die Parteien das Geschäft und dessen Tragweite verstehen und ob das Geschäft ihrem tatsächlichen Willen entspricht. Denkbar wäre, diese Prüfung durch ein elektronisches Verfahren zu ersetzen. Die Identifikation der Parteien könnte ähnlich wie bei einer Online-Kontoeröffnung erfolgen und Übereilung mit einem automatisierten, adaptiven Fragedialog verhindert werden.

Sind elektronische Transaktionsplattform und virtuelle Beurkundung einmal eingeführt, wird somit auch ein Digitalnomade, der wieder sesshaft werden möchte, problemlos von jeder Oase aus ein Grundstück erwerben können.

30 Digitales Bauen: Ersetzt der Computer bald den Bagger?

Dr. Andreas C. Albrecht, LL.M.

Für die Bautätigkeit stehen so viele digitale Instrumente als Unterstützung zur Verfügung, dass bereits ganze Studiengänge zum spezifischen Thema «Digitales Bauen» angeboten werden. Worum geht es dabei?

Ein 3D-Drucker macht noch kein digitales Bauwerk

Der klassische Architekt zeichnete seine Pläne mit Bleistift und Tusche und baute seine Modelle aus Gips. Diese Arbeitsprodukte dienten einerseits dem Bauherrn als Entscheidungsgrundlage und andererseits den Unternehmern als Auftragsbeschrieb.

Seit längerer Zeit werden Bleistift und Tusche kaum noch verwendet. Sie wurden längst ersetzt durch CAD-Programme und Drucker, welche die Vorstellungen des Gestalters präzis und in jeder gewünschten Grösse auf Papier bringen.

Auch Gips wird kaum noch verwendet. Moderne Materialien, die viel einfacher zu verarbeiten sind, sind an die Stelle des weissen Stucks getreten. In jüngster Zeit kommen immer öfter 3D-Drucker zum Einsatz.

Ist das bereits digitales Bauen? Nein! Der Ersatz von Bleistift und Gips durch Drucker und computergesteuerte Modellierungsgeräte hat noch kaum etwas mit dem zu tun, was heute unter digitalem Bauen verstanden wird.

«Building Information Modeling» heisst das Stichwort

Die Idee des digitalen Bauens geht weiter und ist grundsätzlicher. Sie besteht darin, mit einem einzigen Datenmodell zu arbeiten, das sämtliche gestalterischen und technischen Informationen eines Bauwerks in sich vereint. Vom Anfang der Planung bis zur Betriebsphase des Objekts wird derselbe Datensatz verwendet. Dieser beinhaltet zunächst alle Informationen über die physische Gestalt des Baukörpers mit Materialien und Farben. Die Daten umfassen aber auch alle technischen Informationen, etwa zu Leitungen, zu physischen und elektronischen Schnittstellen und zu Heizung, Kühlung, Wasserversorgung und anderen integrierten Systemen.

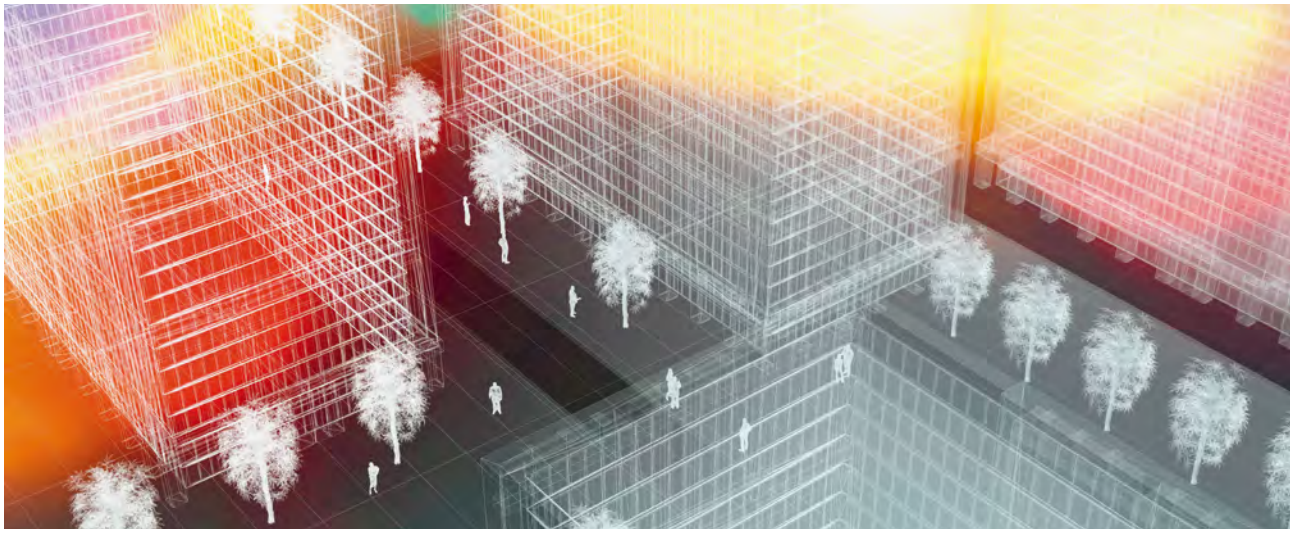
Der Titel, unter dem diese Arbeitsweise entwickelt wird, heisst «Building Information Modeling» oder kurz «BIM». Man spricht auch von «digitalen Gebäudemodellen».

Verantwortungsträger müssen ausgebildet sein

Für die an der Planung und am Bau eines Objekts beteiligten Akteure und auch für die künftigen Betreiber eines Bauwerks ist die Arbeit mit digitalen Gebäudemodellen eine Herausforderung. Um das Potenzial an Effizienz, das in dieser neuen Methodik und den damit verbundenen Technologien verborgen liegt, umfassend nutzen zu können, müssen Arbeitsabläufe vollständig neu gedacht und organisiert werden. Verantwortungs- und Entscheidungsträger müssen ausgebildet sein, um solche Potenziale zu erkennen und die Projektleitung sinnvoll wahrnehmen zu können.

Chancen und Risiken für die Bauherrschaft

Auch für die Bauherrschaft bedeutet «Building Information Modeling» ein neues Zeitalter. Schon in der bautechnischen Klassik war es für die – oft nicht spezifisch baufachlich ausgebildeten – Bauherrenvertreter anspruchsvoll, Pläne und Modelle



genügend zu verstehen, um für die Planer ein qualifiziertes Gegenüber zu sein. Wie oft schon stellte sich ein Objekt nach Fertigstellung anders dar, als es sich der Auftraggeber bei der Besprechung der Pläne vorgestellt hatte.

Digitale Gebäudemodelle bieten auch für die Bauherrschaft Chancen und Risiken. Einerseits können mit einer guten digitalen Datengrundlage verschiedenste Aspekte des Projekts in beliebiger Weise dargestellt werden. Nicht nur die äussere Erscheinung des künftigen Bauwerks, sondern auch Schnittstellen, integrierte Systeme, ökonomische und energetische Kennzahlen und vieles mehr sind viel einfacher zugänglich als mit den klassischen Methoden. Andererseits sind gigantische Datenmengen auch schwieriger zu beherrschen; leicht kann es passieren, dass wesentliche Aspekte übersehen und unwissend mitgenehmigt werden – was nach der Fertigstellung jeweils zu Überraschungen führt.

Vertragswerke müssen auf BIM ausgerichtet sein

Der Zweck und die Funktion digitaler Gebäudemodelle sind nicht grundsätzlich anders als diejenigen von klassischen Plänen und Modellen: Sie dienen sowohl im Verkehr zwischen Bauherr und Planer als auch im Verkehr zwischen Planer und ausführenden Unternehmen als Verständigungsgrundlage. Sie definieren das zu erstellende Bauwerk.

Um in juristisch durchsetzbarer Weise zu gewährleisten, dass ein digitales Gebäudemodell diese Funktionen erfüllt, müssen auch die Verträge zwischen den Akteuren in geeigneter Weise an die neue Methodik angepasst werden. Einige Punkte, die besonderer Beachtung und spezifischer Regelung bedürfen, sind etwa:

- Welcher Standard wird für das Datenmodell verwendet?
- In welcher Weise muss der Planer dem Bauherrn die Gebäudedaten zur Verfügung stellen (im Voraus im Hinblick auf die Genehmigung des Projekts und nach Fertigstellung im Hinblick auf die Nutzungsphase)?
- Über welche Schnittstellenfähigkeiten müssen Fachplaner verfügen? In welcher Weise müssen sie ihre Planungsergebnisse in das Gesamtdatenmodell einarbeiten?
- Wie ist die Verantwortung für den Gesamtdatensatz geregelt, nachdem verschiedene Fachplaner ihre Beiträge dazu geleistet haben?
- Über welche Schnittstellenfähigkeiten müssen ausführende Unternehmer verfügen?
- Wie sind die Aspekte des geistigen Eigentums am Gesamtdatensatz geregelt?

Der Computer wird den Bagger nicht ersetzen. Letztlich ist und bleibt das Bauen eine physisch sichtbare und spürbare Sache. Aber wenn der Computer den Bagger effizient führen soll, dann müssen Bauherren, Planer und Unternehmer entsprechend vorbereitet sein – und so auch deren Rechtsberater.

VISCHER AG

Schützengasse 1 Postfach 5090 CH-8021 Zürich
Tel +41 58 211 34 00 Fax +41 58 211 34 10

Aeschenvorstadt 4 Postfach 526 CH-4010 Basel
Tel +41 58 211 33 00 Fax +41 58 211 33 10

www.vischer.com

11.2016 DE 1000