MME

Legal Due Diligence in der Digital Economy – von der IT Due Diligence zur Digital Due Diligence

Dr. Martin Eckert

Der Kauf von Unternehmen in der Digital Economy erfordert ein vertieftes Verständnis, was die Assets, Werttreiber und Risiken dieser Unternehmen sind. Die herkömmliche IT oder IP Due Diligence genügt nicht mehr. Die Sorgfalt verlangt eine eigentliche «Digital Due Diligence». Dies gilt insbesondere auch für die Legal Due Diligence. Hinter digitalen Geschäftsmodellen lauern erhebliche rechtliche, regulatorische und wirtschaftliche Risiken, die mit einer erweiterten und auf die Geschäftstreiber fokussierten Sorgfaltsprüfung erkannt werden können. Im Vordergrund stehen dabei die Themen Free and Open Source Software (FOSS) und der Umgang mit digitalen Daten.

Die herkömmliche Legal IT und IP Due Diligence deckt vor allem drei Themen ab: Patente, Hardware und Software. Dies ist auch der Ausgangspunkt für digitale Unternehmen, jedoch nicht ausreichend.

Patent Due Diligence

Die Patentierung ist für digitale Technologien erschwert. Software ist in Europa nur ganz eingeschränkt patentierbar (sog. computerimplementierte Erfindungen). Allenfalls ist zu prüfen, ob die Technologie als Business Method geschützt werden kann oder geschützt ist (insbesondere in den USA).

Vielfach verlangt der Käufer eine **Freedom-to-Operate-Analyse** (Ausübungsfreiheit). Er will sicherstellen, dass – insbesondere bei einem künftigen Markteintritt in den USA – der Technologie des zu kaufenden Unternehmens (Targets) nicht Patente oder Business Methoden von Dritten entgegengehalten werden können.

Hardware Due Diligence

Gegenstand der sachlichen Hardware Due Diligence sind der Wert und die Zukunftsfähigkeit der IT Systeme des Targets (Abschreibungsmethode, Investitionsbedarf, Qualität der IT Architektur, Scalability, Agility, Performance, etc.).

Bei der Hardware stehen aus rechtlicher Sicht die Eigentumsverhältnisse im Vordergrund. Dies klingt banal. Im Zeitalter von Cloud Lösungen gibt es aber immer wieder Überraschungen: Die Systeme sind gar nicht im Eigentum des Targets, sondern virtuell in einer Cloud. Der Anspruch des Targets auf IT-Systeme ist also bloss vertraglicher Natur. Die Outsourcing-Verträge sind oft unternehmenskritisch und können zu Abhängigkeiten führen.

Software Due Diligence

Unter Software wird hier der programmierte Code (Quellcode/Source Code) verstanden; nicht aber die digitalen Daten.

Bei der Software Due Diligence ist zwischen eigener und fremder Software zu unterscheiden.

a) Eigene Software des Targets

Die eigene, selbstentwickelte Software ist oft das wertvollste Aktivum von Start-ups in der Digital Economy. Aus rechtlicher Sicht ist zu prüfen, ob das Target wirklich Eigentümer der Software ist und über den Quellcode verfügen kann. Wesentlich ist auch, ob eine saubere Entwicklungsdokumentation erstellt wurde.

Software ist ein Immaterialgut und urheberrechtlich geschützt. Es gibt aber kein Eigentumsregister. Eigentümer des Urheberrechts an Software ist grundsätzlich der Schöpfer, also der Programmierer. Es ist daher zu prüfen, von wem der Quellcode programmiert wurde und ob die Rechte an diesem Code auf das Target übergegangen sind. Hier gibt es zahlreiche Fallstricke, die nur der Spezialist erkennt. Bei den angestellten Programmierern geht das Urheberrecht zwar von Gesetzes wegen auf den Arbeitgeber über, es gibt aber Ausnahmen. Heikel ist es bei Freelancern. Hier braucht es Urheberrechtsübertragungsverträge, die sicherstellen, dass die Urheberrechte vollständig übergegangen sind.

b) Achtung: Free and Open Source Software

Oftmals verwenden Programmierer aus Bequemlichkeit oder Kostengründen sog. Free and Open Source Software (FOSS). Das heisst, sie bauen in den Code Komponenten einer Fremdsoftware ein, die zwar frei zugänglich ist, aber einer speziellen Lizenz unterliegt.

Diese Lizenzbedingungen sind mehr oder weniger einschränkend. Am weitesten verbreitet, aber auch sehr streng ist die GNU General Public License (GNU GPL). Diese verpflichtet den Nutzer dazu, bei Weiterverbreitung der Software in ihrer ursprünglichen oder veränderten Form (sog. abgeleitete Werke), diese ebenfalls unter die Bedingungen der GNU GPL zu stellen (sog. Copyleft-Effekt). Hält sich der Lizenznehmer nicht an die Bedingungen, erlischt die Befugnis zur freien Benutzung rückwirkend. Daher ist der Verwender gehalten den Quellcode zugänglich zu machen und die abgeleitete Software wiederum der GNU GPL zu unterwerfen (sog. «viraler Effekt»).

Werden die Lizenzbedingungen nicht eingehalten, kann durch den viralen Copyleft-Effekt die gesamte proprietäre Software infiziert werden. Schlimmstenfalls steht dann die gesamte Software des Targets unter einer FOSS-Lizenz, sodass ein unter hohem Zeit- und Kostenaufwand entwickeltes Produkt der Allgemeinheit unentgeltlich und quelloffen zur Verfügung gestellt werden muss. Eine wirtschaftliche Verwertung ist damit nahezu ausgeschlossen. Diese Risiken sollten mit einer FOSS Due Diligence (siehe unten) erkannt werden.

c) Fremde Software des Targets

Jedes Unternehmen hat fremde Software im Einsatz. Dadurch können erhebliche Abhängigkeiten entstehen. Die entsprechenden Lizenzverträge sollten im Rahmen der Due Diligence vertieft geprüft werden.

Führende Unternehmen haben ein Software Asset Management System implementiert. Damit soll sichergestellt werden, dass das Unternehmen nicht unterlizenziert ist (Licence Compliance; Gefahr erheblicher Pönalen). Handkehrum besteht auch Einsparpotential bei Überlizenzierungen. Für derartige Lizenzchecks stehen heute Softwaretools zur Verfügung, die auch bei einer Software Due Diligence eingesetzt werden können.

Eine weitere Gefahr ist, dass in Fremdsoftware FOSS-Komponenten eingebaut sind. Wenn nun diese Fremdsoftware mit eigener Software kombiniert wird, kann dies die proprietäre Software infizieren.

FOSS Due Diligence

Der Einsatz von FOSS ist zwar oft effizient und meist gratis, birgt aber hohe Risiken für den Unternehmenskäufer:

- Verlust der Exklusivitätsrechte über die «gekaufte» Software («infizierte» Software)
- Urheberrechtsverletzungen: Wenn das Target FOSS-Komponenten einsetzt und die entsprechenden Lizenzbedingungen nicht einhält, drohen Klagen (Unterlassung; Schadenersatz).
- Security: Die Sicherheit von FOSS-Komponenten ist nicht per se schlechter. Sicherheitslücken sind aber in aller Regel publik. Hacker kennen offene Türen…

Eine FOSS Due Diligence besteht aus zwei Schritten: Zuerst wird die Software des Targets auf FOSS-Komponenten gescannt. Hierzu gibt es Spezialtools (z.B. Black Duck, Palmida, Open Logic) und spezialisierte Anbieter (z.B. BearingPoint). Das Resultat des Scans muss dann juristisch ausgewertet werden (Einhaltung der Lizenzbedingungen). Hierzu bedarf es hochspezialisierten Wissens über die einzelnen strengen (z.B. GNU GPL Licence) und weniger strengen FOSS Lizenzmodelle (z.B. Appache License v2.0). Je nach Resultat sind die Konsequenzen zur beurteilen: Rückstellungsbedarf, Kaufpreisreduktion, Nachbesserungsbedarf, Haftungsfreistellung, Reps and Warranties.

Data Due Diligence

Digitale Geschäftsmodelle beruhen oft auf der Erhebung, Aggregierung und Auswertung von digitalen Daten (z.B. Big Data-Anwendungen).

Auch hier lauern für den Unternehmenskäufer Risiken:

- Eigentum: Gehören die «wertvollen» Daten überhaupt dem Target?
- Compliance: Hält das Target die Vorschriften der – relevanten – Datenschutzgesetzgebung(en) ein? Werden z.B. – verbotenerweise – Daten in die USA übermittelt?
- Aus welcher Quelle stammen die Daten?

Ob es an digitalen Daten überhaupt Eigentum gibt, ist umstritten. Der Autor vertritt die These, dass digitale Daten wie die Elektrizität rechtlich als Sache im Sinne des ZGB behan-

delt werden können. Es ist deshalb auch Eigentum und Besitz an digitalen Daten möglich. Auf jeden Fall sollte sichergestellt werden, dass die Daten nicht Dritten gehören bzw. das Target exklusive/uneingeschränkte Nutzungsrechte hat.

Der Umgang mit Personendaten birgt rechtliche Risiken. Es steht eine Verschärfung der gesetzlichen Vorschriften bevor mit drakonischen Strafen (EU Datenschutzgrundverordnung, ab Mai 2018; Revision des Bundesgesetzes über den Datenschutz).

Auch eine **Data Protection Due Diligence** ist zweistufig. Zuerst erstellen Data Security Spezialisten ein technisches Gutachten (Datenbearbeitungsmodell: Was? Wie? Wo? Assessment Sicherheitskonzept). Dann prüfen die Datenschutzrechtler, wie die Rechtslage ist und ob die gesetzlichen Vorgaben des Datenschutzes für die relevanten Jurisdiktionen eingehalten werden.

Das ganze Prozedere kann weggelassen oder vereinfacht werden, wenn das Target ein ISO-zertifiziertes Datenschutzmanagement implementiert hat und wenn die Produkte selbst (z.B. Apps, Web-Applikationen, Plattformen) ein Datenschutzgütesiegel haben (z.B. www.eprivacy.eu).

Ein immer wichtigeres Thema ist auch, woher das Target seine Daten bezieht (Data Sourcing). Falls die Quellen zweifelhaft sind, kann dies das ganze Geschäftsmodell kontaminieren.

Innovation Protection Due Diligence

Zahlreiche Unternehmen der Digital Economy haben keine immaterialgüterrechtlich geschützten Assets (keine Patente; keine Urheberrechte an Software), sondern basieren auf innovativen Geschäftsideen, wie digital unterstützte Prozesse, Automatisierung, Roboterisierung, Auswertung von Daten, Vernetzung, Internet der Dinge.

Im Rahmen der Innovation Protection Due Diligence stehen dann folgende Themen im Vordergrund: Gibt es sonstigen Schutz (z.B. über originelle Marken, Design)? Können Datenbanken/Datensammlungen Schutz beanspruchen (in der EU/nicht jedoch in der Schweiz)? Sind die Geschäftsgeheimnisse geschützt (gesetzlich; vertraglich; faktisch: effektive Geheimhaltung; Geheimhaltungsvermerke; Eigentumsvermerke; technischer Schutz durch Verschlüsselung/restriktiven Zugriff)? Gibt es Dritte («Ideenlieferanten», Entwickler, Mitwisser, etc.), die Ansprüche erheben könnten? Sind die Rechte an Arbeitsresultaten gesichert? Wie sind die Arbeitsverträge ausgestaltet (Konkurrenzverbote; Geheimhaltungspflichten; IP-Schutzklauseln; Dokumentationspflichten)? Wie sind die Forschungs- und Entwicklungsverträge formuliert? Wie «verwundbar» ist das Unternehmen durch die Konkurrenz? Kann sich das Target gegen Nachahmer schützen? Was sind die Risiken beim Weggang von Schlüsselpersonen? Wie sind das Eigentum und die Nutzungsrechte an Daten geregelt?

Fazit

Die Due Diligence beim Erwerb von Unternehmen der Digital Economy muss besonders sorgfältig und mit spezifischer rechtlicher Fachkenntnis erfolgen. Sonst droht der Erwerb von «heisser Luft».

Ihr Team

Dr. Martin Eckert
Legal Partner, Rechtsanwalt
Head IT/Transaktionsteam

+41 44 254 99 66
martin.eckert@mme.ch