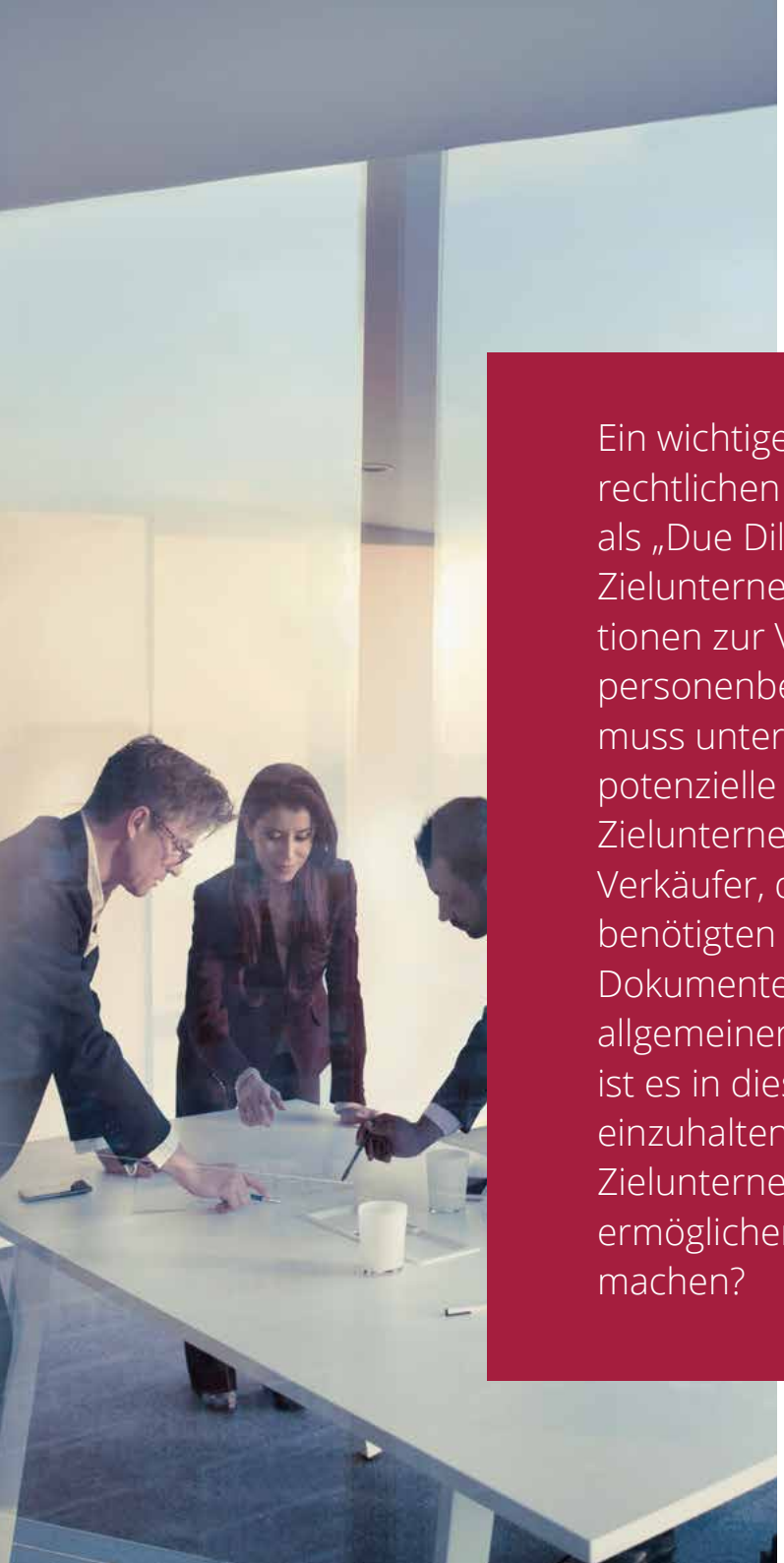
GGV Avocats . Rechtsanwälte

Drooms

DROOMS WHITEPAPER

Umgang mit Datenschutz und Vertraulichkeit in der Due Diligence

drooms.com



Ein wichtiger Schritt bei M&A-Transaktionen ist die Prüfung der finanziellen und rechtlichen Situation des zum Verkauf stehenden Unternehmens, häufig auch als „Due Diligence“ bezeichnet. Im Rahmen dieses Verfahrens stellt das Zielunternehmen dem potenziellen Käufer häufig große Mengen an Informationen zur Verfügung. Das Thema Datenschutz, unter anderem auch der Schutz personenbezogener Daten, steht dabei für alle Beteiligten an erster Stelle und muss unter mehreren Gesichtspunkten betrachtet werden. Zunächst sollten potenzielle Käufer die Einhaltung von Datenschutzgesetzen durch das Zielunternehmen in ihre Analyse aufnehmen. Darüber hinaus muss der Verkäufer, der potenziellen Käufern alle für eine Kosten- und Risikoanalyse benötigten Dokumente bereitstellt, diesen Parteien in den meisten Fällen auch Dokumente und Informationen weiterleiten, die personenbezogene Daten oder allgemeinere vertrauliche Daten und/oder Geschäftsgeheimnisse enthalten. Wie ist es in diesem Kontext jedoch möglich, sowohl die gesetzlichen Anforderungen einzuhalten, die Rechte Dritter nicht zu verletzen und/oder die Interessen des Zielunternehmens zu wahren, und es potenziellen Käufern gleichzeitig zu ermöglichen, sich ein klares Bild des zum Verkauf stehenden Unternehmens zu machen?

Alle wichtigen Fragen

Dazu müssen mehrere Aspekte berücksichtigt werden, zu denen unter anderen auch Folgende gehören:

1. Die Qualifikation der Daten und deren Einteilung in sensible und nicht-sensible Informationen: Werden die Daten unter Einhaltung der Datenschutzgesetze, einschließlich der Datenschutz-Grundverordnung (DSGVO), bereitgestellt? Sind die bereitgestellten Informationen Geschäftsgeheimnisse oder besteht eine Geheimhaltungspflicht (die sich aus den Daten selbst oder einer unterzeichneten Geheimhaltungsvereinbarung ergibt)?

2. Welche technischen und organisatorischen Maßnahmen werden ergriffen, um den Schutz der Daten und ihre Vertraulichkeit zu gewährleisten (ob auf Grundlage von Artikel 5(f), Artikel 24(1) und Artikel 32 DSGVO, gesetzlichen Vorschriften zur Vertraulichkeit von Geschäftsgeheimnissen oder einer Geheimhaltungsvereinbarung, die auch das Zielunternehmen abdeckt)? Folgendes muss sorgfältig durchdacht werden:

- die Auswahl des Hosting-Anbieters, der alle geltenden gesetzlichen Vorschriften erfüllen muss (insbesondere Artikel 28 DSGVO)
- die Anonymisierung oder Pseudonymisierung von Daten
- der Schutz von und die Beschränkung des Zugriffs auf Daten und Informationen auf eine kleine Gruppe entsprechend autorisierter Personen oder Personengruppen unter streng definierten Vorgaben (Verwaltung von Zugriffsrechten, Unterzeichnung von Vertraulichkeitsvereinbarungen mit Sanktionsklauseln für den Fall eines Vertragsbruchs usw.)

Welche Daten sollten besonders aufmerksam behandelt und geschützt werden?

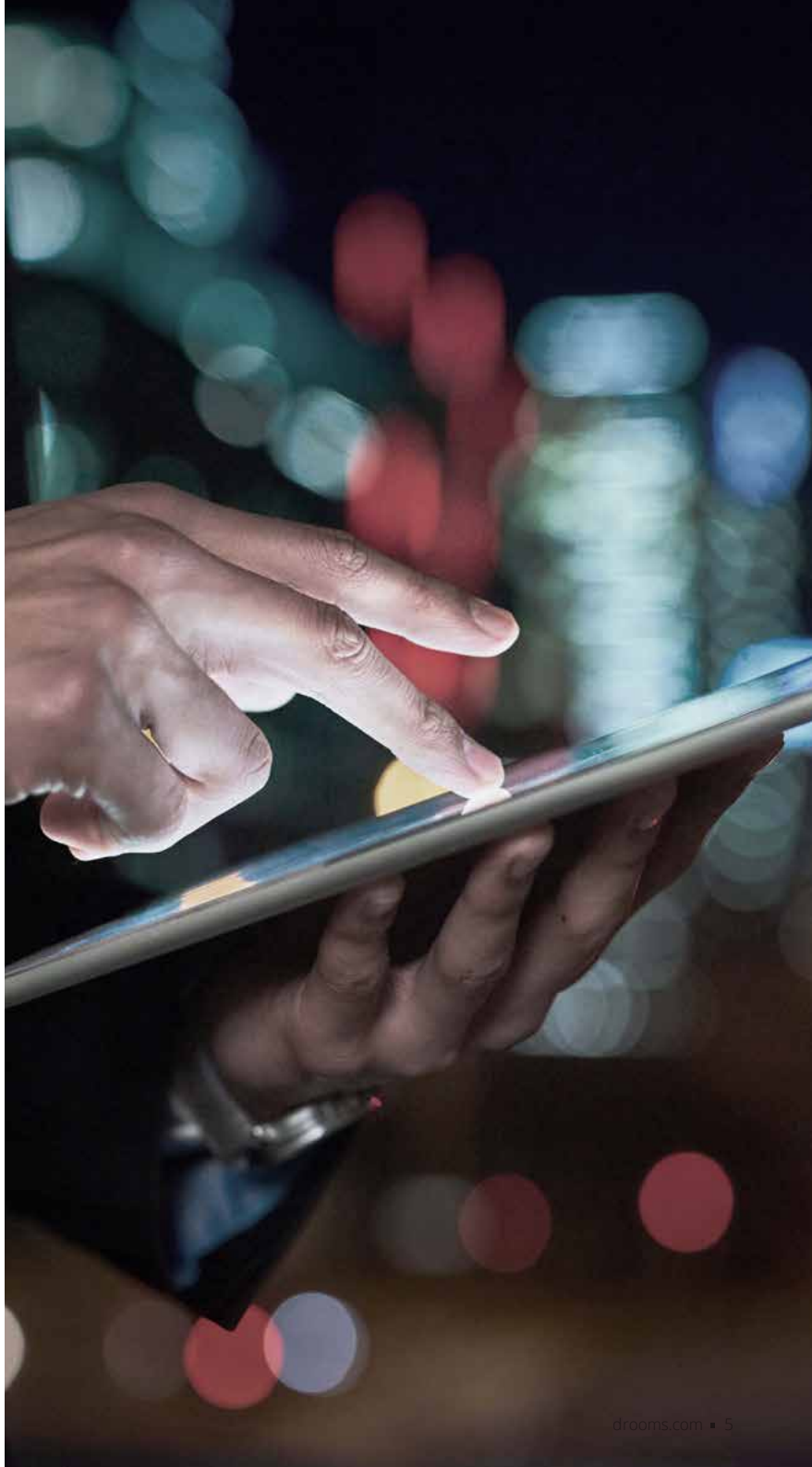
Im Rahmen der Due Diligence werden vom Zielunternehmen meist verschiedene Arten Dokumente und Informationen bereitgestellt. Einige dieser Dokumente oder Informationen enthalten Daten, die aufgrund ihrer Eigenschaften oder des Gesetzes als sensibel oder vertraulich eingestuft werden, oder weil sie zuvor als sensibel oder vertraulich vereinbart wurden. Daten lassen sich in verschiedene Kategorien einordnen. Hier ein paar Beispiele:

a. Von der DSGVO betroffene Daten

Eine der Datenkategorien, denen durch diese Verordnung besonderer Schutz gewährt wird, sind personenbezogene Daten.

Laut DSGVO sind alle Daten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, als personenbezogene Daten einzustufen. Die EU-Verordnung definiert dies wie folgt: „[A]lle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind“ (siehe Artikel 4(a) DSGVO).

Für die Due Diligence bedeutet das, dass folgende Informationen gegenüber potenziellen Kunden offengelegt werden könnten: Daten zu Mitarbeiterinnen und Mitarbeitern, zu Mitarbeitervertretungen, Informationen zum Informationsmanagementteam, Informationen zu Kundinnen und Kunden (insbesondere im Falle von B2C-Unternehmen) usw.



Gemäß EU-Gesetzgebung ist die Verarbeitung von Daten, die als personenbezogene Daten eingestuft werden – insbesondere auch deren Speicherung in der Cloud, ihre Übermittlung über Freigabeplattformen, das Herunterladen usw. –, durch einige Auflagen beschränkt. Sie sind zu Folgendem verpflichtet:

- **Bestimmung der rechtlichen Grundlage für die Datenverarbeitung:** Laut DSGVO ist die Verarbeitung personenbezogener Daten nur dann rechtmäßig, wenn mindestens eine der folgenden Grundlagen zutrifft (siehe Artikel 6 Abs. 1 DSGVO):

  - die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

  - die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Antrag der betroffenen Person erfolgen;

  - die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

  - die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

  - die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;

  - die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Bei den potenziellen Käufern bereitgestellten Daten basiert die Rechtmäßigkeit ihrer Verarbeitung meist auf dem berechtigten Interesse des Datenverantwortlichen (also des Zielunternehmens), das beispielsweise ein berechtigtes Interesse daran hat, einem potenziellen Käufer möglichst vollständige Daten bereitzustellen. Es ist allerdings Aufgabe des Datenverantwortlichen von Fall zu Fall erneut zu prüfen, ob die Verarbeitung der entsprechenden Daten rechtmäßig ist.

- **Einhaltung des Prinzips der Datenminimierung:** Der Datenverantwortliche darf Daten nur in angemessener und relevanter Weise verarbeiten und muss diese Verarbeitung auf das unbedingt notwendige Mindestmaß für den jeweiligen Verarbeitungszweck beschränken (siehe Artikel 5 DSGVO). Daraus folgt, dass Daten nur dann verarbeitet werden sollten, wenn der Zweck dieser Verarbeitung nicht durch andere Mittel erfüllt werden kann (siehe Erwägungsgrund 39 DSGVO).

Für die Due Diligence bedeutet das, dass nur Daten weitergegeben werden dürfen, die für die Fusion oder Übernahme zwingend benötigt werden. Außerdem dürfen diese Daten nur dann gespeichert und weitergegeben werden, wenn sie dem Zweck dienen, dem potenziellen Käufer ein möglichst umfassendes Bild des Zielunternehmens zu vermitteln. Könnten solche Informationen aber auch ohne personenbezogene Daten bereitgestellt werden – beispielsweise, indem sie zuvor anonymisiert wurden –, ist diese Lösung stets anderen Optionen vorzuziehen.

- **Datenintegrität und -schutz:** Personenbezogene Daten dürfen nur so verarbeitet werden, dass sie jederzeit entsprechend geschützt sind – unter anderem auch vor unbefugter oder unrechtmäßiger Verarbeitung sowie unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung. Hierzu müssen geeignete technische und organisatorische Maßnahmen ergriffen werden (siehe Artikel 5 DSGVO).

Im Rahmen der Due Diligence bedeutet das, dass das Zielunternehmen nur Dienstanbieter auswählen darf, die Daten zuverlässig schützen. Zudem liegt es in der Verantwortung des Zielunternehmens, sicherzustellen, dass die Informationen nur an eine kleine Zahl Personen weitergegeben wird, die sich ihrer Verpflichtung zum Schutz dieser Daten bewusst sind. Zu guter Letzt muss außerdem eine Datenspeicherungsrichtlinie implementiert werden, die gewährleistet, dass nicht mehr benötigte Daten gelöscht werden.

Beachten Sie, dass sowohl das Zielunternehmen als auch potenzielle Käufer, die diese Dokumente nach dem Hochladen in die Cloud verarbeiten (z. B. durch Herunterladen und Speichern, Übermittlung an Mitarbeiterinnen und Mitarbeiter und/oder für die Analyse verantwortliche Beraterinnen und Berater, durch interne Analyse usw.), zum Schutz der Daten verpflichtet sind. Zudem muss für jeden Verarbeitungsschritt eine rechtliche Grundlage vorhanden sein.

b. Als Geschäftsgeheimnisse klassifizierte Daten und Informationen

2016 trat eine europäische Richtlinie zum Schutz von Geschäftsgeheimnissen in Kraft, die Innovationen und strategische Informationen wahren soll. Ziel dieser Richtlinie ist der Schutz von Know-how und vertraulichen Geschäftsinformationen vor unrechtmäßigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

Am 8. Juni 2016 wurde die Richtlinie 2016/943/EU für den Schutz von Geschäftsgeheimnissen in Artikel L 151 des französischen Handelsgesetzbuchs in französisches Recht umgesetzt. In diesem Artikel werden Geschäftsgeheimnisse sowie die Voraussetzungen dafür, wann Informationen als Geschäftsgeheimnisse gelten, näher definiert:

- „Alle Informationen, die die folgenden Kriterien erfüllen, werden als Geschäftsgeheimnisse geschützt:

  1°Die Informationen sind nicht selbst oder in ihrer genauen Konfiguration oder Zusammensetzung öffentlich bekannt oder für Personen, die aufgrund ihrer beruflichen Tätigkeit mit solchen Informationen vertraut sind, einfach zugänglich.

  2° Die Informationen besitzen aufgrund ihrer geheimen Natur tatsächlichen oder potenziellen unternehmerischen Wert.

  3° Die Informationen werden vom legitimen Inhaber unter Berücksichtigung der Umstände und ihrer Sensibilität angemessen geschützt.

Informationen, die diese Voraussetzungen erfüllen, gelten als schützenswert. Das bedeutet, dass insbesondere der Inhaber solcher Informationen die Verbreitung oder Nutzung durch Dritte verhindern oder beschränken darf und Rechtsverletzer rechtlich verfolgen lassen darf.

Als Ausnahme für diesen Schutz führt das der EU-Richtlinie folgende französische Gesetz auf, dass gerichtliche Instanzen oder Verwaltungsbehörden Zugriff auf Informationen fordern dürfen, die als Geschäftsgeheimnisse gelten.

Auf der anderen Seite ist es aber nicht möglich, sich auf den Schutz von Geschäftsgeheimnissen zu berufen, wenn die Informationen „zur Aufdeckung einer rechtswidrigen Handlung oder eines anderen Fehlverhaltens, wenn die das Geschäftsgeheimnis erlangende, nutzende oder offenlegende Person in der Absicht handelt, das allgemeine öffentliche Interesse zu schützen“, offengelegt wurden.

Außerdem ist es möglich, dass als Geschäftsgeheimnisse eingestufte Informationen durch Ausübung des Rechts auf Information und Beratung von Mitarbeiterinnen oder Mitarbeitern oder deren Vertretung erlangt werden.

Zu unter die Kategorie „Geschäftsgeheimnisse“ fallenden Informationen gehören unter anderem Know-how, technologische oder technische Kenntnisse und Geschäftsdaten.

Für die Due Diligence bedeutet das, dass die Partei, die die oben stehenden Definitionen erfüllende Informationen verwaltet, selbst entscheiden kann, ob die Offenlegung gegenüber einem potenziellen Käufer notwendig ist und wann „angemessene Schutzmaßnahmen“ ergriffen werden sollten, damit die Informationen weiterhin unter den Geltungsbereich von Artikel I. 151 des französischen Handelsgesetzbuchs fallen.

Im Juni 2016 wurde die EU-Richtlinie 2016/943/EU in Deutschland in Form des „Gesetzes zum Schutz von Geschäftsgeheimnissen“ (GeschGehG) umgesetzt, das vom legitimen Inhaber des Geschäftsgeheimnisses fordert, proaktiv zu handeln, um seinen Schutz durch das Gesetz gewährleisten zu können. Im Gegensatz zur vorherigen Rechtslage reicht es nun nicht mehr aus, lediglich die Absicht zu verfolgen, Geschäftsgeheimnisse zu wahren. Tatsächlich gelten Informationen nur dann als Geschäftsgeheimnisse und profitieren von deren besonderem gesetzlichen Schutz, wenn ihre Offenlegung aktiv durch effektive Präventionsmaßnahmen verhindert wird.

Ergreift der legitime Inhaber der Geschäftsgeheimnisse keine solchen Maßnahmen, sind die betroffenen Informationen nicht nur für Personen außerhalb des Kreises der Eingeweihten zugänglich, sondern werden auch nicht mehr gesetzlich als Geschäftsgeheimnisse geschützt. Deshalb wird wärmstens empfohlen, ein Konzept für die Klassifizierung von

Geschäftsgeheimnissen zu erarbeiten und im Rahmen der Due Diligence anzuwenden. Prozesse, die diese neuen Anforderungen erfüllen, schützen einerseits den Datenübermittler, der ein berechtigtes Interesse daran hat, potenzielle Geschäftsgeheimnisse des Zielunternehmens nicht problemlos zugänglich zu machen, und andererseits auch den potenziellen Käufer vor der Haftung für die Offenlegung dieser Informationen.

Damit dies nicht geschieht, sollten Kundendatenbanken, innovative Ideen, technische Zeichnungen und andere Geschäftsgeheimnisse nur falls notwendig über einen Datenraum bereitgestellt und nur für eine beschränkte Personengruppe zugänglich gemacht werden. Die entsprechenden Daten müssen eigens als vertraulich ausgewiesen und, falls notwendig, durch Verschlüsselung geschützt sein.

Damit der Inhaber der Geschäftsgeheimnisse zudem in der Lage ist zu dokumentieren, dass angemessene Schritte für den proaktiven Schutz der Daten unternommen wurden, müssen alle an der Due Diligence Beteiligten unter den Geltungsbereich einer Geheimhaltungsvereinbarung fallen. Außerdem sollte nur eine beschränkte Personengruppe Zugriff auf die entsprechenden Informationen erhalten.

c. Daten und Informationen, die durch eine Geheimhaltungsvereinbarung geschützt werden, deren Vertragspartei das Zielunternehmen ist

Unter Umständen hat das Zielunternehmen im Laufe seines Geschäftsbetriebs Informationen von Dritten erhalten und diesen Dritten die Vertraulichkeit dieser Daten zugesichert.

Bei Abschluss solcher uni- oder bilateraler Geheimhaltungsvereinbarungen willigen die Vertragsparteien meist ein, dass sie die von der Vereinbarung abgedeckten Daten vertraulich behandeln. Dies impliziert im Allgemeinen, dass diese Daten ohne ausdrückliche Zustimmung der anderen Vertragspartei nicht gegenüber Dritten offengelegt werden dürfen.

In den meisten Rechtssystemen darf der Bruch von Vertragspflichten oder -forderungen bestraft werden.

Deshalb muss das Zielunternehmen im Fall einer Übernahme noch vor der Freigabe seiner Daten prüfen, ob es über diese frei verfügen darf oder ob sie durch eine Geheimhaltungsvereinbarung geschützt werden.

d. Alle anderen Daten und Informationen des Zielunternehmens, die anderweitig geschützt werden (z. B. Daten mit Bezug zu Arbeitgeber-/Arbeitnehmer-beziehungen, geistiges Eigentum, Patente usw.)

Einige Daten gelten aufgrund ihrer Eigenschaften automatisch als vertraulich, ohne dass sie als Geschäftsgeheimnisse eingestuft werden. Hierunter fallen unter anderem die dem Betriebsrat im Rahmen der Suche nach einem Käufer bereitgestellten Daten, wenn die Schließung eines Standorts erwägt wird (Artikel L1233-57-15 des französischen Arbeitsgesetzbuches).

Diese Informationen dürfen auch im Rahmen der Due Diligence weitergegeben werden.

Die wachsende Bedrohung durch Datenlecks

Nur wenige Unternehmen sind auf Verletzungen der Datensicherheit vorbereitet und rechnen damit, Opfer eines Sicherheitsvorfalls zu werden, bevor es zu spät ist und ihre Systeme und/oder Daten bereits gefährdet wurden. Laut aktuellen Zahlen eines führenden Anbieters für Cyberrisiko- und Datenschutzmanagementlösungen, IT Governance, wurden zwischen Januar und Juni 2021 729 Sicherheits-vorfälle gemeldet, wodurch weltweit 3.947.030.094 Datensätze offengelegt wurden. Wie verhält sich das nun im Vergleich zu den Vorjahren?

Die Daten zeigen, dass die Anzahl der Einzelvorfälle zwar zunimmt, aber durch sie immer weniger Individuen betroffen sind. In der ersten Hälfte des Jahres 2021 waren 118,6 Millionen Menschen von Sicherheitsvorfällen betroffen. Das waren deutlich weniger als die sage und schreibe 2,5 Milliarden Opfer, die 2016 verzeichnet wurden. Laut Identity Theft Resource Center (ITRC) lässt sich das durch die veränderten Ansätze von Cyberkriminellen erklären, die sich größere Ransomware-Zahlungen sichern möchten, indem sie schlecht ausgestattete Firmen und Kriminelle angreifen. Besonders in der Fertigung und im Sektor der professionellen Dienstleistungen haben digitale Bedrohungen stark zugenommen, während die Angriffe auf den Einzelhandel beispielsweise abnahmen.

Das ITRC und das US-Gesundheitsministerium berichteten, dass mehr als 98,2 Millionen Menschen von den zehn größten Datenlecks in der ersten Hälfte des Jahres 2021 betroffen waren.

Nach dem Angriff auf die Server der Infinity Insurance Company im Dezember 2020 waren Daten von 5,72 Millionen Menschen betroffen, unter anderen auch die aktueller und ehemaliger Mitarbeiterinnen und Mitarbeiter. Zu diesen Daten zählten unter anderem Führerscheinnummern und Sozialversicherungsdaten sowie die Krankengeschichte der Mitarbeiterinnen und Mitarbeiter.

Eine der beliebtesten Fitness-Apps, Jetfit, wurde im März 2021 Opfer eines Cyberangriffs, von dem mehr als 9 Millionen vor September 2020 registrierte Konten betroffen waren. Zu den

personenbezogenen Daten, auf die zugegriffen wurde, zählten unter anderem E-Mail- und IP-Adressen sowie Passwortinformationen.

ParkMobile, ein Unternehmen, das elektronische und digitale Parklösungen anbietet, wurde ebenfalls Opfer eines Datenlecks, das durch die Verwendung von Drittanbieter-Software im eigenen Haus entstand. Im März 2021 wurde der Vorfall bemerkt, der 21 Millionen Personen betraf, auf deren Daten (wie Telefonnummern, E-Mail-Adressen und Nummernschilder) unrechtmäßig zugegriffen wurde.

Eines haben wir gelernt: Jedes Unternehmen kann, unabhängig von seiner Größe, betroffen sein – sogar Technologieriesen. Zum Beispiel erlitt Facebook ein weiteres Datenleck, obwohl das Unternehmen noch versuchte, ein Leck aus dem dritten Quartal 2019 zu beheben. Unglaubliche 533 Millionen Benutzerinnen und Benutzer aus 106 Ländern waren betroffen. Bei den meisten von ihnen wurden Telefon-nummern, Benutzer-IDs, Kontoerstellungsdatum, Lebenslauf, Geburtsdatum, vollständiger Name, vergangene Standortdaten und Beziehungsstatus von den Servern gestohlen.

Im April 2021 wurde auch Apple zur Zielscheibe. Der angeblich vom russischen Hackerkollektiv REvil durchgeführte Ransomware-Angriff, bei dem 50 Millionen US-Dollar Lösegeld gefordert wurden, führte zum Diebstahl von technischen und Fertigungsplänen des Partners Quanta, von denen einige inzwischen online veröffentlicht wurden.

Benutzerinnen und Benutzer des privaten Fintech-Unternehmens Klarna meldeten im Mai 2021, dass sie aus ihrem eigenen Konto ab- und in anderen Konten angemeldet wurden, wo sie auf die privaten Daten anderer Kundinnen und Kunden zugreifen konnten – einschließlich Bankkartendaten und Postanschrift. Wie viele Personen von diesem Vorfall betroffen waren, lässt sich noch nicht genau beziffern.

Am 14. Mai 2021 wurden der irischen Gesundheitsbehörde The Health Service Executive (HSE) 700 MB Patientendaten gestohlen, die von den Hackern teilweise veröffentlicht wurden. Seither verlangten die Cyberkriminellen mehr als 20 Millionen US-Dollar, um die Online-Veröffentlichung weiterer Patientenakten einzustellen. Die Behörde muss nun ein Bußgeld entrichten und sieht sich mit potenziellen Klagen der Opfer konfrontiert.

Der Hackerangriff auf Microsoft Exchange schien auf den ersten Blick hauptsächlich Großkonzerne und Regierungsbehörden zum Ziel zu haben, war aber tatsächlich ein Angriff auf Unternehmen aller Größen und Branchen. Laut Volexity – der Sicherheitsfirma, die das Problem aufdeckte – weitete sich der Angriff plötzlich explosionsartig aus und traf auch viele schlecht vorbereitete kleine und mittelständische Unternehmen.

Morgan Stanley, eine US-amerikanische, international agierende Investmentbank und Finanzdienstleister, war im Mai 2021 in ein Sicherheitsleck verwickelt, der die vom

Wartungsdienstleister Guidehouse gespeicherten Kundendaten betraf. Personenbezogene Daten wie Adressen, Namen, Sozialversicherungsnummern und Geburtsdaten wurden gestohlen.

Im Juni 2021 wurde gemeldet, dass Daten von 92 % der Benutzerinnen und Benutzer von LinkedIn zum Verkauf stünden. Laut der VPN-Reviewseite Privacy Sharks wurden 700 Millionen Datensätze in einem Hackerforum gefunden. Die beruflich orientierte Netzwerkplattform bestritt jedoch, dass Namen, E-Mail-Adressen und Telefonnummern gestohlen worden waren.

Eines der bekanntesten Unternehmen, die Opfer eines Sicherheitsvorfalls wurden, der 3,3 Millionen Menschen in den USA und Kanada betraf, war die Volkswagen Group of America. Laut Informationen, die die Unternehmensgruppe im Juni 2021 veröffentlichte, kaufte ein Dritter über einen Anbieter, der von anderen Autoherstellern und -verkäufern wie Audi verwendet wird, Daten zu Vertriebs- und Marketingzwecken. Unter den betroffenen bestehenden und potenziellen Kundinnen und Kunden befanden sich 90.000 Menschen, deren sensible Daten gestohlen wurden (darunter auch Führerscheinnummern), während von anderen Personen Name, E-Mail-Adresse, Anschrift, Telefonnummer, Geburtsdatum, Sozialversicherungsnummer, Konto- oder Darlehensnummer, Steuernummer und Fahrzeugdaten offengelegt wurden.

Unternehmen leiden unter unzureichender Vorbereitung

Laut Untersuchungen, die das Cybersicherheitsunternehmen FireEye veröffentlichte, sind mehr als die Hälfte aller Organisationen weltweit nicht auf einen Sicherheitsvorfall vorbereitet. In seinem Cyber Trendscape Report 2020, in dem 800 CISOs und leitende Mitarbeiterinnen und Mitarbeiter in Europa, Nordamerika und Asien befragt wurden, gaben erstaunliche 50 % aller CEOs an, ihr Unternehmen sei nicht gut auf den Umgang mit Cybergefahren vorbereitet. Weitere 29 % der Firmen wiesen eine unzureichende Teststrategie auf, die Lücken in ihrer Verteidigung übersah.

Viele der Befragten gaben an zu glauben, Cyberbedrohungen würden in Zukunft immer häufiger und schlimmer werden. Im neuesten jährlich veröffentlichten Bericht zu den Kosten eines Datenlecks, dem „Cost of a Data Breach 2021“, des Ponemon Institute in Zusammenarbeit mit IBM Security, wurde ersichtlich, dass die steigenden Gesamtkosten eines Datenlecks in den vergangenen Monaten unter anderem auf die Homeoffice-Vorschriften nach Ausbruch der Covid-19-Pandemie zurückzuführen waren.

Welche Faktoren tragen zu Datenlecks bei? Neben Schwachstellen im IT-System spielen auch Menschen häufig eine wichtige Rolle.

Große Risiken

Schon ein einziger Cyberangriff kann ein Unternehmen langfristig schädigen. Verlieren Kundinnen und Kunden das Vertrauen in den betroffenen Anbieter, kann es dazu kommen, dass sich die Menschen der Konkurrenz zuwenden. Es ist somit unwahrscheinlicher, dass ein Unternehmen neue Kundinnen und Kunden gewinnen kann. Aber auch die Lieferkette kann betroffen sein und Zulieferer sich nach einem anderen Käufer umsehen. Auch für Investorinnen und Investoren werden betroffene Unternehmen uninteressanter und zu guter Letzt sind auch Gewinnmargen und Aktienpreise negativ betroffen.

Ein von Aon und Pentland veröffentlichter Analysebericht beschäftigte sich mit den Risiken, die das Cyberzeitalter mit sich bringt. Er zeigte, welche extremen Folgen ein Datenleck für Unternehmen haben kann: Einige Firmen berichteten von einer Abnahme ihres Marktwerts von 25 % innerhalb der 12 Monate nach einem Angriff. Ein besonders bekannter Fall ist Yahoo. Das Unternehmen wurde 2013 Opfer eines Angriffs, der den Preis der Unternehmensaktien zum Einsturz brachte und den geschätzten Unternehmenswert drei Jahre später bei Übernahme durch Verizon auf gerade einmal 4,48 Milliarden US-Dollar drückte.

Audit- und Versicherungsriese PricewaterhouseCoopers (PwC) berichtete über anhaltend fehlendes Vertrauen unter befragten Verbraucherinnen und Verbrauchern, von denen 69 % angaben, die von ihnen genutzten Dienstleister seien derzeit nicht auf einen Hackerangriff vorbereitet. Laut der Umfrage von PwC sind 87 % aller Verbraucherinnen und Verbraucher bereit, den Anbieter zu wechseln, falls es zu einem Vorfall kommen sollte.

Das Telekommunikationsunternehmen TalkTalk bekam hiervon eine Kostprobe, als ein 150.000 Kundinnen und Kunden betreffender Hackerangriff dazu führte, dass das Unternehmen 2016 mehr als ein Drittel seines Werts sowie 100.000 Benutzerinnen und Benutzer einbüßte.

Finanzielle Verluste durch Entschädigungen für Kundinnen und Kunden, Reaktion auf Vorfälle, Investitionen in neue Schutzmaßnahmen, Untersuchungen, Ausfallzeiten und Unterbrechung des Geschäftsbetriebs stellen ebenfalls ein großes Risiko für Unternehmen dar, die Opfer von Datenlecks und Sicherheitsvorfällen werden.

Außerdem sollte man keinesfalls unterschätzen, welche Bußgelder und Strafen mit einer Verletzung der DSGVO

einhergehen. Diese können bis zu 4 % des weltweit erwirtschafteten jährlichen Umsatzes oder 20 Millionen Euro betragen, je nachdem, welcher Betrag der höhere ist.

2015 waren es noch 3 Billionen US-Dollar weltweit, die Cyberkriminalität Unternehmen kostete, doch laut Prognosen wird sich dieser Betrag in den kommenden fünf Jahren jährlich um 15 Prozent erhöhen und bis 2025 einen Betrag von 10,5 Billionen US-Dollar jährlich erreichen, so Cybersecurity Ventures.

Auch Klagen durch von Cyberangriffen Betroffene, die eine Entschädigung erwirken möchten, stellen ein großes Risiko für das Überleben eines Unternehmens dar. Besonders in den USA und im Vereinigten Königreich kam es in den vergangenen Jahren zu immer mehr Sammelklagen nach dem Verlust personenbezogener Daten. Mit zunehmender Schwere der Fälle kann nicht damit gerechnet werden, dass sich dieser Trend demnächst umkehren wird. 2017 waren 145 Millionen Menschen weltweit vom Equifax-Datenleck betroffen, in dessen Folge die Wirtschaftsauskunftei alleine an die betroffenen Kundinnen und Kunden aus den USA mehr als 700 Millionen Dollar Entschädigung zahlen musste.

Zu guter Letzt kann der Verlust hochsensibler personenbezogener Daten nach Auftreten eines Sicherheitslecks noch deutlich schlimmere Folgen als eine finanzielle und Rufschädigung nach sich ziehen. Biometrische und genetische Daten, die zur Identifikation einer Person verwendet werden können, sind für Cyberkriminelle unschätzbar wertvoll. Und die Löschung von Krankenakten kann einen wesentlichen negativen Einfluss auf die medizinische Behandlung und somit auf das Leben von Patientinnen und Patienten nehmen.

Mit welchen Maßnahmen können die Datenschutzanforderungen erfüllt werden?

Für personenbezogene Daten wird in Artikel 32 der DSGVO gefordert, dass Datenverantwortliche „geeignete technische und organisatorische Maßnahmen [treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

Ähnliche Maßnahmen sollten oder können auch für den Schutz anderer sensibler und/oder vertraulicher Daten ergriffen werden, die das Zielunternehmen verwaltet.

Auswahl eines Cloud-Dienstleisters

Cloud-Computing lässt sich zwar auf verschiedene Arten einsetzen, Cloudspeicher werden allerdings nach wie vor am liebsten von Unternehmen eingesetzt. Im Gegensatz zu herkömmlichen Speichermethoden werden in Cloudspeichern Daten virtuell auf Servern hinterlegt. Cloudspeicher basieren auf einem On-Demand-Computing-Modell, bei dem für die Freigabe von und den Zugriff auf Daten eine Internetverbindung notwendig ist. Werden Daten in der Cloud, also auf dem Server eines Drittanbieters, gespeichert, können sie über viele verschiedene Geräte sowie von überall auf der Welt aufgerufen werden, solange eine stabile Internetverbindung vorhanden ist. So können Unternehmen schneller und effizienter arbeiten.

Der große Erfolg der Cloud ist größtenteils auf die zahlreichen Vorteile zurückzuführen, die sie bietet – unter anderem größere Sicherheit im Vergleich zu Hardware, die beschädigt werden oder Defekte aufweisen kann.

Doch Cloud-Dienst ist nicht gleich Cloud-Dienst. Es ist daher sehr wichtig, dass bei der Auswahl eines Anbieters sorgfältig vorgegangen wird, da sonst große Risiken aufgrund von Infrastrukturfehlkonfigurationen auftreten können. Für die Dokumentenverwaltung gewinnen virtuelle Datenräume (VDR) immer mehr an Beliebtheit und werden inzwischen häufiger genutzt als allgemeine Dateifreigabedienste. Anbieter dieser allgemeinen Freigabedienste bemühen sich meist darum, die Dateifreigabe möglichst unkompliziert zu gestalten und die Dateien während der ursprünglichen Übermittlung zu schützen. Ein VDR hingegen schützt darüber hinaus auch langfristig vor Veränderung, Verarbeitung und Verlust der Daten, und verfügt außerdem meist über eine große Auswahl zusätzlicher Schutzfunktionen. Ein kurzes Beispiel: 2016 musste Dropbox eingestehen, dass die Kennwörter und E-Mail-Adressen von mehr als 68 Millionen Benutzerinnen und Benutzern bekannt geworden waren. Da Sicherheit bei virtuellen Datenräumen sowohl während als auch nach dem Hochladen an erster Stelle steht, sind Datenlecks bei ihnen deutlich unwahrscheinlicher.

Umgebungen mit virtuellen Datenräumen profitieren darüber hinaus von sicheren Anmeldesystemen, die häufig mit Mehrfaktorauthentifizierung arbeiten. Zudem garantieren sie in den meisten Fällen eine schnelle Sicherung und Wiederherstellung, sodass das Risiko kostenintensiver Ausfallzeiten abnimmt. Benutzerinnen und Benutzer erhalten folgende Vorteile:

- **Kontinuierliche Datenüberwachung** – Sie werden auf Wunsch sofort über ungewöhnliches Verhalten externer oder interner Quellen informiert.
- **Bessere Verschlüsselung** – Dateien lassen sich umfassend verschlüsseln, sodass Daten nur schwer nachverfolgt und entschlüsselt werden können.
- **Umfassendere Compliance** – Daten können gemäß neuesten Richtlinien gespeichert werden, unter anderem auch konform mit der Datenschutz-Grundverordnung (DSGVO).

Die Infrastruktur ist auf mehrere Nutzungsszenarien ausgerichtet und lässt sich individuell konfigurieren. VDRs unterstützen aber nicht nur eine sichere Dateifreigabe und -speicherung, Due Diligence Verfahren und Kommunikation auf Vorstandsebene, sondern sind inzwischen auch zu einer etablierten Plattform für ein effektives Portfoliomanagement geworden. Sie bieten eine Rundumlösung für den gesamten Asset-Lebenszyklus und ermöglichen es Nutzerinnen und Nutzern deshalb, Probleme im Zusammenhang mit Datenlücken und unterschiedlichen Dateiformaten zu lösen.

Wie verarbeitet Drooms über seine Plattform übermittelte Daten? Erfolgt die-se Verarbeitung DSGVO-konform?

› **Wir schützen Daten und Informationen und gewährleisten deren Vertraulichkeit durch Bereitstellung einer Infrastruktur, die alle Anforderungen der Verordnung erfüllt.**

Seit Inkrafttreten EU-Datenschutz-Grundverordnung sind Datenverantwortliche dazu verpflichtet, aktuelle Anbieter zu prüfen und ausschließlich zuverlässige Partner für die Datenverarbeitung auszuwählen. Als vollständig DSGVO-konform arbeitender europäischer Anbieter mit Hauptsitz in Deutschland musste sich Drooms niemals auf riskante Zusatzschutzmaßnahmen wie Modellklauseln berufen. Drooms führt unternehmerische Kernaufgaben und Funktionen, wie beispielsweise Rechnungsstellung, IT, Kundendienst und Hosting, ausschließlich innerhalb der EU durch, um das Risiko zu minimieren. Hosting, Rechnungsstellung und/oder IT-Support werden nicht an Dritte oder Auftragnehmer übergeben, die für Unternehmen meist das größte Risiko eines Datenlecks darstellen. Sämtliche Daten werden auf firmeneigenen, ISO-zertifizierten Servern in Deutschland oder der Schweiz gespeichert, zu denen ausschließlich eigens autorisierte Drooms-Mitarbeiterinnen und -Mitarbeiter zu Wartungszwecken Zugang erhalten. Sämtliche Datenverarbeitungsaktivitäten finden ausschließlich in Deutschland statt. Unseren Schweizer Kundinnen und Kunden bieten wir als Sonderkondition eine Datenspeicherung in der Schweiz an.

Drooms führt außerdem interne Scans auf Sicherheitslücken sowie Penetrationstests durch. Sollte ein Notfall eintreten, wird durch unseren Plan für eine Notfallwiederherstellung gewährleistet, dass die bei uns gespeicherten Daten hiervon nicht betroffen sind. Mit dem „N+1“-Konzept, Datenverschlüsselung auch während ihrer Speicherung und einer sicheren Schutzarchitektur bleiben Ihre Daten bei Drooms stets vertraulich, sicher und jederzeit verfügbar.

Eines der zentralen Anliegen von Drooms ist der Schutz der Daten seiner Kundinnen und Kunden. Aus diesem Grund werden personenbezogene Daten, die Sie in unsere Datenräume hochladen, keinesfalls für künftige Recherchen oder Nutzung für andere Zwecke gespeichert oder analysiert. Selbst für die Rechnungsstellung bewahren wir nur die absolut notwendigen Daten in unserer Datenbank auf, die für die Verarbeitung von Zahlungen zwingend benötigt werden. Damit wir uns besser gegen Cyberangriffe wappnen können, sind alle unsere Mitarbeiterinnen und Mitarbeiter verpflichtet, regelmäßige Sicherheitsschulungen zu besuchen.

Wie verarbeitet Drooms über seine Plattform übermittelte Daten? Erfolgt die-se Verarbeitung DSGVO-konform?

Außerdem bieten wir Tools an, mit deren Hilfe der Zugriff auf Daten und Informationen verwaltet werden kann (unter anderem durch Festlegung von Zugriffsrechten, die Umsetzung einer Datenlöschungsrichtlinie usw.).

Die resilienzbasierte Architektur von Drooms baut auf dem Konzept maximaler Sicherheit auf und umfasst eine große Auswahl an Tools, die für die Zugriffskontrolle eingesetzt werden können. Zu einigen der Datenraumfunktionen, die für sichere Arbeitsprozesse sorgen, gehören:

- IP-Filterung: Sie können den Zugriff auf den Datenraum auf Gruppenniveau beschränken, festgelegt auf bestimmte Geräte mit bestimmten IP-Adressen.
- Mehrfaktorauthentifizierung: Es besteht die Möglichkeit, sich mithilfe eines zusätzlichen, per SMS übermittelten Sicherheitscodes bei Drooms anzumelden.
- Hochmoderne Verschlüsselung: Für besonders umfangreichen Schutz sind Datenübertragungen nur über TLS-Verbindungen mit aktuellsten Verschlüsselungsprotokollen und Chiffren möglich.
- Benutzerrechte und deren Steuerung: Gewähren Sie Rechte für das Prüfen, Drucken und/oder Speichern auf Benutzer- oder Dokumentenebene und machen Sie Gebrauch von dynamischen Wasserzeichen.
- Detaillierte Berichterstellung: Drooms bietet vollständige Aktivitätsberichte für alle Benutzerinnen und Benutzer eines Datenraums an.

Drooms setzt Künstliche Intelligenz (KI) ein, um Arbeitsabläufe zu automatisieren und effizienter zu gestalten. Damit der dem Unternehmen wichtige hohe Sicherheits- und Zuverlässigkeits-standard garantiert werden kann, entwickelte und integrierte Drooms seine Technologien intern und verließ sich dabei nicht auf Angebote von Dritten. Auch Datenschutz und Data Governance sowie eine Kontrolle durch Menschen zählen zu den Kernprinzipien von Drooms. Das bedeutet, dass immer ein Mensch eingebunden wird, um die von der Künstlichen Intelligenz erstellten Vorschläge zu prüfen und eine hohe Qualität der Ergebnisse sowie Verantwortlichkeit zu gewährleisten. Ähnlich berücksichtigt das Unternehmen auch Leitprinzipien für die Entwicklung intelligenter Lösungen, in deren Mittelpunkt Verantwortungsbewusstsein, Erklärbarkeit, Genauigkeit, Verantwortlichkeit und Gerechtigkeit stehen.

Anonymisierung oder Pseudonymisierung von Daten und Informationen

In der DSGVO werden Datenverantwortliche nicht zur Anonymisierung von Daten verpflichtet, doch wird ausdrücklich gefordert, dass diese geschützt werden müssen. Als mögliche Mittel hierfür werden unter anderem Verschlüsselung und Pseudonymisierung angeführt (siehe Artikel 32). Pseudonymisierung bedeutet, dass (personenbezogene) Daten so verarbeitet werden, dass sie ohne zusätzliche Informationen nicht mehr einer bestimmten Person zugeordnet werden können. Anonymisierung hingegen bedeutet, dass Daten gar nicht mehr einer einzelnen Person zugeordnet werden können.

Diese beiden Verfahren, die oft nur schwer voneinander unterscheidbar sind, lassen sich somit durch die Unumkehrbarkeit der auf die Daten angewandten Verarbeitung voneinander abgrenzen. Anonymisierung ist somit ein Vorgang, bei dem (bei richtiger Anwendung) die Rechte der betroffenen Person gewahrt werden, da die Daten dadurch ihren persönlichen Charakter verlieren.

Bevor man sich jedoch für das eine oder andere Verfahren entscheidet, muss bestimmt werden, ob der Vorgang rückgängig gemacht werden können soll oder nicht. Dabei spielen Eigenschaften und Sensibilität dieser Daten eine große Rolle.

Schutz bei Datenzugriff durch Dritte mithilfe von Geheimhaltungsvereinbarungen

Geheimhaltungsvereinbarungen werden meist von der die Daten offenlegenden und der die Daten empfangenden Partei unterzeichnet. Auch der Zugriff auf einen Datenraum kann unter Voraussetzung der Unterzeichnung einer solchen Vereinbarung gewährt werden.

Geheimhaltungsvereinbarungen umfassen meist die folgenden Bestandteile:

- Definition: Zweck dieses Abschnitts ist es, die Geltung der Geheimhaltung von Daten in Bezug auf das von den Parteien erwägte Projekt zu bestimmen.

- Geltungsbereich: Zweck dieses Abschnitts ist es, die Rechte und Pflichten der Vertragsparteien in Bezug auf die vertraulichen Daten zu definieren. Außerdem verpflichten sich die Unterzeichnen-den zur allgemeinen Geheimhaltung der Daten durch alle am Projekt beteiligten Parteien (einschließlich Mitarbeiterinnen und Mitarbeitern, Beraterinnen und Beratern, Vertreterinnen und Vertretern).

- Ausschlüsse: Hier werden allgemein nicht unter den Geltungsbereich der Geheimhaltungsvereinbarung fallende Informationen definiert, (i) die zum Zeitpunkt der Offenlegung bereits öffentlich bekannt waren oder nach Offenlegung auf einem anderen Weg als durch Handlung oder Fahrlässigkeit des Empfängers öffentlich bekannt werden; (ii) bei denen der Empfänger beweisen kann, dass er zum Zeitpunkt der Offenlegung bereits auf legalem Wege in Besitz dieser Informationen gelangt war, diese Informationen nicht jedoch direkt oder indirekt von der offenlegenden Partei bezogen hatte; (iii) die legal von Dritten erhalten wurden, die zur Offenlegung der Daten autorisiert waren; (iv) die unabhängig von den Mitarbeiterinnen und Mitarbeitern des Empfängers entwickelt wurden, ohne sich auf vertrauliche Daten zu beziehen oder zu stützen; (v) die nach schriftlicher Zustimmung der offenlegenden Partei veröffentlicht werden; oder (vi) die von Gesetzes wegen oder aufgrund einer rechtsgültigen Anforderung durch eine Regierungs- oder Justizbehörde, aufgrund einer gerichtlichen Anordnung oder einer gesetzlichen Pflicht offengelegt werden.

- Laufzeit: Wird in der Geheimhaltungsvereinbarung keine Gültigkeitsdauer festgelegt, ist der Vertrag unbeschränkt gültig und eine Partei kann ihn ohne Entschädigung jederzeit kündigen.

- Vertragsende: Die Parteien verpflichten sich dazu, die Informationen nach Ablauf des Vertrags nicht länger zu nutzen und sie zurückzugeben (zulässige Zeiträume und Verfahren hierfür müssen im Vertrag definiert werden).

- Keine Übertragung von Eigentumsrechten: In der Geheimhaltungsvereinbarung wird allgemein angegeben, dass die vertraulichen Informationen Eigentum der jeweiligen Partei bleiben.

- Keine weiteren Verpflichtungen: Meist ist in der Geheimhaltungsvereinbarung festgelegt, dass die Bereitstellung vertraulicher Informationen keine Verpflichtung zur Durchführung des Projekts darstellt, das durch einen separaten Vertrag abgedeckt wird.

- Strafklausel: Für den Fall eines Bruchs der Vertragsbedingungen einer Geheimhaltungsvereinbarung wird meist ein Schadensersatz vereinbart. Es liegt allerdings in der Verantwortung des Opfers, den Schaden und die Höhe der Kosten zu beziffern, was häufig zu Schwierigkeiten führt. Manchmal werden solche Probleme in Geheimhaltungsvereinbarungen von vornherein gelöst, indem die Strafklausel bereits eine Schadensersatzsumme für den Fall des Vertragsbruchs enthält.

- Geltendes Recht und Gerichtsstand: Dieser Abschnitt ist besonders dann wichtig, wenn die Vertragsparteien in unterschiedlichen Ländern ansässig sind.

Neben ihrer Hauptfunktion erfüllt eine allen Benutzerinnen und Benutzern zur Zustimmung vorgelegte Geheimhaltungsvereinbarung häufig auch noch einen weiteren Zweck: Sie macht die Benutzerinnen und Benutzer darauf aufmerksam, dass bestimmte Daten vertraulich und/oder schützenswert sind.

Sobald die Geheimhaltungsvereinbarung unterzeichnet wurde, liegt es in der Verantwortung des Datenempfängers sicherzustellen, dass die in der Vereinbarung erwähnten Pflichten von Mitarbeiterinnen und Mitarbeitern sowie externen Beraterinnen und Beratern eingehalten werden. Dies geschieht mittels Vertraulichkeitsklauseln in Arbeits- oder Serviceverträgen. Zudem muss der Empfänger betriebliche und technische Maßnahmen zum Schutz der Daten ergreifen. Handelt es sich bei den Daten um personenbezogene Daten und wird die Verarbeitung mithilfe von Auftragnehmern im Sinne von Artikel 28 DSGVO durchgeführt, muss mit diesen Anbietern eine Vereinbarung über die Datenverarbeitung geschlossen werden.

All diese Aspekte sollten in die Hände einer fähigen Anwältin oder eines fähigen Anwalts gegeben werden, die bzw. der selbst einer Geheimhaltungspflicht unterliegt, die sich aus dem Verhaltenskodex des Berufsstands ergibt und bei Verletzung strafrechtlich verfolgt wird.

GGV Avocats – Rechtsanwälte ist eine Pariser Anwaltskanzlei, die sich auf grenzübergreifende Verträge spezialisiert.

Mit 20 Anwältinnen und Anwälten und sieben Fachbereichen (M&A-Transaktionen/Gesellschaftsrecht, Arbeitsrecht, Steuerrecht, Immobilienrecht, Handelsrecht, Rechtsstreitigkeiten, Datenschutz/IT/geistiges Eigentum) ist GGV Avocats – Rechtsanwälte dazu in der Lage, Sie bei allen Schritten Ihrer Transaktion zu unterstützen: bei der Verkäufer-Due-Diligence, der Auswahl der für den Upload in den Datenraum erforderlichen Dokumente, der Einrichtung und Strukturierung der Datenrauminhalte, Q&A-Tools, Entwurf und Prüfung von Geheimhaltungsvereinbarungen, Entwurf der entsprechenden Verträge (Anteilskaufverträge, Übertragung von Assets, Fusionen, Investitionsverträge, Gewährleistungen und Haftung, Managementpakete, Gesellschaftervereinbarungen usw.) sowie bei den Verhandlungen selbst bis hin zu Abschluss von Vertrag und Transaktion.

Mitwirkende GGV

Catherine Stary ist Anwältin bei der Pariser Anwaltskammer, CIPP-E zertifiziert und Beraterin bei GGV Avocats Rechtsanwälte. Darüber hinaus ist sie auch als externe Datenschutzbeauftragte tätig. Bei GGV Avocats Rechtsanwälte ist Stary für die Bereiche Datenschutz und IP/IT-Recht zuständig. Hierbei berät und unterstützt sie – insbesondere als externe Datenschutzbeauftragte – verschiedene deutsche Unternehmen bei Aktivitäten in Frankreich.

Caroline Blondel ist Anwältin bei der Pariser Anwaltskammer und Partnerin bei GGV Avocats Rechtsanwälte. Blondel berät internationale Unternehmen bei M&A sowie in gesellschafts- und handelsrechtlichen Fragen, in Bezug auf ihre französischen Tochtergesellschaften.