Die DSGVO als Paradigmenwechsel in der Unternehmensleitung

Dimitrios Karathanassis

Nachdem am 25. Mai 2018 die neue Datenschutzverordnung der EU (DSGVO) in Kraft getreten ist, lassen sich nun zwei Jahre danach erste Schlüsse über die Bedeutung dieses Regelwerks für (Schweizer) Unternehmen ziehen. Obwohl ein Regelwerk der EU, hat die DSGVO zweifellos für viele Schweizer Unternehmen Zusatzkosten verursacht, von der Abklärung einzelner Sachverhalte bis hin zur Revidierung von Datenschutzerklärungen. Absehbar ist jedoch schon bereits nach zwei Jahren, dass die DSGVO immer mehr zu einem Paradigmenwechsel in der Unternehmensleitung und Unternehmensorganisation führt, und zwar nicht nur in Bezug auf den Datenschutz, sondern deutlich tiefgreifender.

Datenschutz im Rahmen von Compliance

Datenschutz fällt heute – immer noch – primär in den Bereich der *Compliance*, und zwar *Compliance* verstanden als Sammelbegriff für sämtliche organisatorische Massnahmen und interne Abläufe in einem Unternehmen zur Verhinderung von Rechtsverstössen sowie zur adäquaten Reaktion auf solche. In diesem Sinne liegt der Fokus beim Datenschutz für Unternehmen in der Aufgabe, die geltenden datenschutzrechtlichen Bestimmungen zu wahren und mögliche Rechtsverstösse zu vermeiden. Um dies zu erreichen stehen verschiedene Mittel zur Verfügung, wie beispielsweise die Erhebung der gesetzlichen Grundlagen, die Ernennung eines betrieblichen Datenschutzbeauftragten, der Erlass von internen Weisungen, die Erhebung der Datensammlungen einschliesslich Konformitätsbeurteilung, die Gewährleistung der Datensicherheit sowie die Schulung der Mitarbeitenden. Allen diesen Massnahmen ist gemein, dass sie präventive Mechanismen darstellen, die im Kern die Verletzung von datenschutzrechtlichen Bestimmungen zu vermeiden suchen. Sie schaffen im Idealfall ein kohärentes unternehmensinternes Regelwerk, das die bestehenden gesetzlichen Normen widerspiegelt – gar oftmals verschärfend übertrifft – und damit für jede einzelne Geschäftshandlung und Transaktion des betroffenen Unternehmens sicherstellt, dass diese gesetzeskonform sind.

Man könnte nun von der Annahme verleitet werden, dass die DSGVO lediglich die Compliance-Abteilungen der betroffenen Unternehmen zusätzlich bemühen und belasten wird. Das dies schon der Fall ist und weiterhin sein wird ist selbsterklärend, weil jede zusätzliche gesetzliche Vorgabe fachliches Knowhow und Ressourcen benötigt, um sie schlussendlich umsetzen zu können. Die DSGVO stellt dabei keine Ausnahme da.

Obgleich die DSGVO jedoch Gesetzescharakter geniesst, vermischen sich in ihr normative und regulatorische Elemente. Normative Elemente, also Gesetze, geben – so vorliegend postuliert –, klassisch einen Rahmen vor, innerhalb welchem man gesetzeskonform handelt und ausserhalb dessen man es eben nicht mehr tut. Regulierung hingegen geht weiter und verlangt bestimmte Verhaltensweisen und die Umsetzung konkreter Massnahmen. Das Bundesgesetz über den Datenschutz (DSG) – vor seiner jetzigen Revision – muss vorwiegend als normatives Element verstanden werden, das im Grunde seit seinem Inkrafttreten im Juli 1993 einen rechtlich verbindlichen Rahmen vorgibt.

Die DSGVO hingegen ist ein Kind ihrer Zeit, in der die Grenze zwischen normativen und regulatorischen Elementen schwindet. Also solche stellt sie den betroffenen Unternehmen nicht nur einen Rahmen vor, innerhalb dessen sie sich gesetzeskonform bewegen können, sondern sieht explizit Anweisungen für bestimmte Verhaltensweisen und konkrete Massnamen für die Unternehmen vor. Man kann die DSGVO deshalb als *regulatorisches Gesetz* aufassen. Es ist daher anzunehmen, dass die DSGVO für den Datenschutz die Änderungen einleiten wird, welche die Gründung der Eidgenössischen Finanzmarktaufsicht (FINMA) für die Finanzinstitute bereithielt

Auswirkung des Datenschutzes auf die Unternehmensstrukturen

Generelle Regulierungen – neben normativen Vorgaben – im Finanzmarktsektor hat es selbstredend schon vor 2009 gegeben, aber nach Aufnahme ihrer Tätigkeit entwickelte sich die FINMA schnell zu einer umfassenden «Regulierungsfabrik». Auf ihr gesetzliches Mandat stützend erliess und erlässt sie fortdauernd Aufsichtsmitteilungen, Rundschreiben, Stellungnahmen und andere Publikationen, oftmals ohne abschliessende Sicherheit für die Adressaten, welche normative Bedeutung diesen zukommt, und übt damit die Regulierung aus. Die immer konkreteren Anweisungen für bestimmte Verhaltensweisen und die zu treffenden Massnamen führten langsam dazu, dass strategische Unternehmensentscheide nicht nur im Hinblick auf den normativen Rahmen gefällt werden, sondern zunehmend (und teilweise inzwischen ausschliesslich) durch die Linse der regulatorischen Vorgaben betrachtet werden.

Es macht einen erheblichen Unterschied, ob von den Finanzintermediären vom Gesetzgeber verlangt wird, bei der Aufnahme von Geschäftsbeziehungen die Vertragspartei aufgrund eines beweiskräftigen Dokumentes [zu] identifizieren (Art. 3 Abs. 1 Geldwäschereigesetz, GwG) oder ob von ihnen von der FINMA verlangt wird, Kriterien zu entwickeln, die auf Geschäftsbeziehungen mit erhöhten Risiken hinweisen (Art. 13 Abs. 1 Geldwäschereiverordnung-FINMA, GwV-FINMA) sowie Kriterien zur Erkennung von Transaktionen mit erhöhten Risiken (Art. 14 Abs. 1 GwV-FINMA) und dabei nicht nur die Kriterien (Art. 14 Abs. 2 GwV-FINMA) aufgelistet werden, sondern auch die Mittel der Abklärung (Art. 16 GwV-FINMA) und der Zeitpunkt der Abklärung (Art. 17 GwV-FINMA). Anders gewendet: es macht einen Unterschied, ob es verboten ist, der Geldwäscherei Vorschub zu leisten oder ob um dieses Ziel zu erreichen, die Finanzintermediäre einen peniblen Katalog mit auszuführenden Massnahmen erhalten.

In Verbindung mit den immer schärferen Strafen, welche Verstösse ahnden, rückte das Einhalten von regulatorischen Vorgaben von den Rechts- und Compliance-Abteilungen der Unternehmen immer mehr in den Vordergrund bei strategischen Grundsatzentscheidungen. Fragen nach den Staaten, in denen investiert wird und nach der Herkunft von Geldern, die man annimmt und weiterleitet, gab es schon vorher, aber die regulatorischen Kosten und die drohenden Strafen, welche diesen Fragestellungen nun anhaftet, verleiht ihnen eine für die Geschäftstätigkeit der Finanzintermediäre sehr relevante, häufig gar existenzielle Bedeutung.

Regulierung geht in diesem Sinne über den gesetzlichen Rahmen hinaus, weil sie einzelne Handlungen der Unternehmen nicht einfach als gesetzeskonform respektive dagegen verstossend qualifiziert, sondern mittelbar (und teilweise sogar unmittelbar) die Strukturen und Funktionsweisen dieser Unternehmen bestimmt, in denen sie konkrete umzusetzende Massnahmen verlangt. Eine Compliance-Abteilung einer Bank aus dem Jahr 2020 dürfte bei vielen Banken im Jahr 1990 Unverständnis hervorgerufen haben.

Im Ergebnis geht (extensive) Regulierung damit über eine Verhaltenssteuerung hinaus und muss deshalb als Strukturgestaltung verstanden werden. Dies bedeutet, dass nunmehr nicht nur

die einzelnen Unternehmenshandlungen, sondern auch die Unternehmensstruktur – über die gesellschafsrechtlichen Bestimmungen hinaus – als solche den regulatorischen Vorgaben entsprechen und genügen muss. Die betroffenen Unternehmen implementieren damit regulatorische Vorgaben nicht nur in den einzelnen Geschäftshandlungen oder Transaktionen, sondern durch eine (teils grundlegende) Umgestaltung ihrer Strukturen. Regulierung und die *Compliance* damit sind somit nicht nur «ein verbindlicher Bestandteil einer guten Unternehmensorganisation», sondern geben zu einem grossen Teil die Unternehmensorganisation selbst vor.

> Im Ergebnis geht (extensive) Regulierung damit über eine Verhaltenssteuerung hinaus und muss deshalb als Strukturgestaltung verstanden werden.

Eine ähnliche Entwicklung dürfte es nun auch nach dem Inkrafttreten der DSGVO geben. Die vielfältigen Pflichten, welche die DSGVO den Unternehmen aufbürdet, hebt den Datenschutz aus der Compliance-Abteilung in die obersten Entscheidungsgremien der Unternehmen. Die Verarbeitung von Personendaten und die Auflagen der DSGVO heften sich nun an strategische Fragen, wie zum Beispiel wo ein Unternehmen investiert oder welche Geschäftszweige es verfolgen will. Wie Müller bereits 2018 richtig bemerkte (G. V. Müller: «Datenschutz heisst Schutz der Privatsphäre», NZZ, 25. Januar 2018), wird Datenschutz, ähnlich wie die *Compliance* mit den regulatorischen Vorgaben der FINMA oder das Einhalten von Umweltstandards, zum wesentlichen Bestandteil des Riskmanagements von Unternehmen. Die Verarbeitung von Personendaten wird somit eine immer zentralere Rolle spielen, wenn es um unternehmerische Entscheidungen geht. Die in Art. 35 DSGVO vorgesehene Datenschutz-Folgenabschätzung macht z.B. deutlich, dass zukünftige Sachverhalte und die Delegation von Verantwortung in unternehmerischen Entscheidungen berücksichtigt werden müssen. Die in Art. 25 DSGVO verlangten Datenschutz durch Technik (*data protection by design*) und datenschutzfreundliche Voreinstellungen (*data protection by default*) erfordern wiederum Massnahmen, die interne Unternehmensstrukturen und verwendete Programme massiv formen und ihnen eine Form geben werden, die den Bestimmungen der DSGVO entsprechen. Das Einsetzen eines Auftragsverarbeiters wird durch Art. 28 Abs. 3 DSGVO, worin die diesbezüglichen Vertragsinhalte bestimmt werden, die davon berührte Vertragsgestaltung nicht nur prägen, sondern grösstenteils vorgeben. Wie ein erster und wohl rudimentärer Massnahmenplan für Unternehmen aussehen kann, beschreibt die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in Deutschland in ihrem *Kurzpapier Nr. 8 Maßnahmenplan „DSGVO» für Unternehmen*. Vorgeschlagen werden dort Massnahmen wie die Anpassung der betroffenen Prozesse und Strukturen, die Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie Dokumentation von Interessenabwägungen, die Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten, die Anpassung der Datenschutzorganisation, die Bestellung eines Datenschutzbeauftragten, die Reaktionsmechanismen auf Datenpannen, die Organisation von Meldepflichten, die Anpassung der Dienstleistungsbeziehungen, die Aufbau der Dokumentation, die Anpassung der IT-Sicherheit und die Anpassung der Betriebsvereinbarungen.

Diese Auflistung gibt einen ersten Hinweis darauf, welchen Herausforderungen sich die betroffenen Unternehmen werden stellen müssen. Das Ausmass der Neuerungen ist zurzeit nicht abschliessend abschätzbar, aber der Umfang der DSGVO, in ihrer deutschen Fassung immerhin 78 Seiten lang, kann als erster Indikator dienen. Diese sind nicht nur kostspielig, sondern greifen mittelbar auch in die primären Geschäftsinteressen der Betroffenen ein. Zählt man dazu noch die Beweislastumkehr, welche in Art. 5 Abs. 2 DSGVO verankert ist und nach der nun eine Rechenschaftspflicht (*accountability*) des Verantwortlichen besteht, «wonach dieser die Einhaltung der allgemeinen Grundsätze (vgl. Art. 5 Abs. 2 DSGVO) aktiv nachweisen können» muss, so wird deutlich, dass eine Anpassung von Unternehmensstrukturen unumgänglich sein wird, um diesen Vorgaben zu genügen.

Gewappnet für diese Entwicklung sind, wie G. V. Müller zu Recht feststellt, am ehesten die Pharma- und Finanzbranche, in der diese Veränderung schon Eingang gefunden hat. Grund dafür ist vor allem die Tatsache, dass die Verarbeitung von personenbezogenen Daten immer mehr in die Geschäftsprozesse von Unternehmen dieser Branchen einfliesst. Pharmaunternehmen, wie auch Banken, gründen einen grossen Teil ihres Geschäfts auf personenbezogene Daten und der mögliche Umgang damit ist mehr eine Frage der strategischen Ausrichtung dieser Unternehmen als der lediglichen Einhaltung von datenschutzrechtlichen Bestimmungen. Gerade jedoch, weil Daten, und dabei insbesondere vor allem Personendaten, der «Rohstoff der Zukunft» sind, werden zunehmend mehr Unternehmen aus diversen Branchen von der DSGVO und anderen Datenschutzgesetzgebungen betroffen sein. Der Umgang damit wird die Unternehmen ähnlich prägen, wie der Umgang mit den ursprünglichen Rohstoffen marktwirtschaftlicher Betätigung Arbeit und Kapital. Begreift man also Personendaten als wertvolle Ressourcen, so ist die Einhaltung ihrer gesetzlichen Schutzbestimmungen essentiell und wirkt sich unmittelbar auf den Umgang und schlussendlich auf den Wert dieser Ressourcen aus. Die DSGVO, regulatorisch tief eingreifend, gibt die ersten Strukturen vor, die sich die betroffenen Unternehmen einverleiben werden müssen, um den unternehmerischen Umgang mit diesen Ressourcen erfolgreich zu bewerkstelligen. Dass die DSGVO zudem territorial nicht begrenzt ist und für jeden Teilnehmer am europäischen Binnenmarkt verpflichtend ist, verleiht ihr auch wirtschaftlich eine hohe Signifikanz.

Die DSGVO, das ist unbestritten, verstärkt den Schutz personenbezogener Daten. Gleichzeitig aber stellt sie die davon betroffenen Unternehmen vor enormen Herausforderungen. Leidtragende der durch die DSGVO bedingten Anpassungen in den Unternehmensabläufen und Unternehmensstrukturen sind dann auch die KMU, welche die Kosten für diese Implementierungen nur schwer stemmen können werden. Die Vorteile eines einheitlichen europäischen Binnenmarktes mit freiem Zugang dazu werden für die KMU durch die DSGVO getrübt. Während die grossen Konzerne diese Anpassungen eher bewältigen und dabei auf die Hilfe von Rechtsanwälten und Beratungsfirmen zurückgreifen können, stellt sich für die KMU erstmal die Frage nach der wirtschaftlichen Tragfähigkeit. Nicht selten dürfte der europäische Absatzmarkt nun an Attraktivität verlieren. Das Feld, man muss es so deutlich sagen, wird den Grossen überlassen. Die Parallelen zur Geldwäschereigesetzgebung, welche durch ihre regulatorischen Vorgaben viele Märkte für kleine und mittlere Banken aus rein auf regulatorischen Vorgaben basierende wirtschaftliche Gründen unattraktiv gemacht hat, sind unübersehbar. Ursprünglich eigentlich hehre Vorsätze, nämlich Transparenz und Datenschutz, alterieren ungewollt zu einem Wettbewerbsvorteil für markt- und finanzstarke Unternehmen.

Festhalten kann man schliesslich, dass Datenschutz, wie zuvor auch die Geldwäschereibestimmungen, als ursprünglich konzipierte Verhaltenskontrollen schleichend den Kern des

Wirtschaftens erreichen und damit mittelbar auch eine liberale und wettbewerbsfreie Wirtschaft gefährden, weil sie die Vielzahl der gesellschaftsrechtlichen Strukturen tangieren. Die Gesellschaftsrechtlichen Unterschiede zwischen einer Kapital- und Personengesellschaft rücken verlieren im Angesicht der für alle gleich geltenden regulatorischen Vorgaben an Gewicht. Ob dies alles im Sinne des Erfinders ist, sei freilich dahingestellt. Niemand bezweifelt, dass die Bekämpfung von Geldwäscherei und die Einhaltung des Datenschutzes essentiell sind, doch bei der Art und Weise, wie man diese Thematiken angeht, dürfen die einzelnen Nebeneffekte nicht ausser Acht gelassen werden. Den Konsumenten ist nicht gedient, wenn ihre Daten zwar sicher, aber nur von wenigen und marktmächtigen Unternehmen gehalten werden können. Die Nachteile des dann schrumpfenden liberalen Wettbewerbs kann eine so gestaltete Datenschutzgesetzgebung jedenfalls nicht korrigieren.