Daten- und Informationsmanagement

Das Gold einer di

Daten, ganz gleich ob mit oder ohne Personenbezug, sind das unverzichtbare Fundament der Digitalisierung von Big Data, Cloud-Computing, Facebook und Co. Ob als Firma, Beauftragter oder Privatperson: Das Sammeln, Auswerten, Nutzen von Daten und Informationen wird immer verlockender und einfacher. Der Schutz sowie der verantwortungsbewusste Umgang hatten mit dieser Entwicklung leider nicht in gleichem Maße Schritt.

Verfolgt man die öffentliche Berichterstattung, rücken sowohl der Umgang mit personenbezogenen Daten wie auch ihr Schutz immer mehr ins Blickfeld. Der Gesetzgeber hat hierfür seit über einem Jahr eine neue Verordnung mit dem vielsagenden Namen „Datenschutz-Grundverordnung" ins Leben gerufen.

Was im Sinne der Sache gut gemeint ist, kommt jedoch längst nicht bei jedermann gut an. Bei unseren Nachbarn in Österreich hat es das Wort Datenschutz-Grundverordnung (DSGVO) sogar zum Unwort des Jahres 2018 geschafft. Begründung: „Dieses Wortungetüm steht für die an sich wichtige Zielsetzung des Schutzes der privaten elektronischen Daten. Seine überaus komplizierte und mit hohem bürokratischen Aufwand verbundene Umsetzung – in Kombination mit der Tatsache, dass die großen internationalen Akteure im Umgang mit Daten von den Regelungen kaum betroffen sind – macht die Sache zu einer Perversion des gut gemeinten Vorhabens und den Begriff damit zu einem Unwort." Demnach wären die Vorgaben der DSGVO kompliziert, deren Umsetzung mit hohem bürokratischem Aufwand verbunden, die Regelungen teilweise nicht relevant (gerade für internationale Akteure) und somit das eigentlich positive Ziel eines wirksamen Datenschutzes pervertiert.

Aber: Selbst wenn uns die Umsetzung so mancher Vorgabe Kopfschmerzen bereitet und uns entsprechend fluchen lässt: Wie sieht die Realität ein Jahr nach Inkrafttreten der DSGVO aus? Wer ist für die operative Umsetzung zum Schutz der Daten verantwortlich? Und wird die der Umsetzung zugrunde liegende Grundhaltung den Zielen des Schutzes von Daten gerecht? Kann auf so einer Grundlage ein effektiver und ernst gemeinter Schutz von Daten stattfinden?

Fluch und Segen

Es lohnt sich, an dieser Stelle einmal kurz innezuhalten und darüber nachzudenken, worum es hier eigentlich geht.

Daten und Informationen sind das Gold des digitalen Zeitalters. Sie sind der Schmierstoff gut laufender Geschäftsmodelle. Korrekte Daten sind der Garant für Zuverlässigkeit und geschäftliche Erfolge. Sowohl kleine Fintechs wie auch große Konzerne sind hinter den Daten von Kunden her wie der Teufel hinter der armen Seele. Daher ist der Schutz von Daten eigentlich das Synonym für das Recht des Einzelnen auf informelle Selbstbestimmung.

Der Schutz von Daten und Informationen bei juristischen Personen ist heute mehr denn je im Zusammenhang mit ihrer korrekten und jederzeitigen Verfügbarkeit sowie der Verhinderung ihrer unlauteren Erlangung zu sehen. Dargelegt sind solche Szenarien in diversen Gesetzen. Bei sogenannten „kritischen Infrastrukturen" des öffentlichen Interesses sind zudem Aufsichtsbehörden und Staaten als „Gatekeeper" aktiv oder treten mittelbar in Erscheinung. Denn schlussendlich kann das Wohl einer ganzen Firma, ihrer Kunden und Mitarbeiter oder aber einer ganzen Bevölkerungsschicht (oder alternativ: eines Staates) gefährdet sein: Wenn Daten missbraucht werden, sie urplötzlich und unwiderruflich nicht mehr für Entscheidungsfindungen zur Verfügung stehen oder ggf. falsch verknüpft werden und in der Folge unzutreffende Analysen mit verhängnisvollen Entscheidungen getroffen werden.

gitalen Welt

Datenschutz bei natürlichen Personen ist sogar im Grundgesetz verankert. Der Schutz unserer Daten ist ein Grundrecht, auf dessen Einhaltung wir alle beharren können, sollen und im Zeitalter fortschreitender Digitalisierungen sogar müssen.

Mehr als ein Kostenfaktor

Warum wird der sich auf den Datenschutz beziehende Aufwand als so bürokratisch und realitätsfern beschrieben? Warum müssen sich Firmen bzw. Datenschützer und Informationssicherheitsbeauftragte für ihre Tätigkeit oder ihren angemessenen Aufwand rechtfertigen?

Liegt es vielleicht daran, dass noch immer kein angemessenes Maß für eine akzeptierte „Best Practice" gefunden wurde? Oder ist es einfach fehlende Konsequenz, dass der Schutz der Daten von vielen Firmen zwar einerseits als in höchstem Maße wichtig und sogar als verkaufsförderndes Marketinginstrument angesehen wird, andererseits aber in der Umsetzungsrealität kaum Beachtung findet, weil der Aufwand schlichtweg als zu teuer und bisweilen unnötig angesehen wird?

Das Ziel von Informationssicherheit und Datenschutz in seiner aktuellen Form ist, den Nachweis tatsächlich wirksamer Maßnahmen zu initiieren. Der Gesetzgeber bzw. die Aufsicht will nachvollziehen können, dass angemessene und wirksame Maßnahmen getroffen wurden. Das ist vor dem Hintergrund der faktischen Risiken und gemachten Erfahrungen nachvollziehbar und durchaus legitim.

Jeder Bürger, dessen Identität oder dessen Bankkonto schon einmal in betrügerischer Weise missbraucht wurde, weiß um die Notwendigkeit wirksamer Schutzmechanismen. Jede Firma, die aufgrund falscher, unvollständiger oder vielleicht sogar gestohlener Daten einen unternehmerischen Schaden hat erleiden müssen, kann den betriebswirtschaftlichen Wert eindeutig beziffern. Somit ist der Schutz von Daten gerade nicht der so oft kolportierte Hemmschuh des Fortschritts digitaler Entwicklungen, sondern im Gegenteil: Er ist die Voraussetzung für einen nachhaltigen digitalen Fortschritt. Ohne wirksamen Schutz von Daten und Informationen in einer Firma kein Vertrauen, ohne Vertrauen in diese Firma kein Geschäft.

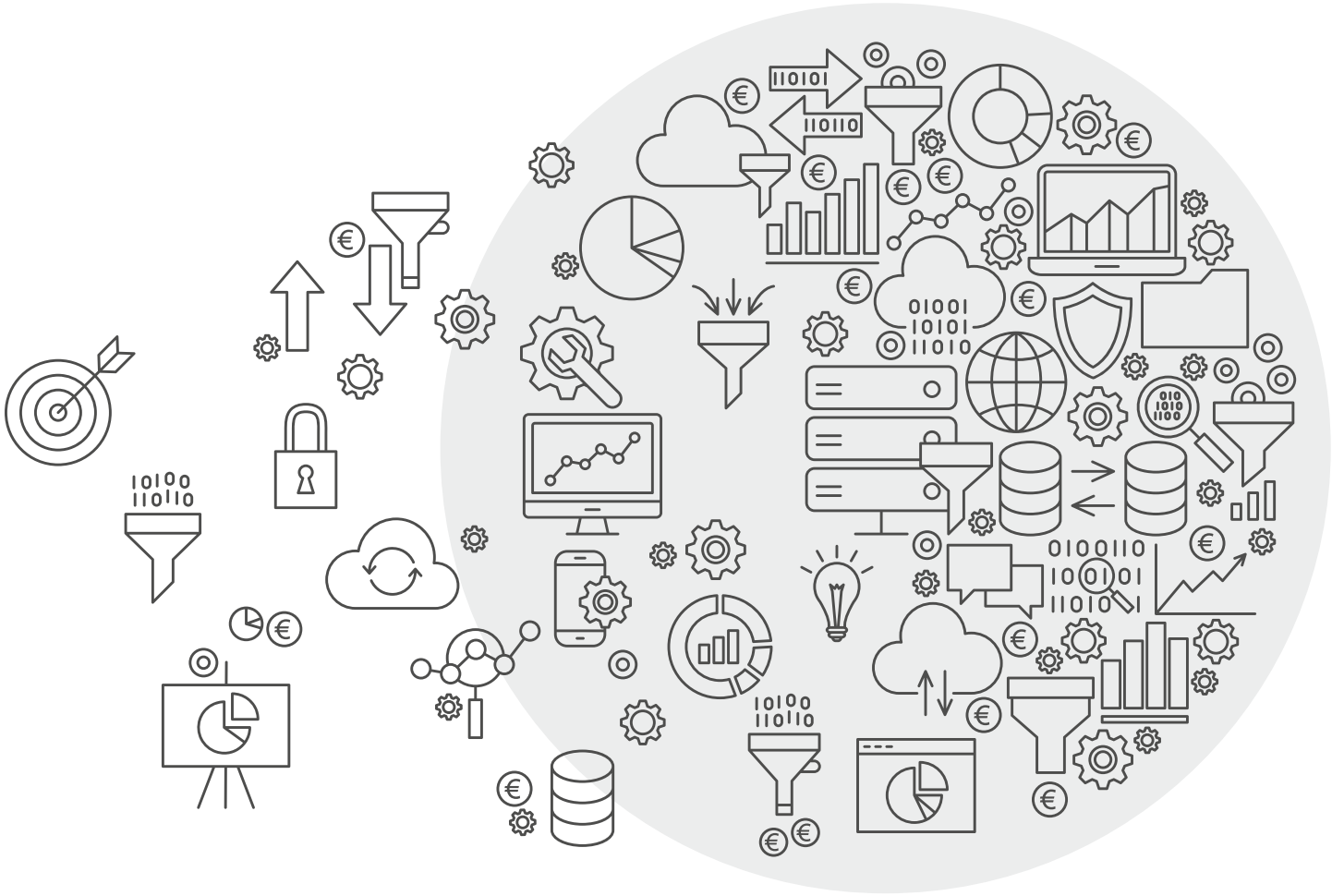
Und gerade deshalb ist es eine große Herausforderung für Beauftragte in ihrer Rolle als Schützer von Informationen und Daten, die Aufwände für diese Aufgaben zu erklären. Sie sind eben nicht als reiner Kostenfaktor zu betrachten. Sie sind vielmehr elementarer Bestandteil erfolgreicher Geschäftsmodelle und als solche glaubwürdig zu integrieren. Immerhin gilt es, wichtige Geschäftsgeheimnisse und den Geschäftsbetrieb der Firma und das Grundrecht der Kunden der Firma gleichermaßen zu schützen. Dies gelingt nur, wenn eine transparente, belastbare Verbindung zwischen regulatorisch und gesetzlich relevanten Informationen und Datenhaushalten, dem entsprechend konformen Umgang damit und den zu ihrer Nutzung vorgesehenen Geschäftsprozessen und Systemen hergestellt werden kann.

Wirksame Daten- und Informationssicherheit

Voraussetzung ist eine Detailtiefe in Bezug auf Abläufe und Prozesse, die schon im Stellenprofil der Beauftragten verankert sein muss. Eine ausschließlich theoretische Betrachtungsweise gesetzlicher Vorgaben wird nur bedingten operativen Erfolg haben. Eine gewisse Begeisterung für die Inhalte und Ziele des Datenschutzes und der Informationssicherheit erhöht die Chancen für pragmatische und zugleich effiziente Lösungen dagegen ungemein. Dies ist im Übrigen auch ein Argument dafür, auf externe Unterstützung zurückzugreifen: Für externe Beauftragte ist der Schutz von Informationen und Daten absolutes Kerngeschäft. Sie machen bei vielen verschiedenen Mandanten nichts anderes und bauen somit ein Qualifikationsprofil auf, das den hohen aufsichtsrechtlichen und gesetzlichen Anforderungen entspricht. Sie „brennen" erfahrungsgemäß auch für ihr Thema. Das kann insbesondere für kleinere und mittlere Häuser interessant werden. Sie verschaffen sich somit einen betriebswirtschaftlich optimierten Zugang zu fachlicher und prozessualer Intelligenz und damit zu einem wirksam(er)en Schutz.

Eine weitere Voraussetzung für eine wirksame Daten- und Informationssicherheit liegt in einem integrativen Ansatz.

Grundlage für die geschäftlichen Operationen der Finanzdienstleistungsbranche ist seit jeher das, was heute die „Schätze des digitalen Zeitalters" sind: die Informationen und Daten >



zu ihren Kunden. Aktualität, Korrektheit, jederzeitige Verfügbarkeit und Schutz gegen „Angriffe“ von außen sind von nachhaltiger Bedeutung, denn:

- Geschäftsmodelle sind nur mit korrekten Daten wirklich erfolgreich.
- Kunden bekommen nur auf Basis korrekter Analysen individuelle und bestmögliche Lösungen angeboten.
- Vertrauen ist das Kernkapital einer gesunden Kunde-Bank-Beziehung: Ein sorgsamer Umgang mit Daten gehört deshalb zu den ersten Pflichten.

Eine der Kernaufgaben des modernen Beauftragtenwesens ist die Absicht, diese vorgenannten Zielsetzungen durch eine nachhaltige Aufgabenerledigung zu erreichen.

Vor dem Hintergrund, dass Daten- und Informationssicherheit heute – ohne Zweifel – elementar für die Bankenbranche ist, ist es nur schwer nachvollziehbar, dass sich Datenschutz- oder Informationssicherheitsbeauftragte für ihre Initiativen und Aufwände rechtfertigen müssen, weil diese den geschäftlichen Erfolg schmälern könnten. Oder anders formuliert: Es ist schlicht kontraproduktiv, wenn immer noch – insbesondere digitale – Geschäftsmodelle ohne die Integration regulatorischer Zielvorgaben gedacht werden und die Regulatorik als „Feindbild“ geschäftlicher Opportunitäten betrachtet wird. Geschäftsmodelle und die Ziele von Regulatorik dürfen sich nicht gegenseitig ausschließen, sondern sind idealerweise als Einheit zu betrachten.

AUTOR UND ANSPRECHPARTNER

Andreas Marbeiter
Geschäftsführung,
E-Mail: andreas.marbeiter@dz-cp.de

Das bedingt, dass die Zielsetzungen der jeweiligen Geschäftsmodelle einerseits und der Regulatorik andererseits pragmatisch und integrativ aufbereitet werden. Dies an sich ist schon eine sehr herausfordernde eigene Exzellenz, die – unter anderem – der Beauftragte ins Unternehmen einbringen muss.
Der Beauftragte benötigt dazu

- fundierte Kenntnisse der rechtlichen Rahmenbedingungen und dessen, was möglich ist,
- professionelle Erfahrung in Bezug auf relevante Arbeitsabläufe im Unternehmen,
- eine nachhaltige Expertise in Bezug auf prozessuale Ausgestaltungen sowie
- eine klare Lösungsorientierung.

Idealerweise liefert ihm die Organisation, in der er arbeitet, entsprechend unterstützende Rahmenbedingungen. Ohne diese Grundvoraussetzungen wird es schwierig, einen finanziell lohnenden Trade-off zwischen dem Aufwand der Regulatorik und dem Erfolg von Geschäftsmodellen zu gestalten.

Beauftragtentätigkeit als Erfolgsfaktor

Als Mehrmandantendienstleister optimiert die DZ CompliancePartner fortlaufend ihre Unterstützungsleistung

- mit Blick auf neue regulatorische Anforderungen (Stichwort DSGVO, BAIT etc.), aber auch
- hinsichtlich gesellschaftspolitischer Anforderungen, insbesondere der Digitalisierung, und
- der betriebswirtschaftlichen, bankenindividuellen Anforderungen (Stichwort Prozessintelligenz, Lernkurveneffekte, Kosten-Nutzen-Balance etc.).

Auch für uns ist dies ein Prozess, der langfristig angelegt und auch nicht ohne Rückschläge ist.

Als Ihr Beauftragter verstehen wir uns als Sparringspartner, wenn es darum geht, Ihr Geschäftsmodell für die digitalen und aufsichtsrechtlichen Herausforderungen abzusichern und auch fit zu machen. Wir wollen Ihnen

- aufsichtlich akzeptierte Vorgehensmodelle zur Gestaltung des Beauftragtenwesens bieten,
- Zugang zu der gesammelten Expertise und idealen Lösungen in der Genossenschaftlichen FinanzGruppe durch optimales Wissensmanagement verschaffen,
- ein Team von Kolleginnen und Kollegen zur Verfügung stellen, die sich für die Umsetzung dieser Aufgaben begeistern.

Schlussendlich können wir als Mehrmandantendienstleister dem Mehraufwand Prozessintelligenz entgegensetzen. Standardisierung und Automatisierung sorgen nicht nur für Transparenz und Sicherheit in der Funktion, sondern auch in der betriebswirtschaftlichen Steuerung. Ihnen steht ein gleichermaßen angemessenes wie wirksames Vorgehen zur Verfügung, das die nötigen Aufwände an den tatsächlichen Erfordernissen ausrichtet. Die Eintrittswahrscheinlichkeit für sanktionierbares Fehlverhalten kann deutlich reduziert werden.

Datenschutz und Informationssicherheit sind zur Zeit einer der regulatorischen Kernthemen, der alle Marktteilnehmer, Unternehmen ebenso wie Kunden, beschäftigt und auch weiterhin beschäftigen wird. Organisatorisch und strukturell richten wir aktuell unseren Fachbereich auf genau diese Anforderungen aus, um unsere Dienstleistungen im Sinne unserer Kunden auch zukünftig erfolgreich zu gestalten.

Die DZ CompliancePartner unterstützt diese Prozesse bereits inhaltlich für die von ihr selbst angebotenen Auslagerungsdienstleistungen. Ferner stellen wir auch Arbeitsmittel für das Auslagerungsmanagement zur Verfügung, damit Ihr Haus das Auslagerungsmanagement in dem geforderten Umfang und betriebswirtschaftlich sinnvoll erfüllen kann. ▬