Datenschutzgrundverordnung

„Einige Maßnahmen sollte man schon angehen“

Ende Mai wird die EU-Datenschutzgrundverordnung „scharf geschaltet“. Und dann? Muss der eigene Betrieb nun zum Hochsicherheitsrechenzentrum mutieren? Versicherungsberater Christian Müller gibt in seinem Gastbeitrag „etwas Entwarnung“, doch „einige Maßnahmen sollte man schon angehen“, empfiehlt er Maklern. Welche das im Detail sind, erfahren Sie hier.

Vor der Regulation ist nach der Regulation – man könnte auch sagen: „Brave New World“ aus Brüssel...

Die erste Regulatorik-Hürde ist genommen und schon wird das nächste Thema durchs Dorf getrieben. Dieses sperrige Konstrukt nennt sich EU-DSGVO, das für EU-Datenschutzgrundverordnung steht.

Aktuell liest man zu dem Thema viel, meist handelt es sich dabei um Extremszenarien, die vielfach in der täglichen Praxis so nicht vorkommen werden – gerne in Form von Checklisten, juristischen Auslegungen oder technologiegetriebenen Tipps. Für die Praxis bleiben die Fragen, was das bringen soll und wie man es umsetzen soll?

Gesunder Menschenverstand hilft

Zunächst etwas Entwarnung: Gesunder Menschenverstand und fachlich qualitätsgesicherte Informationen sind der erste Schritt, sich dem Problem zu stellen. Doch beginnen wir bei der Basis.

Datenschutz ist kein neues Thema und das Bundesdatenschutzgesetz existiert auch schon seit mehreren Jahren. Die Regulationsbehörden hatten für sich festgestellt, dass de jure ein Rahmenwerk existiert, jedoch die praktische Umsetzung beziehungsweise die Erhöhung des Sicherheitsniveaus in den Unternehmen auf sich warten lässt.

Das veranlasste sowohl die EU als auch den nationalen Gesetzgeber dazu, ein ganzes Stakkato an sperrigen Gesetzen und Richtlinien zu verabschieden. IT-Sicherheitsgesetz, BDSG neu, Corporate-Compliance-Kodex – woher kommt das – und viel wichtiger – wer bitte soll da noch durchblicken, wenn selbst im juristischen Lager unterschiedliche Auslegungen existieren?

Die EU-DSGVO gibt es schon seit zwei Jahren, jedoch wird die Regelung erst im Mai 2018 „scharf“ geschaltet und sanktioniert. Das ist auch die Information, die aktuell in der Presse und in den Fachzeitschriften publiziert wird. Nun stellt sich die Frage, was eigentlich neu ist an der ganzen Thematik?

Neu in der EU ist, dass drakonische Strafmaße, wie sie sonst nur im angelsächsischen Raum bekannt sind, eingeführt werden – man kennt‘s aus Netflix-Serien wie Suits oder schlechten amerikanischen B-Movies. Und daher rührt auch die Welle her, denn im internationalen Kontext kollidieren die Rechtsrahmen deutlich. Während in den USA der Erbringer einer Dienstleistung drakonische bestraft wird, wenn ein Produkt oder eine Dienstleistung einen Verbraucher schädigen ist es im europäischen Rechtsrahmen anders: Dort droht bei der Produktentwicklung beziehungsweise in der sogenannten In-Verkehr-Bringung ein drakonisches Strafmaß beziehungsweise Haftungsrahmen. Frei nach America first setzt sich im Datenschutz das anglosächsische Prinzip in der Auslegung durch.

Großer Köcher an Sanktionsmaßnahmen

Hohe Geldstrafen bis zu 4 Prozent des Gesamtumsatzes eines Unternehmens, Freiheitsstrafen aber auch Berufsverbot umfasst der Köcher der Sanktionsmaßnahmen. Bekannt aus Funk und Fernsehen.

Das lässt zunächst aufhorchen. Und genau das ist auch gewollt, nämlich dass die Thematik Datenschutz auch den Weg in die Räume der Geschäftsleitung findet und mit entsprechender Priorität behandelt wird. Die Vielzahl der erscheinenden Fachartikel bestätigt dieses auch. Ein Grundprinzip ist wichtig zu verstehen: Der Unternehmer beziehungsweise seine Repräsentanten sind verantwortlich/in der Haftung.

Neu sind auch die gestärkten Rechte der Kunden. Einige sind bereits bekannt und realisierte Praxis. Das Recht auf Auskunft, Löschung und Sperrung dürften bekannt sein, weniger prominent kommuniziert ist aber das Recht auf Übergabe der Daten in einem lesbaren Format, damit diese Daten auch von einem anderen Dienstleister verarbeitet werden können.

Wie das genau zu verstehen ist, das lässt der Gesetzgeber bewusst offen. Ob nun technische Schnittstellen wie GDV oder BIPRO gemeint ist oder es auch eine einfache csv- oder Excel-Datei tut? Das ist offen und wird sich in der Praxis erarbeiten müssen – und wird sicherlich zu einigen FAQ führen. Soviel ist gewiss.

Wichtig bei dem Kanon der Neuerungen ist jedoch die Beweislastumkehr. Im Fall eines Datenschutzverstoßes ist der Unternehmer in der Beweislast darzulegen, welche technischen und

organisatorischen Maßnahmen er unternommen hat, um dem Datenschutz gerecht zu werden.

Und genau das ist der springende Punkt auf den es ankommt. Je nachdem wie hoch das installierte Risikomanagement ist und welche Maßnahmen ergriffen wurden steuert nämlich das Maß der Sanktionen. Ah, halt – es geht also darum, einen geregelten Prozess zum Risikomanagement zu etablieren. In dem Kontext ergibt das Ganze wieder einen Sinn. Während das IT-Sicherheitsgesetz darauf abzielt, kritische Infrastrukturen zu schützen (das IT-Sicherheitsgesetz wurde recht stumpf aus dem NIS-Rahmen der USA abgekupfert) und den Datenverkehr im World Wide Web zu schützen, zielen wir mit dem BSI-(Bundesministerium für Sicherheit und Informationstechnik)-Katalog auf sicherheitsanfällige Komponenten ab.

Muss der eigene Betrieb zum Hochsicherheitsrechenzentrum mutieren?

Für die Praxis heißt das, dass die technischen Komponenten einer IT-Umgebung durch diesen Rechtsrahmen besonders abgesichert sein sollen. Ob das die Kommunikation mit E-Mail, Messengern, Cloud Dateidiensten ist, aber auch der Datenaustausch über Schnittstellen. Technisch soll die Kommunikation End-to-End verschlüsselt sein, revisionssicher, mit Zugangsvorrichtungen und Passwortrichtlinien versehen sein – und all den anderen netten Komponenten die IBM, HP, Cisco und Microsoft so gerne im Angebot haben und gut und teuer sind.

Das stellt man sich ernsthaft die Frage, ob der eigene Betrieb zum Hochsicherheitsrechenzentrum mutieren soll? Die Zahnärzte, zum Beispiel mit der neuen Telematik-Infrastruktur im Rahmen der e-Health Kampagne, können ein Lied davon singen. Und ich befürchte, in deutscher Gründlichkeit werden wir wie immer über das Ziel hinausschießen und versuchen alles physikalisch Denkbare in Gesetze zu pressen und so in den Markt zu drücken. Das wird noch spannend werden.

Doch zurück zum Risikomanagement. Und was konzeptionell eigentlich gewollt ist, dazu ein Beispiel, wie man sich das vorstellen kann: Ein Unternehmer, der umfassende Maßnahmen wie einen Datenschutzbeauftragten, technisch organisatorische Maßnahmen wie Verfahrensverzeichnisse, Verschlüsselung der Daten aber auch Zutrittsberechtigungen geregelt hat, dürfte im Fall der Fälle mit einer geringeren Sanktion rechnen als jemand der sich nur minimal gekümmert hat und nur Impressum, verschlüsselte E-Mails und saubere Datenschutzerklärungen vorweisen kann.

Also hier greift dann das Prinzip der Exkulpation. Und mit diesem Mechanismus möchte man das Thema Datenschutz konzeptionell treiben in Richtung Risikomanagement. Risikomanagement in dem Sinne, dass im Unternehmen ein Bündel von Maßnahmen umgesetzt wird, die regelmäßig einer Überprüfung unterzogen werden und durch sukzessive Dokumentation der Feststellungen und Korrektur-Maßnahmen zu einem gesteigerten Sicherheitsniveau führt.

Das ist die Intention dieser Regulierungen. Nun, jetzt mal aus 10.000 Meter akademischer Flughöhe runterkommend auf praktische, sinngebende Maßnahmen. Es ist keinesfalls so, dass ich bis 28. Mai 2018 alle denkbaren theoretischen Maßnahmen umgesetzt haben muss.

Das ist zum Teil technisch auch noch gar nicht machbar, man denke an das Thema E-Mail-Archivierung von verschlüsselten Mails. Da gibt es noch keine saubere technische Lösung! Aber einige Maßnahmen sollte man schon angehen: Sauberes Impressum, saubere Datenschutz- und Einwilligungserklärungen, Absicherung der Webseite mit SSL-Zertifikaten und Mail-Verschlüsselung sind solche ersten Schritte, die man ohne hohen und kostenintensiven technischen Aufwand umsetzen kann. Schritt für Schritt. Und auch im laufenden Betrieb.

Was sicherlich neu diskutiert werden muss, ist der Einsatz von Cloud-Technologien. Denn im Sinne eines alternativen Risikotransfers lässt sich mit einem Cloud-Software-as-a-Service-Konzept ein Großteil der technologischen Risiken auf den Cloud-Anbieter verlagern. Das Mantra, meine Daten gehören mir und wo das Blech ist, ist die Musik, dürfte hier einen neuen Ansatz erfahren und sicherlich auch die Geschäftsmodelle von Pools und MVP-Anbietern berühren.

Es bleibt also spannend und alles was nach Risiko klingt, kann auch eine Chance sein. Einfach alles mal aus der Risikomanagement-Brille betrachten und auch mögliche Chancen erkennen – und bitte nicht jedem klappernden Sarg hinterherlaufen. Auch mit einfachen Maßnahmen lässt sich technisch, juristisch und organisatorisch einiges erreichen. Und glauben Sie mir: Ich weiß wovon ich schreibe, in unserm Betrieb, der als BU-Leistungsfall-Dienstleister hochkritische Daten bearbeitet unterliegen wir besonders hohen Anforderungen an die Datensicherheit. Und last not least. Beginnen Sie bereits heute. Hat Ihre Webseite ein Kontaktformular und ein SSL-Zertifikat? Sollten Sie haben...

Über den Autoren

Diplom-Kaufmann Christian Müller ist Unternehmens- und Versicherungsberater und TÜV ISO 9001 Auditor. Ehrenamtlich arbeitet er als Vorstand im Bundesverband der Sachverständigen für das Versicherungswesen BVSV. Gemeinsam mit seiner Frau Esther Riehl Müller ist er Teilhaber der **RWM Group in Kassel**.

Dieser Artikel erschien am **03.04.2018** unter folgendem Link: