DSGVO - Panik?!

Wieso die Panikmache rund um die DSGVO unbegründet ist.

Von Michael J. Erner und Dr. Bruno Wildhaber

27.10.2017

Inhaltsverzeichnis

1 Was ist die DSGVO

Die DSGVO (Datenschutz Grundverordnung) oder auch GDPR (General Data Protection Regulation) ist eine

EU-weite Norm für Datenschutz.

Sie ist im Mai 2016 in Kraft getreten und wird anwendbar am 25.05.2018. D.h., derzeit läuft eine Übergangsphase, am

25.05.2018 muss die DSGVO innerbetrieblich umgesetzt sein.

2 Was unterscheidet sie von früheren Regelungen

Sie ist keine Richtlinie oder Direktive der EU, sondern eine Verordnung und hat damit unmittelbaren Gesetzescharakter, d.h. ist sofort anwendbar.

Sie gilt für alle EU Staaten.

Nationale Interpretationen und Umsetzungen sind in Gestalt verschiedener Öffnungsklauseln zwar möglich, die Übertragung in nationales Recht der Mitgliedstaaten wird stattfinden und findet auch bereits statt. Die Umsetzung darf aber die Grundzüge der DSGVO nicht unterschreiten.

3 Schafft die DSGVO einen Selbstbedienungsladen für Anwälte und Berater?

Die DSGVO bringt zwar neue Anforderungen, denn es gibt in der DSGVO neue Bestimmungen, die zusätzliche Maßnahmen erfordern. Diese sind jedoch in ihren Prinzipien auch schon aus der alten Rechtslage bekannt, und damit beherrschbar. Aus der Umsetzungspraxis in D und CH heraus betrachtet sind die Anforderungen deshalb nicht so schwerwiegend, wie diverse Rechtsberater, Anwälte und Co. potenziellen Kunden glauben machen wollen.

Es geht primär darum, mit dem FUD (Fear, Uncertainty and Doubt) - Prinzip Ängste zu verbreiten, um neue Kunden zu gewinnen.

4 Aber was ist denn jetzt mit diesen hohen Bußgeldern?

Große Panikmache gibt es zum Thema Bußgelder: 4% vom Konzernumsatz (max. 20 Mio. €) sind ja mal was.

Doch halt! Wenn Sie als Unternehmen die heute geltenden Regeln des CH/D Datenschutzes einhalten und befolgen, ist Panik unnötig. Zudem ist noch lange nicht geklärt, wie so eine Summe überhaupt verhängt werden soll. Hier sind weiterhin Fragen unbeantwortet wie: Wer verhängt diese Busse und was sind die Rechtsmittel? Welche Grundlagen gelten für die Beurteilung einer möglichen Gesetzesverletzung?

Letzteres bildet den wunden Punkt in der ganzen Debatte:

Es gibt noch keine nationalen oder europaweiten Grundlagen für die Beurteilung der rechtlichen Konformität der Datenbearbeitung, denn diese müssen zuerst durch die Behörden aufgebaut werden.

Wir wissen das, weil wir schon seit 10 Jahren behördlich akkreditierte Prüfstelle für Datenschutz sind und mit den Prozessen vertraut. Derzeit ist es so, dass erst dann, wenn ein abgestimmter Kriterienkatalog existiert, Beurteilungen überhaupt möglich sind! Zudem müssten Verfehlungen vorsätzlich begangen werden, um eine Höchstsumme von 4% des weltweiten Jahresumsatzes als Bußgeld verhängen zu können. Vorsätzlich heißt „bewusst und gewollt" gegen Datenschutzbestimmungen zu verstoßen. Allerdings ist auch ein sog. Eventualvorsatz nicht unbedeutend. D.h., die „billigende Inkaufnahme" einer fehlenden Komplianz zur DSGVO ist ein nicht zu unterschätzendes Risiko. In der Regel geht es in der Praxis jedoch **nur** um fahrlässige Verstöße und diese werden je nach Expertengutachten unterschiedlich hoch gewichtet. D.h. der Grundsatz der freien Beweiswürdigung gilt auch hier, allerdings dürfte die notwendige Sorgfalt einer Organisation höher angesetzt werden als in der Vergangenheit.

Sollten Sie allerdings vorsätzlich Datenschutzverstösse im Rahmen Ihrer Geschäftstätigkeit begehen, dann wären Sie schlimmer als jene, die in den letzten Jahren mit Bußgeldern von sich reden gemacht haben. Eine Selbstanzeige wäre damit angesagt.

5 Was müss(t)en Sie heute schon beherrschen

Sie fragen sich, was Sie beherrschen müssen, um die DSGVO zu erfüllen?

Hier gelten die Uralt-Prinzipien aller Datenschutzgesetze:

- Sie wissen, wo Ihre personenbezogenen **Daten gespeichert** sind und können darüber auch auf Basis von Dokumentationen Auskünfte erteilen [1].
- Sie können personenbezogene Daten **löschen**: Sie kennen die **Daten-Lebenszyklen** und können sie aktiv steuern (Information Governance) [2], [3].
- Sie kennen ihre **IT-Risiken** und haben im Idealfall ein **Risk Management System** im Einsatz (ISMS)
- Ihre **Verträge** enthalten keine unzulässigen Klauseln und sind transparent bezüglich der Datenhaltung
- Sie **prüfen neue Datenhaltungen/Projekte** vorrangig auf mögliche Probleme mit dem Datenschutz (Risikofolgenabschätzung VOR Inbetriebnahme der Lösung)
- Sie kennen Ihre **Datenflüsse** (und sind damit auch gerüstet für die Datenschutzfolgenabschätzung nach DSGVO)

Kurzum:
Sie beherrschen Ihre IT-Prozesse und haben Information Governance zumindest für die personenbezogenen Daten umgesetzt.

Und denken Sie daran: Nur wer Daten löschen kann, beherrscht sie!

6 Was ändert sich mit der DSGVO?

Verantwortlichkeiten werden klarer definiert, Datenflüsse transparenter gestaltet und Ländergrenzen schärfer gezogen (EU). Natürlich ist das nicht alles. Manches wird einfacher, anderes schwieriger, aber unter dem Strich ist das alles kein Hexenwerk, sondern nur eine Frage von Betriebsrisiken. Das ist auch aus anderen Fachbereichen bekannt. ISMS, Compliance und IT-Governance lösen schon seit Jahrzehnten keine Panik mehr aus. So sollte es auch mit der DSGVO sein. Wir reden hier über zumeist technische Prozesse, die unter neue Bedingungen gestellt werden, sich dennoch in der Sache nicht verändert haben: Nullen und Einsen. Die aber mehr und mehr von einem Ort zum anderen transportiert werden und das ist es, was sich verändert: Die

Welt um uns herum. Und deshalb braucht es eine DSGVO. Technische Möglichkeiten lassen Begehrlichkeiten aufkommen und diese gilt es zu kontrollieren. Denn Europa ist mit seinen Regelwerken nicht allein auf dem Planeten. D.h., ein Schwerpunkt der DSGVO liegt in Transferleistungen in Regionen außerhalb Europas und den sich daraus ergebenden Schutzfunktionen für die Bürger der Union. Wer das beherrscht, braucht sich vor der DSGVO nicht zu scheuen.

7 Werden für die Verarbeitungen nach DSGVO Zertifizierungen angeboten?

In absehbarer Zeit, ja. Noch ist es aber nicht so weit, da sich die Bundes- und Landesbehörden in einem Abstimmungsprozess befinden, wie zukünftig mit Zertifizierungen verfahren werden soll. Hier spielt die DAkkS (Deutsche Akkreditierungsstelle) auch eine Rolle. Inhaltlich ist bislang sichere Erkenntnis, dass Zertifizierungen in Abhängigkeit zu Schutzklassen ab dem 26.10.2018 Zwang, und in Form von Datenschutzfolgenabschätzungen gem. Art. 33 DSGVO von den Behörden bei Audits abgefragt werden. Das heißt nicht, dass jede einzelne Applikation, die personenbezogene Daten verarbeitet oder verarbeitbar macht, zu dokumentieren ist. Denn Datenschutzfolgenabschätzung steht nicht für die Folgen, die Datenschutz für Unternehmen haben kann, sondern für Folgen, die einem Betroffenen aus Verarbeitungsprozessen seiner personenbezogenen Daten entstehen können.

Damit lassen sich notwendige „DSFA" auf betroffene Personengruppen reduzieren. Mitarbeiter, Kunden, Lieferanten ... und ein paar andere. Eine DSFA ist somit nichts anderes als eine zusammenfassende Dokumentation von Prozessen, von denen Personen betroffen sein können. Natürlich braucht man dafür Grundlagen, z.B. eine Übersicht der im Betrieb eingesetzten Applikationen, Datenfeldlisten, Schnittstellenbeschreibung u.a. Aber die sollten ohnehin schon da sein, denn wenn nicht, kommt die Ausgangsfrage wieder auf: Beherrschen Sie Ihre Prozesse?

Wiederum: Kein Hexenwerk, denn es ist alles schon einmal da gewesen. Einer der Vorteile, den die DSGVO bietet, ist z.B. darin zu sehen, dass Zertifizierungen nicht von jedem Auftraggeber durchgeführt werden müssen, sondern bei Vorhandensein von den Auftragsverarbeitern (nicht mehr Auftragsdatenverarbeiter) vorgelegt werden können. Der AG muss nur noch auf Schlüssigkeit prüfen.

Aber:

Nichtvorhandensein einer DSFA ist schon ein Prüfungsergebnis und löst Bußgelder aus.

Wie Sie Ihre Informationen beherrschen, finden Sie im Leitfaden Information Governance des KRM [4].

8 Ist Datenschutz einfach ein Teil des normalen Risikomanagements?

Natürlich: Datenschutz ist (endlich) im Risikomanagement angekommen. Am Ende des Tages geht es damit bei den täglichen Prozessen auch im Datenschutz um die Frage:

Wie hoch ist das Betriebsrisiko und wie gehe ich damit um?

Um hier anzukommen, oder DSGVO – konform Betriebsprozesse zu gestalten, müssen Transparenz und Beherrschbarkeit Einzug in den Datenalltag halten. Wie auch in allen anderen Compliance Fragestellungen gibt es kaum je eine schwarz-weiß Betrachtung, geschweige denn Lösung. Das Management wird verstärkt in die Verantwortung genommen und muss sich nun aktiv um die Risiken kümmern, welche mit der Bearbeitung von personenbezogenen Daten verbunden sind.

Dann ist auch eine DSGVO nur eine Aufgabe mehr auf der Tagesagenda. Eine Aufgabe, vor der man sich nicht scheuen und auch nicht panisch machen lassen muss.

9 Wo stehen Sie heute?

Möchten Sie eine Einschätzung zu Ihrer Organisation? Dann führen Sie unser kurzes DSGVO Assessment durch [5].

Dieses Assessment gibt Ihnen eine erste Einschätzung darüber, auf welcher Stufe Ihre Organisation heute bezüglich Datenschutz steht und wo zentraler Handlungsbedarf gegeben ist.

10 Die Situation in der Schweiz

10.1 Was sind die Unterschiede zur Rechtslage in der Schweiz?

Die Schweiz ist der DSGVO faktisch nicht unterworfen, da sie nicht EU-Land ist. Da aber ein Datenaustausch aus den Mitgliedstaaten der EU in die Schweiz den Regularien der DSGVO zu unterwerfen ist (es dürfen nur Daten in Länder transferiert werden, in denen ein der EU gleichwertiges Datenschutzniveau vorherrscht), müssen Schweizer Unternehmen, die mit EU-Daten arbeiten, DSGVO-konform sein. Anderenfalls wäre ein Transfer in die Schweiz einem Datentransfer in unsichere Drittstaaten gleichgestellt, was nicht unerhebliche Konsequenzen bis z.B. hin zu Verfahrensuntersagungen durch die Behörden haben kann.

Die Schweiz revidiert deshalb ihr DSG und passt es gegenwärtig der DSGVO an.

Der aktuelle Entwurf (Stand September 2017) dürfte die Gleichwertigkeit mit der DSGVO allerdings kaum erfüllen (vgl. den Artikel von B. Wildhaber vom 10.10.2017).

10.2 Was geschieht, wenn die Schweiz das nationale Recht bis im Mai 2018 nicht angepasst hat?

Vorerst passiert einmal nichts. Da aber die Verordnung in der EU sofortige Wirkung hat, müssen sich Unternehmen, die mit CH-Partnern Geschäfte betreiben und personenbezogene Daten bearbeiten, versichern, dass ein der DSGVO konformes Datenschutzniveau bei ihren CH-Partnern gewährleistet ist. Allenfalls werden Teile des Schweizerischen DSG bereits vor dem 25.5.18 aktualisiert, dies ist jedoch derzeit noch unbestimmt.

Aus diesem Grund sollten sich Organisationen in der Schweiz so dokumentieren, dass sie die Konformität mit der DSGVO nachweisen können.

Dazu kann z.B. eine Verfahrensdokumentation erstellt werden, wie sie z.B. für die Compliance Zertifizierung zum Einsatz kommt [1].

11 Literaturverzeichnis

[1] KRM, *Verfahrensdokumentation,* KRM, 2017.

[2] *Was ist Information Governance?.* [Film]. KRM, 2016.

[3] B. Wildhaber, Information Governance, KRM, Hrsg., Zollikon, ZH: KRM, 2015.

[4] Kompetenzzentrum Records Management, Records Management, K. R. Management, Hrsg., Zürich: Kompetenzzentrum Records Management, 2008.

[5] KRM / M100, „DSGVO Kurzcheck," 2017: https://informationgovernance.ch/angebote/beratungsleistungen/dsgvo-kurz-assessment/

12 Die Autoren und Unternehmen

Michael J. Erner ist Jurist und Vorstandsvorsitzender von MISSION 100. Als langjähriger Datenschutzsachverständiger und –berater kümmert er sich vornehmlich um Konzerndatenschutz im internationalen Umfeld.

Dr. iur Bruno Wildhaber, CISA CISM CIP CGEIT ist selbständiger Unternehmer und Geschäftsleitungsmitglied des KRM sowie Datenschutz-Gutachter. Sein Schwerpunkt liegt in der Beratung von Unternehmen im Umgang mit Information mit einem Fokus auf Compliance und Information Governance.

Mission 100

MISSION 100 e.V. wurde im Jahr 2007 von langjährigen Datenschutz- und Informationssicherheitsexperten gegründet. Die Vereinsmitglieder sind selbstständig als Unternehmer oder Freiberufler am Markt tätig und bündeln Ihre Kapazitäten sowie Erfahrungen über den Verein. Für Sie heißt das geringe Beratungskosten durch eine schlanke Verwaltungsstruktur. Für uns ist der Name Programm. Es müssen nicht immer 100% Risikomanagement, Datenschutz oder Informationssicherheit sein. Denn es geht auch weniger. So wie Sie es wünschen, ist das eine oder das andere unsere Mission.

Unsere Berater sind u.a. beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) als anerkannte Sachverständige (Recht/Technik) tätig.

Informationen und Website: http://mission100.org/

Das Kompetenzzentrum Records Management (KRM)

Das KRM fokussiert sich auf Information Governance und betreibt dazu das erste Kompetenzzentrum in Europa. Wir steigern den Wert von Information für unsere Kunden und verknüpfen dabei die klassischen Mittel der Informationstechnik, des Rechts und der Informationswissenschaft mit der neuen Welt der sozialen Medien. Wir schlagen Brücken zwischen hochspezialisierten Bereichen und fördern umfassende Lösungen. Trotzdem verlieren wir nie den Sinn für das Machbare und die kurzfristig notwendigen Resultate. Wir verlangen von unseren Partnern interdisziplinäres Denken und unternehmerische Weitsicht sowie die notwendige Fachkompetenz in ihren Fokusgebieten.

KRM (Kompetenzzentrum Records Management) GmbH
Rotfluhstrasse 91
8702 Zollikon
http://www.informationgovernance.ch/ Mail: info@informationgovernance.ch