Von der DSGVO zur Umsetzung des Datenschutzes

ASCON HORIZON INNOVATION GROUP (GmbH)
Stewardstrasse 23, 14169 Berlin
Tel +49 (0)1711291339
avh@ahig-group.com, kvh@ahig-group.com

Geschäftsführer: Andreas v.Heinemann, Katarzyna v.Heinemann-Szawelska
Registergericht: Amtsgericht Berlin-Charlottenburg, HRB 134574B

Berlin, 29.01.2018

Inhaltsverzeichnis

1. DSGVO – in aller Munde – und die Umsetzung? 3

2. Die Prozess- und IT-Ebene im Fokus der Umsetzung 3

3. In Sieben-Meilenstiefeln zur Umsetzung..... 5

4. Der kontinuierliche Verbesserungsprozess..... 7

5. Die DSGVO nützt dem Unternehmen, seinen Kunden und Angestellten..... 8

1. DSGVO – IN ALLER MUNDE – UND DIE UMSETZUNG?

Die Informations-Veranstaltungen und Seminare füllen sich mit interessierten Zuhörern, die gerne mehr über die Gesetzeswelt des Datenschutzes erfahren möchten. Ab dem 25. Mai dieses Jahres wird es nun ernst! Es verbleiben knapp drei Monate; und die Uhr tickt! Doch wer die Veranstaltung verlässt, weiß bisweilen, welche Veränderungen und Neuerungen der Gesetzgeber vorschreibt, sieht sich aber mit der Umsetzung alleine gelassen.

„Nur weil man die Straßenverkehrsordnung auswendig kennt, ist man noch lange kein guter Fahrer“. Um bei dem Bild zu bleiben, müssen Unternehmer und Geschäftsführer nicht nur bis zum Mai die Verkehrsregeln des Datenschutzes beherrschen, sie müssen danach auch ihr Unternehmen auf der Prozess- und IT-Ebene sicher lenken, steuern und führen.

2. DIE PROZESS- UND IT-EBENE IM FOKUS DER UMSETZUNG

Aus praktischer Erfahrung hat sich die Darstellung der Zusammenhänge, der Maßnahmen zur Umsetzung und der Kontrollen auf drei Ebenen bewährt. Diese sind:

- **Die Juristische Ebene**: Hier greifen gesetzliche Regelwerke mehrerer Rechtsquellen ineinander, z.B. die DSGVO, das BDSG, das Telekommunikationsgesetz, speziellere Gesetze wie Steuer- und Sozialgesetze, etc.
- **Die Prozessuale Ebene**: Hier werden in zeitlicher Reihenfolge Aufgaben nacheinander ausgeführt, z.B. Registrierung eines neuen Kunden oder Mandanten sowie Aufnahme der Kundendaten und -wünsche bis hin zum Versand und Mahnung einer Rechnung.
- **Die IT-technische Ebene**: Hier werden die juristischen und fachlichen Anforderungen in den Applikationen (Software) umgesetzt. So werden z.B. die Schutzmaßnahmen, die Berechtigungen, die Datensperrungen sowie Löschfristen und die Reports zur Kontrolle automatisiert in dem jeweiligen Programm hinterlegt.

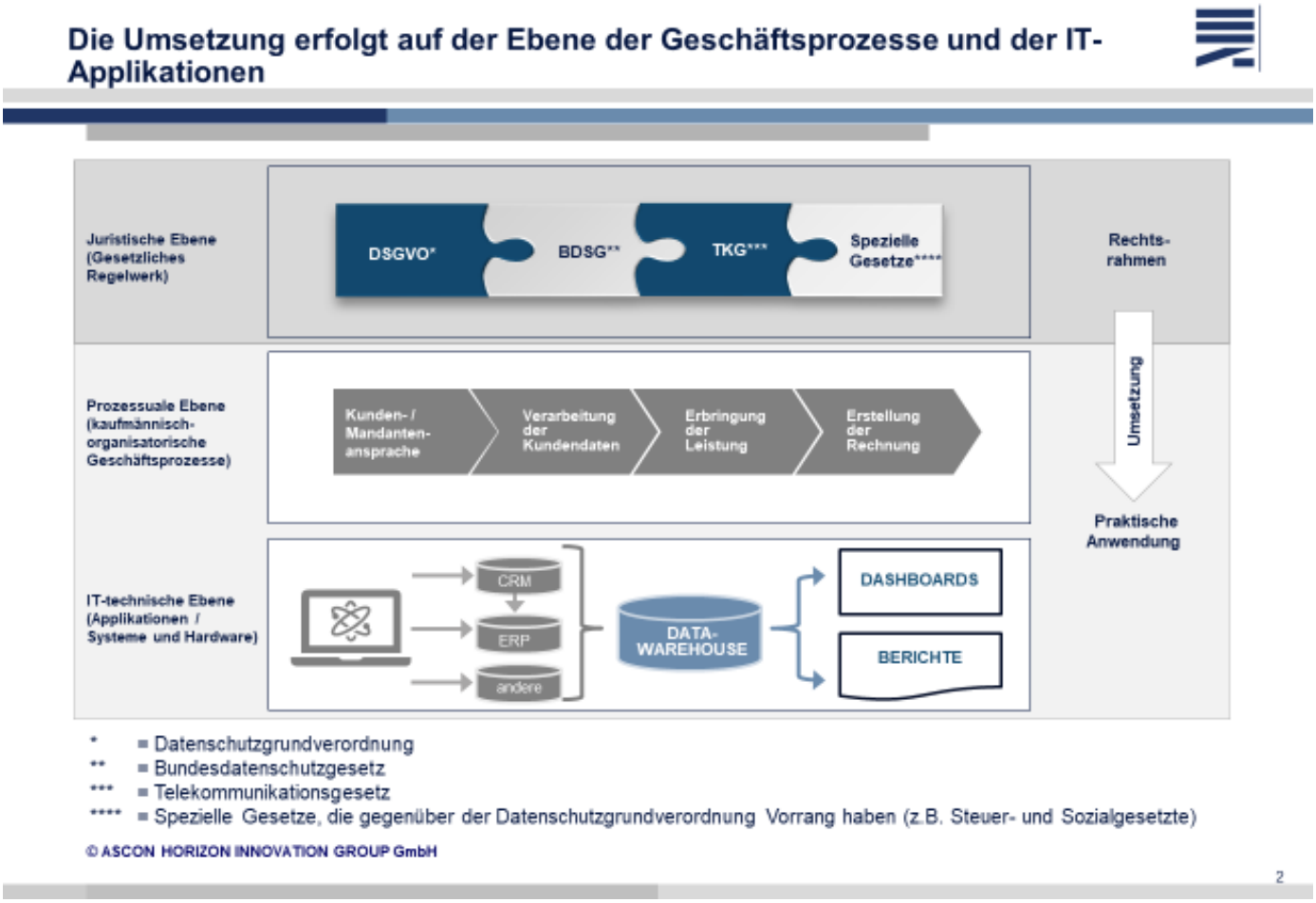

Abbildung 1: Darstellung der juristischen, prozessualen und IT-technischen Ebene

Das vielfältige juristische Regelwerk mit unterschiedlichen Rechtsquellen der ersten Ebene muss nun auf den zwei praktischen Ebenen umgesetzt werden. Auf der prozessualen Ebene stellt sich die Frage, welche Schritte und Aufgaben entlang der Geschäftsprozesse angepasst werden müssen, welche Formulare wie verändert werden und wie die konkrete Umsetzung der eigenen Nachweispflicht erfolgen soll, um zum einen datenschutzkonformes Verhalten zu erreichen und gleichzeitig den Ablauf nicht zu stören. Auf der IT-technischen Ebene zielen die Maßnahmen auf die Datenschutzkonformität der IT-Landschaft ab, also dem Applikationsverbund aller genutzten Systeme (z.B. leitet ein CRM die Daten an das ERP weiter? etc.). Ziel muss es sein, so viele Datenschutzpflichten wie möglich auf der IT-technischen Ebene automatisiert zu erfüllen, so dass diese im Hintergrund unbemerkt und unter Entlastung der kaufmännisch-organisatorischen Prozesse erfolgen und menschlichen Fehlerquellen entzogen sind. Im Umkehrschluss bedeutet dies, dass alles, was sich nicht auf der IT-technischen Ebene automatisiert umsetzen lässt, durch manuelle Maßnahmen der Mitarbeiter zusätzlich ausgeführt und durch die zuständigen Führungskräfte angewiesen, geschult und kontrolliert werden muss.

3. In Sieben-Meilenstiefeln zur Umsetzung

Der kurze Zeitraum bis zum 25.Mai 2018 lässt in vielen Fällen keine umfassende Analyse, detaillierte Abstimmung der Prozesse und Abläufe sowie eine Umsetzung 1:1 in den IT-Systemen zu. Daher empfiehlt es sich, vom Kern her sukzessiv Schritt um Schritt das gesetzlich vorgeschriebene Datenschutz-Management System in seiner automatisierten Form zu entwickeln.

Abbildung 2: Darstellung eines zügigen Umsetzungsprozesses

Kern und Ausgangspunkt stellen hier die personenbezogenen Daten bzw. die besonderen Kategorien personenbezogener Daten dar. Hier ist im ersten Schritt zu prüfen, welche Daten wo in welcher Form vorliegen und wozu diese in welchem Prozessschritt durch welche Systeme verarbeitet werden. Im zweiten Schritt ist zu prüfen, warum diese überhaupt verarbeitet werden, also ob ein Zweck und eine Rechtsgrundlage im Sinne der DSGVO überhaupt vorliegt. Hier ist je Zweck auch bei gleichem Datum eine getrennte Zweckbestimmung vorzunehmen. Dies bedeutet, dass ein und der gleiche Datensatz in unterschiedlichen Programmen zu unterschiedlichen Zwecken verwendet werden kann. So liegen Name und Adresse eines Beschäftigten vor, um z.B. Lohn- und Gehaltsberechnungen vorzunehmen als auch ihm als Kunden des Unternehmens Produkte zuzusenden, die er gekauft hat. Im dritten Schritt ist zu prüfen, ob abhängig von dem jeweiligen Zweck

- die richtigen Personen Zugriff auf die Daten erlangen,
- über die Daten gem. DSGVO Auskunft erteilt werden kann,
- eine korrekte Protokollierung der Vorgänge und des Zugriffs erfolgt
- Aufbewahrungsfristen, -verfahren und Löschvorschriften installiert sind.

Im vierten Schritt prüft man die Form und Sicherheit der Datenübertragung. Im nächsten Schritt werden die bestehenden Formen der Dokumentations- und Nachweispflichten überprüft.

Im darauffolgenden Schritt werden, abhängig von den Prüfungsergebnissen, dann je Prüfungsschritt Maßnahmen definiert. Diese Maßnahmen führen dann zu Ergebnissen, die oftmals erst rein organisatorische Regelungen und manuelle Aufgaben umfassen bevor sie dann im siebten Schritt in den IT-Systemen hinterlegt werden.

Auch mit organisatorisch-manuellen Lösungen könnte durchaus den Anforderungen der DSGVO erst einmal entsprochen werden.

4. DER KONTINUIERLICHE VERBESSERUNGSPROZESS

Zur Entlastung der Mitarbeiter und Führungskräfte als auch zur zügigen Reaktion bei Anfragen Dritter ist eine sukzessive Umsetzung in den IT-Systemen zu empfehlen. Hierzu kann der kontinuierliche Verbesserungsprozess genutzt werden. Wie in der Grafik dargestellt zielt der kontinuierliche Verbesserungsprozess auf drei Effekte ab:

- Systematischer Vorgang in der Analyse und Umsetzung erkannter Verbesserungsmöglichkeiten
- Priorisierung der Maßnahmen inkl. einer Kosten-Nutzen- Abschätzung (z.B. auf Basis einer dokumentierten Risikoeinschätzung)
- Dokumentation der Maßnahmen und Überprüfung deren Ergebnis in der Praxis.

Abbildung 3: Darstellung des kontinuierlichen Verbesserungsprozesses

5. DIE DSGVO NÜTZT DEM UNTERNEHMEN, SEINEN KUNDEN UND ANGESTELLTEN

Die DSGVO ist kein Schreckgespenst, im Gegenteil! In einer Welt, in der „Daten als das Öl des 21. Jahrhunderts“ bezeichnet werden, ist der Schutz dieses Gutes in unser aller Sinne. Datenschutz ist Teil eines wirksamen IT-Schutzes und beide schaffen, wie in der Darstellung aufgeführt, einen zusätzlichen Wert für alle Beteiligten.

Abbildung 4: Nutzen der Beteiligten durch die DSGVO