DSGVO: Fremdgesteuerte Kosten !

Wo können Versicherungen und Dienstleister helfen ?

von Marc Latza

Im Grunde ist der Umgang mit der DSGVO nicht sonderlich schwer, wenn man sich vorab 2 Dinge vor Augen führt:

- Die DSGVO ist ein sog. Betroffenenrecht und
- schützenswerte Daten beinhalten mind. 2 Informationen, die einen Rückschluss auf eine Person zulassen (Name und Ort, Name und Handynummer, Personalnummer und Firma usw.)

Verinnerlicht man diese beiden Hauptkriterien, werden viele Neuerungen verständlicher. Wobei man ehrlicher Weise sagen muss, dass einige dieser „Neuerungen" auch schon vorher im Rahmen des Bundesdatenschutzgesetzes gegolten haben, es hat nur keinen sonderlich interessiert.

Wirklich neu ist hingegen z.B. die sog. Informationspflicht.

Wenn eine Firma Daten erfasst, um z.B. ein Angebot zu erstellen, dann dürfen eben nur die dafür konkret benötigten Daten erhoben werden und keine Zusätzlichen, wobei es hier und da Ansichtssache ist, wann Daten konkret benötigt werden und wann Daten eher als Zusätzlich anzusehen sind. Aber es bedarf schon einer sehr guten Argumentation, warum z.B. für die Angebotserstellung für neue Fenster der Familienstand des Kunden erforderlich ist.

Ferner muss bei der Datenerhebung im Vorfeld darauf hingewiesen werden, was mit diesen erhobenen Daten passiert. Wer bekommt die Daten sonst noch und wann werden sie gelöscht – ganz im Sinne des Betroffenen, daher „Betroffenenrecht".

Dieser Informationspflicht sehr nahe kommend ist auch die sog. Meldepflicht bei drohenden Datenverlusten oder –manipulationen. Wichtig ist hier, dass die theoretische Möglichkeit der Datenmanipulation für eine Meldung ausreicht.

Wenn z.B. das Smartphone im Hotel vergessen und erst Tage später einem per Post zugeschickt wird (also länger als 72 Stunden keine Kontrolle über die sich darauf befindlichen Daten), wird eine Meldung nötig. Die Meldepflicht gilt auch bei „unverschuldeten" Verlust des Smartphones, z.B. durch Diebstahl.

Der Haken an der Sache:
Ist eine „besonders große Gruppe" von dem möglichen Datenverlust oder von der möglichen Datenmanipulation betroffen, ist „die Öffentlichkeit" durch Zeitungsanzeigen zu informieren, die mindestens eine halbe Seite umfassen und in mindestens zwei bundesweit erscheinenden Tageszeitungen zu platzieren sind. Eine Anzeige nach diesen Kriterien dürfte pro Zeitung im sechsstelligen Bereich liegen, und da ist die Anzeige als solche (also die graphische Erstellung) noch nicht enthalten.

Der Gesetzgeber sieht aber in so einem Fall auch eine Alternative vor, nämlich eine „in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme", was z.B. durch Radiospots oder TV-Beiträgen zu leisten wäre.

Eine SendeSEKUNDE kostet ca. 10,- EUR. Um eine verständliche Warnung hinsichtlich des denkbaren Datenverlustes zu formulieren, sind sicherlich 10 Sekunden nötig. Da wäre man also mit 100,- EUR vergleichsweise günstig dabei… weit gefehlt.

Der Spot muss natürlich bundesweit auf mehreren Sendern mehrmals am Tag laufen. Zudem muss so ein Spot aufwendig im Studio eingesprochen werden und dies nicht irgendwann, sondern kurzfristig. Hier sind also Mehrkosten für Überstunden des Studioteams sowie ggf. höhere Mietkosten denkbar, da der Spot z.B. nur noch am Samstagabend erstellt werden kann, da am Montag die Warnung im Radio laufen muss.

Hinzu kommt ein enormer Reputationsschaden !

Was also tun ? An welcher Stelle können Versicherungen und Dienstleister hier helfen ?

Man kann sich gegen die drohenden Benachrichtigungskosten versichern. Die sog. Cyber-Policen beinhalten zumeist eine entsprechende Kostenposition, die natürlich bezogen auf die Kundenanzahl und deren regionale Verteilung (landesweit, bundesweit, europaweit) adäquat bemessen sein sollte.

Gute Cyber-Policen arbeiten im Schadensfall mit spezialisierten Werbeagenturen zusammen, die zwar den Datenverlust und dessen Meldung nicht verhindern, aber schnellsten mit einer entsprechenden PR-Strategie die Rufschädigung mindern können.

Sehr gute Cyber-Policen übernehmen sogar Vertragsstrafen von der Payment-Card-Industrie. Die werden dann z.B. fällig, wenn ein Restaurant als Vertragspartner von VISA durch eine unsichere WLAN-Verbindung das Abfischen von Kreditkartendaten zulässt.

Insgesamt ist das Thema der versicherbaren Kosten im Cyber-Bereich spannend.

Sofern man nicht gerade technikaffin ist, dürfte mit Eintreffen eines entsprechenden Anschreibens eines sog. Abmahnanwaltes oder sogar der Staatsanwaltschaft ein gewisses Ohnmachtsgefühl eintreten. Wenn der Vorwurf eines Hackerangriffes durch mein Laptop im Raum steht, kann der Einsatz eines Daten-Forensikers ggf. das Schlimmste verhindern, in dem dieser Spezialist den Vorwurf entkräftet. Diese Kosten übernehmen i.d.R. Cyber-Policen ebenfalls.

Auch beim Thema „Datenschutzbeauftragter“ können externe Dienstleister helfen.

Firmeninhaber sollten sich aber an dieser Stelle folgenden Satz merken:
Der Datenschutzbeauftragte ist nicht der Datenschutzverantwortliche !

Die Verantwortlichkeit verbleibt auch bei Einsatz eines DSB beim Firmeninhaber.

Leider gibt es keinen echten Fixwert, an dem man den Einsatz eines DSB ausmachen kann.

Es gibt zwar die Zahl 10 (es werden in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt), aber genauso gibt es Einzelfallentscheidungen.

Bei der Addition der Personen zählen nur „die Köpfe“, nicht die geleistete Stundenzahl oder ob es Angestellte sind. Also auch freie Mitarbeiter, Halbtagskräfte etc. sind entsprechend hinzu zu zählen.

Eine „automatisierten Verarbeitung personenbezogener Daten“ liegt z.B. schon dann vor, wenn der Mitarbeiter auf seinem privaten Smartphone berufliche E-Mails abrufen kann oder Namen und Telefonnummern von Kunden gespeichert hat.

Übrigens: Ein betrieblicher Datenschutzbeauftragter muss mit dem in Kraft treten der Datenschutz-Grundverordnung (DSGVO) europaweit spätestens bis Mai 2018 von Unternehmen bestellt werden, deren Tätigkeit einer besonderen Kontrolle bedarf (Art. 35 ff. DSGVO).

Es besteht also erstmals eine europaweit geltende Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten. Sobald ein DSB bestellt ist, sollte auch ein entsprechender Hinweis auf der Internetseite des jeweiligen Unternehmens erfolgen, um sog. Abmahnanwälten den Wind aus den Segeln zu nehmen.

Inwieweit man hier einen internen DSB oder einen Externen nimmt, ist seitens der DSGVO egal.

Bei einem internen DSB handelt es sich i.d.R. um einen bereits vorhandenen Mitarbeiter (der interne DSB darf nicht aus der Geschäftsleitung kommen !), der für teure Schulungen und seiner Arbeit als DSB abgestellt wird. Die Kosten sind entsprechend hoch. Hinzu kommt ein besondere Kündigungsrecht für den DSB, dass mit einem Kündigungsschutz eines Betriebsrats vergleichbar ist.

Externe DSB sind im Vergleich hierzu günstiger, da sofort einsetzbar (also keine Schulungen mehr). Hinsichtlich des „Kündigungsschutzes“ gibt es einige externe DSB, die Vertragslaufzeiten von mind. 2 oder 3 Jahren festlegen, um das Thema Datenschutz auch qualitativ vernünftig und nachhaltig in dem Unternehmen nach vorne zu bringen.

So oder so ist die Einschaltung eines DSB auch eine „Kopfsache“ des Firmeninhabers. Er muss in jedem dieser Fällen einem Dritten Einblick in die zum Teil sensiblen Bereiche der Firma gewähren.

[Ende]