Datenschutz Leitfaden

	TOP 9 Umsetzungspunkte der DSGVO für den Fachhandel	

1. DSGVO = Datenschutzgrundverordnung

Seit dem 25.05.2018 ist die DSGVO anwendbar. Ab jetzt sollte jedes Unternehmen die Umsetzung der Datenschutzanforderungen der DSGVO nachweisen können. Da die DSGVO einige Öffnungsklauseln hat, sollte man auch noch das BDSG neu im Kopf haben, wenn man auf Umsetzung prüft. Nachfolgend exemplarisch die TOP-9-Anforderungen, die Sie unbedingt umsetzen bzw. prüfen sollten – ohne Anspruch auf Vollständigkeit.

2. TOP-9-Umsetzungspunkte der DSGVO

Die jeweiligen Gesetzestexte zur DSGVO und zum BDSG neu finden Sie hier: https://dsgvo-gesetz.de/

Im Artikel 4 der DSGVO finden Sie die Begriffsbestimmungen, z.B. für personenbezogene Daten, Verarbeitungen, Verantwortlicher etc.
Zahlreiche Aufsichtsbehörden bieten Umsetzungsmaterial, Informationen und Vorlagen.

2.1 Klären: Brauche ich einen Datenschutzbeauftragten?

Laut $BDSG_{neu}$ brauche ich einen Datenschutzbeauftragten, wenn sich in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Das ist z.B. der Fall, wenn 10 Mitarbeiter auch jeweils ein E-Mail-Postfach haben.

2.2 Sensibilisieren

Geschäftsführung und Datenschutzbeauftragte sollten mindestens den Führungskreis insoweit sensibilisieren, dass die DSGVO sich direkt auf Unternehmensprozesse auswirkt. Die Führungskräfte schulen dann wiederum Ihre Mitarbeiter. Man sollte sich klarmachen, dass es sich um personenbezogene und auch sensible Daten handelt: Name, Anschrift, Zugehörigkeit zu einem Unternehmen, Kontaktdaten, Alter, Geschlecht, Sozialversicherungsangaben, Gesundheitsdaten z.B. Maßdaten für die Kompressionsstrumpfversorgung.

2.3 Bestandsaufnahme

In welchen Verfahren, bei welchen Tätigkeiten gehe ich mit personenbezogenen Daten um?
Wo sind die sensibelsten Daten? Wenn diese verloren gehen würden oder unbefugter Zugriff erfolgt, wo sind die höchsten Konsequenzen zu befürchten?
Schon haben Sie eine Mini-Risikoabschätzung. Sehen Sie sich zuerst die Prozesse/Tätigkeiten an, in denen Sie kritische Daten verarbeiten.

2.4 Verarbeitungsverzeichnis erstellen (Rechtsgrundlage prüfen)

Die Daten aus der Bestandsaufnahme übertragen Sie nun z.B. in eine Excel-Tabelle und erfassen, auf welcher Rechtsgrundlage (Einwilligung, Vertrag, Gesetz oder berechtigtes Interesse) die Verarbeitung beruht, welche Daten genau verarbeitet werden, wo die Daten herkommen und wer die Empfänger der Daten sind. Muster findet man z.B. hier: bitkom, LDA

2.5 Informations- und Auskunftspflichten prüfen

Bei der Ersterhebung von Daten besteht eine Informationspflicht: Der Verantwortliche teilt der betroffenen Person zum Zeitpunkt der Erhebung mit, zu welchem Zweck die Daten erhoben werden und macht Angaben zu den Empfängern, zur Speicherdauer, zu den Betroffenenrechten und zur Beschwerdestelle. Hier sollte ein Informationsblatt erstellt werden, das Bestandteil des Vertrags wird. So kann man bei Bedarf ebenfalls nachweisen, dass die Informationspflichten eingehalten wurden. Deshalb muss z.B. die Datenschutzerklärung auf der Webseite angepasst werden oder ein Aushang erfolgen, wenn Videoüberwachung eingesetzt wird. Insbesondere sollte man sich Neukundenformulare o.ä. anschauen und ergänzen.

2.6 Einwilligung prüfen

Beruht die Verarbeitung der Daten auf einer Einwilligung des Betroffenen, muss geprüft werden, ob alle Anforderungen erfüllt sind: Information über Widerspruchsrecht, bei Widerspruch ggf. das Löschen von Daten.

2.7 Vertraulichkeitsverpflichtung von Beschäftigen

Auch wenn bestehende Verpflichtungen weiter gelten, sollte man noch einmal alle Mitarbeiter neu verpflichten. Die Verpflichtung auf die Vertraulichkeit löst die Verpflichtung auf das Datengeheimnis ab. Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DSGVO erfolgt.

2.8 Sicherheit der Verarbeitung

Um die sensiblen Patientendaten bei der Verarbeitung zu schützen, sind neben Standardmaßnahmen (z.B. aktuelle Betriebssysteme, Passwortschutz, Virenscanner) weitere Maßnahmen zu treffen. So sollte das Patientendatenverwaltungssystem von anderen PCs getrennt werden und der Zugriff auf Patientendaten auch nur denjenigen gewährt werden, die diesen für ihre Arbeit benötigen. Patientendaten dürfen auch nicht unverschlüsselt per E-Mail gesendet werden!

2.9 Dokumentation des Datenschutzmanagement(system)s

Folgende Fragen sollten Sie sich selber stellen und die Antworten dokumentieren, um ihren Rechenschaftspflichten nachkommen zu können.
Wie sind die Betroffenenrechte organisiert? Was passiert bei einem Sicherheitsvorfall/Datenpanne? Wie sieht mein Löschkonzept aus? Wie sensibilisiere ich meine Mitarbeiter? Wie gewährleiste ich die technische Sicherheit meiner Daten? Wie weise ich nach, dass ich eine Risikoabschätzung für die Verarbeitung durchgeführt habe?

	TOP 9 Umsetzungspunkte der DSGVO für den Fachhandel	

3. Fazit

Datenschutz darf nicht mehr klein gehalten werden. Es war schon immer Chefsache und muss es auch bleiben.

Jeder Mitarbeiter, jeder Projektleiter, jede Führungskraft, jeder ist im Unternehmen für die Einhaltung der Regelungen in seinem Bereich verantwortlich.

Dr. Marion Herrmann
Geschäftsführerin Datenschutz Symbiose

Quellen:

- www.lda.bayern.de
- www.bitkom.org
- www.gdd.de