DSGVO-MASSNAHMENPLAN

So gehen Sie Schritt für Schritt vor

von Michael Rohrlich, Rechtsanwalt und zertifizierter Datenschutzbeauftragter TÜV-Süd

Die EU-Datenschutzgrundverordnung (DSGVO) ist im Mai 2016 in Kraft getreten. Aufgrund einer zweijährigen Übergangszeit hat sie ihre Wirkung am 25. Mai 2018 entfaltet. Sie gilt grundsätzlich für alle Unternehmen – unabhängig von Branche, Größe, Mitarbeiteranzahl oder Umsatz.

Damit Sie Ihr Unternehmen DSGVO-konform machen können, haben wir für Sie einen 6-Punkte-Maßnahmenplan erstellt.

1. Herausforderung annehmen

- **Wissen aneignen**
- **Personal, Zeit und Geld einplanen**
- **Verantwortliche bestimmen**

Die „Vogel-Strauß-Methode“ funktioniert nicht – die DSGVO ist da und muss beachtet werden. Sie enthält das sogenannte Nachweis-Prinzip. Das heißt: Sie müssen in der Lage sein, der Aufsichtsbehörde auf Anfrage zu belegen, dass Sie rechtskonform handeln. Bisher musste Ihnen ein fehlerhaftes Verhalten erst nachgewiesen werden.

Für Sie bedeutet das: Es reicht nun nicht mehr aus, Datenschutz-Maßnahmen im Unternehmen umzusetzen, diese müssen auch dokumentiert werden.

Bauen Sie gezielt Grundlagenwissen auf

Es ist wichtig, dass Sie sich zunächst ein gewisses Grundlagenwissen aneignen, um das Projekt DSGVO effizient in Angriff nehmen zu können. Sie sollten die wichtigsten Begrifflichkeiten und Grundsätze kennen. Zum Beispiel sollten Sie wissen, wer als Betroffener und wer als Verantwortlicher bezeichnet wird und was man unter dem Rechtmäßigkeitsprinzip oder dem Zweckbindungsgrundsatz versteht.

Da stets die Geschäftsführung im Unternehmen für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich ist, sollte insbesondere in dieser Ebene das Basis-Know-how aufgebaut werden. Ist ein Datenschutzbeauftragter vorhanden, muss natürlich auch dieser sein Wissen auf den aktuellen Stand bringen. Aber: nicht jeder muss alles wissen. Die Informationen sollten also nicht nach dem „Gießkannenprinzip“ verteilt werden. Es reicht vollkommen aus, wenn z.B. die Marketingabteilung die Besonderheiten im Bereich Werbung oder die IT-Abteilung die speziellen technikbezogenen Themen kennen.

Planen Sie ausreichend Budget und Personal ein

Insbesondere wenn in Ihrem Unternehmen noch keinerlei Unterlagen in puncto Datenschutz existieren, sollten Sie den Aufwand zur Umstellung auf die DSGVO nicht unterschätzen und entsprechend ausreichende Mittel einplanen. Je größer Ihr Unternehmen ist, desto mehr Personal, Zeit und Geld muss bereitgestellt werden. Während beispielweise in einem kleinen Handwerksbetrieb ein „DSGVO-Manager“ ausreicht, muss in einem

mittelständischen Produktionsbetrieb mit 70 Mitarbeitern hingegen eher ein „Datenschutz-Team“ etabliert werden, in dem je ein Verantwortlicher aus den einzelnen Abteilungen (Personal, Buchhaltung, IT, Marketing etc.) in die DSGVO-Vorbereitung eingebunden wird.

2. Bestandsaufnahme durchführen

- **Prozesse analysieren**
- **Verzeichnis von Verarbeitungstätigkeiten anlegen**
- **Technische und organisatorische Maßnahmen dokumentieren**
- **Liste mit Dienstleistern anlegen**

Zunächst sollten Sie alle Arbeitsabläufe (Prozesse) in Ihrem Unternehmen auflisten, mit denen personenbezogene Daten verarbeitet werden. Typische Prozesse in Unternehmen sind u.a. das Führen von Personalakten, die Buchhaltung, das Durchführen von Bewerbungsverfahren, der Versand von Werbe-Mails, Videoüberwachung im Gebäude oder auch die Vernichtung von Papierunterlagen. Die einzelnen Prozesse sollten zumindest stichpunktartig beschrieben und/oder durch ein Ablaufdiagramm grafisch dargestellt werden (wer ein Qualitätsmanagement-Handbuch oder z.B. eine ISO9001-Zertifizierung o.ä. besitzt, verfügt dadurch schon über eine ganz gute Grundlage). Um die nötigen Informationen zu erhalten, können Sie beispielsweise „geleitete Interviews“ mit den einzelnen Verantwortlichen für Personal, Buchhaltung, IT, Marketing etc. durchführen. Ziel ist es, ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen, das als zentrale Datenschutz-Management-Quelle und ggf. zur Erfüllung Ihrer Nachweispflicht dient.

Dokumentieren Sie Ihre TOM und Dienstleister

Neben den Beschreibungen der Prozesse müssen Sie auch Ihre vorhandenen technischen und organisatorischen Maßnahmen (kurz: TOM) dokumentieren. Dazu zählen beispielsweise eine Zutrittskontrolle zum Gebäude, die Sicherung des Serverraums, die Pflicht zum Anmelden am Computer mittels Kennung und Passwort, der Einsatz von Antiviren-Software und Firewall etc.

Außerdem sollten Sie eine Liste sämtlicher Dienstleister anfertigen, mit denen Sie zusammenarbeiten. Typischerweise sind das Cloud-Anbieter, E-Mail- bzw. Web-Hoster, IT-Dienstleister für die Drucker- / Kopierer-Wartung, externe Lohnbuchhalter, Entsorgungsunternehmen o.ä. Hier müssen zusätzlich zu den eigentlichen Dienstleistungsverträgen auch sogenannte Auftragsverarbeitungsverträge geschlossen werden. Diese Pflicht ist nicht neu und galt auch schon unter dem alten Bundesdatenschutzgesetz (BDSG). Bereits bestehende Verträge sollten Sie daher an die DSGVO anpassen.

3. Lücken erkennen und schließen

- **Verfahrensbeschreibungen gemäß DSGVO vervollständigen**
- **Technische und organisatorische Maßnahmen prüfen & ggf. anpassen**

Nachdem Sie die Bestandsaufnahme durchgeführt haben, müssen die Vorgaben der DSGVO in Ihrem Unternehmen umgesetzt werden, die noch nicht berücksichtigt werden. Das kann durch Maßnahmen geschehen, wie z.B. die Aktualisierung des Betriebssystems, die Wahl einer anderen Cloud-Anwendung oder die Verwendung eines Verschlüsselungszertifikats für die eigene Internetseite (insbesondere wichtig bei Webshops oder auch bei Verwendung eines Kontaktformulars). Unter Umständen ergibt die Prüfung aber auch, dass Sie bislang Werbe-Mails an Kunden verschicken, die Ihnen dafür gar nicht die Einwilligung erteilt haben.

4. Rechtsprüfung durchführen (lassen)

- **Verträge prüfen & anpassen (lassen)**
- **Neue Verträge erstellen (lassen)**
- **Ggf. Rechtsrat einholen**

In jedem Fall sollte eine rechtliche Prüfung erfolgen. Denn personenbezogene Daten dürfen grundsätzlich nicht verarbeitet werden – es sei denn, es liegt eine Einwilligung des Betroffenen vor. Es gibt allerdings einen gesetzlichen Ausnahmetatbestand, oder es bestehen überwiegende berechtigte Interessen des Verantwortlichen. Wichtige Erlaubnistatbestände in der DSGVO erlauben die Datenverarbeitung u.a.:

- zur Erfüllung eines Vertrages (z.B. Durchführung eines Kundenauftrags),
- aufgrund einer rechtlichen Verpflichtung (z.B. steuerrechtliche Aufbewahrungsfristen) oder
- zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe bzw. Ausübung öffentlicher Gewalt (z.B. „Knöllchen“ vom Ordnungsamt).

Der Schutz vor Betrug oder auch das Direktmarketing gelten nach Maßgabe der DSGVO übrigens als berechtigtes Interessen zur Verarbeitung personenbezogener Daten durch Unternehmen.

Geben Sie zu jedem Prozess die Rechtsgrundlage an

Im Rahmen des Verzeichnisses der Verarbeitungstätigkeiten muss zu jedem einzelnen Prozess die entsprechende Rechtsgrundlage angegeben werden, auf deren Basis die Verarbeitung der jeweiligen Daten erfolgt. Daher müssen Sie abklären, um welche Rechtsgrundlagen es sich handelt und ob ggf. Verträge aktualisiert werden müssen.

Darüber hinaus müssen Sie bei bestimmten Verarbeitungstätigkeiten, wie z.B. der Verarbeitung von besonders sensiblen Daten (Gesundheitsdaten o.ä.), Videoüberwachung öffentlicher Bereiche oder Profiling-Maßnahmen, eine sogenannte Datenschutz-Folgenabschätzung durchführen. Hierdurch soll das potentielle Risiko für die Betroffenen ermittelt werden. Je nach Ausmaß des ermittelten Risikos muss dann vor Durchführung der Datenverarbeitung die Aufsichtsbehörde darüber informiert werden.

5. Maßnahmen mit Außenwirkung

- **Online-Datenschutzerklärung anpassen**
- **Ggf. Datenschutzbeauftragten benennen und/oder melden**

Ob Sie die Datenschutzvorgaben einhalten oder nicht, lässt sich am besten anhand der Maßnahmen überprüfen, die für andere „sichtbar“ sind. Ob Sie bei der Abwicklung einer Kundenbestellung alles korrekt beachten, können Außenstehende nur schlecht beurteilen. Aber der Umstand, dass Sie einen Datenschutzbeauftragten brauchen und diesen dann auch der zuständigen Aufsichtsbehörde melden müssen, hat eine gewisse Außenwirkung und ist deshalb auch eher nachvollziehbar. Das Gleiche gilt für eine korrekte Datenschutzerklärung auf Ihrer Internetseite. Hier kann sogar eine automatisierte Prüfung durch die Aufsichtsbehörde oder auch von Ihrer Konkurrenz erfolgen. Diese Punkte sollten daher weit oben auf Ihrer To-Do-Liste stehen und DSGVO-konform umgesetzt werden.

6. Neue Arbeitsabläufe etablieren

- **Geschäftsabläufe zur Wahrung der Betroffenenrechte umsetzen**
- **Auf mögliche Datenpannen vorbereiten**
- **Prozesse zur regelmäßigen Prüfung einrichten**
- **Ggf. Datenschutz-Management-System einführen**

Ein wichtiger Aspekt der DSGVO sind die Rechte der Betroffenen, also der Personen, deren Daten Sie in Ihrem Unternehmen verarbeiten. Sie müssen insbesondere verschiedene Informationsrechte beachten, etwa bei der erstmaligen Erhebung von Daten, bei etwaigen Datenpannen oder eben auch in der Online-Datenschutzerklärung. Außerdem müssen Sie sicherstellen, dass z.B. bei Auskunftsanfragen oder auch bei Datenpannen Ihre Mitarbeiter alle wissen, wie vorzugehen ist. Hierzu können Sie etwa entsprechende Arbeitsanweisungen erteilen oder Prozessbeschreibungen im Datenschutz-Management-System hinterlegen (sofern vorhanden). Auch das frühzeitige Formulieren von Musterschreiben für die Erteilung von Auskünften oder Mitteilungen an die Aufsichtsbehörde ist sinnvoll, damit Sie im Falle des Falles schnell reagieren können.

Aktualisieren Sie Ihre Prozess-Dokumentationen bei Änderungen

Die DSGVO sieht vor, dass Sie Ihre Arbeitsabläufe regelmäßig überprüfen – zumindest immer dann, wenn sich daran etwas ändert oder Sie neue Prozesse einführen. Wechseln Sie z.B. den Mail-Provider oder installieren Sie ein Zeiterfassungssystem für Ihre Mitarbeiter, müssen Sie auch die entsprechenden Änderungen im Verzeichnis von Verarbeitungstätigkeiten aufnehmen.

Rechtsanwalt Michael Rohrlich

www.ra-rohrlich.de