To-do-Liste DSGVO

General Info

14 Maßnahmen, die Sie ergreifen sollten

Sehr lange ist es nicht mehr: Bis zum 25.05.2018 müssen Unternehmen fit für die dann europaweit geltende Datenschutzgrundverordnung (DS-GVO oder DSGVO) sein. Rechtsanwalt Rolf Becker, Partner bei Wienke & Becker, Köln, gibt konkrete Tipps in Form von 14 Maßnahmen, die Sie jetzt umsetzen müssen. Allerdings steckt der Teufel im Detail, und detailreich sind die Anforderungen an die Gestaltung eines Datenschutzmanagementkonzepts.

Der Beweislastumkehr begegnen

War es bislang so, dass etwa eine Datenschutzbehörde Ihnen bei einer Beschwerde oder einem Datenunfall nachweisen musste, dass etwas im Organisationsmanagement Ihres Unternehmens nicht stimmt, ändert sich dies mit der Geltung der DSGVO grundlegend. Können Sie dann in einem solchen Fall nicht nachweisen, dass die Daten datenschutzgerecht verarbeitet wurden, haben Sie ein Problem. Dieses Problem dokumentiert sich am wirkungsvollsten mit der Drohung von Bußgeldern von bis zu 20 Mio. Euro oder 4% des Weltumsatzes, je nachdem, welcher Betrag höher ist.

Der Nachweis erfolgt zunächst einmal durch strikte Einhaltung der Dokumentation Ihrer Datenverarbeitung. Sie müssen die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nachweisen können, z.B. müssen personenbezogene Daten

- auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
- für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, **unverzüglich gelöscht oder berichtigt** werden.

Gelten Ausnahmen?

Diese Frage wird immer zuerst gestellt auf der Suche nach einem Schlupfloch, um den Anforderungen zu entgehen. Es gibt solche Schlupflöcher, aber kaum ein Unternehmen passt hindurch. Nur dann, wenn Sie weniger als 250 Mitarbeiter beschäftigen und „nur gelegentlich“ mit Datenverarbeitung in Ihrem Geschäft beschäftigt sind (letzteres Merkmal fehlt aber schon z.B. bei allen Versandhändlern), könnten Sie mit weniger Pflichten auskommen. Selbst dann könnten noch besondere Risiken oder die Verarbeitung sensibler Daten, wie Kontodaten und dergleichen, wieder den vollen Pflichtenkreis begründen.

To-do-Liste

Die Vorgehensweise kann hier nur thematisch angerissen werden. Die zu behandelnden Themen sind wichtig, aber aufgrund des Umfangs nachstehend nicht zwingend vollständig angesprochen.

1. Bilden Sie in Ihrem Unternehmen ein **Team aus den relevanten Bereichen**, in denen Daten erhoben werden (z.B. Personalabteilung, Lohnbuchhaltung, Kundenservice, Versand/Logistik, Werbeabteilung, IT). Ziehen Sie den Datenschutzbeauftragten von Beginn an hinzu. Binden Sie den Betriebsrat mit ein.

2. Identifizieren Sie die **datenschutzrechtlich relevanten Bereiche** und verabreden Sie, wie und in welcher Art die einzelnen Datenerhebungen, ihre Zwecke, die Berechtigungen und die Löschung der Daten beschrieben werden. Denken Sie auch an das Bewerbermanagement, Reisekostenabrechnungssystem, die Schlüsselverwaltung, Zeiterfassungen, E-Mail-System, Lieferantenverwaltung, Lagerverwaltung, Videoüberwachung, Firewall, Social Media Policy, Kundenkartenprogramme, Trackingmaßnahmen, Direktwerbeformen, personalisierte Werbung usw. Überall dort, wo personenbezogene Daten anfallen, setzt die Dokumentationspflicht an. Das gilt auch für inoffizielle Schubladenlisten und Excel-Tabellen Ihrer Mitarbeiter, mit denen man gleich im Zuge der Arbeiten aufräumen sollte. Vor allem mitarbeitereigene Hardware kann erhebliche Datenschutzprobleme und Risiken mit sich bringen.

3. In diesem Zusammenhang sind sog. Verfahrensverzeichnisse bzw. nach der DSGVO „**Verarbeitungsverzeichnisse**“ zu erstellen. Mit deren Hilfe kann man sich schon bei der Beschreibung vergewissern, ob der gesamte Prozess von der Datenerhebung bis zur Nutzung und Löschung datenschutzkonform erfolgt bzw. welche Maßnahmen getroffen werden müssen, um die Konformität sicherzustellen (**Ist-Soll-Analyse**). Im Verarbeitungsverzeichnis erfolgt die grundlegende Dokumentation aller datenschutzrelevanteren Vorgänge, und die Behörde kann Einsicht in dieses verlangen.

4. Ein Verfahrensverzeichnis kann **auch elektronisch** geführt werden. Es gibt spezielle Softwareangebote, die mit Strukturen und vorgegebenen Inhalten die Erstellung erleichtern können. Das Verfahrensverzeichnis enthält jeweils u.a. Angaben zum Verantwortlichen, zu den Verarbeitungszwecken, den Kategorien der betroffenen Personen und Daten, den Kategorien der Empfänger, Angaben zu Übermittlungen außerhalb der EU (z.B. bei Trackern), Angaben zur Löschung und die Beschreibung der Sicherheitsmaßnahmen (technisch-organisatorische Maßnahmen, sog. TOMs).

5 Identifizieren Sie am besten gleich, auf welcher **Rechtsbasis** die jeweilige Nutzung erfolgt. Entweder sind es gesetzliche Tatbestände, wie die Durchführung des Vertrages, oder es sind Einwilligungen. **Dokumentieren Sie die Einwilligungstexte** und die Prozesse der Einholung der Einwilligung und der Archivierung und lassen Sie diese auf **Rechtskonformität prüfen**. Halten Sie fest, welche **Informationen bei jeder Datenerhebung** vermittelt werden, und lassen Sie rechtlich prüfen, ob diese ausreichen.

6 Erstellen Sie ein **Überwachungskonzept**: Wie, wann und mit welcher Regelmäßigkeit kann zumindest stichprobenartig die Übereinstimmung von Einwilligungen und Eintragungen in Ihrer Software geprüft werden? Welche sonstigen Sicherheitsmaßnahmen werden getroffen? Das Gesetz sieht vor, dass Sie ein **Daten- und Sicherheitsmanagement** implementieren und künftig leben. Die **IT-Sicherheit** steht dabei besonders im Fokus. Sie müssen alle Maßnahmen zusammentragen, die Sie hier ergriffen haben oder noch ergreifen wollen. Das fängt bei dem Zutritt zu den Büroräumen und dem Serverraum an und hört bei der Firewall nicht unbedingt auf. Hier alle relevanten Fakten zusammenzutragen und so zu beschreiben, dass sich die Zusammenstellung künftig pflegen und an Veränderungen anpassen lässt, ist eine besondere Herausforderung. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt eine Reihe von Checklisten und Formulare zur Verfügung.

7 Sie müssen durch Dokumentation nachweisen können, dass das Unternehmen Verfahren und Regeln aufgestellt hat (Richtlinien, Prozesse usw.), die die Informationssicherheit dauerhaft definieren, steuern, überwachen und verbessern. Nachweise für ein gesetzeskonformes Management können auch durch **Zertifizierungen** erbracht werden. Denken Sie frühzeitig über eine solche, dann allerdings möglichst DSGVO-konforme, Zertifizierung zumindest der IT nach.

8 In besonders kritischen Bereichen müssen Sie eine sog. **Datenschutzfolgenabschätzung** implementieren. Das gilt, wenn die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Die EU-Datenschutzgruppe (Art. 29-Gruppe) hat 10 Kriterien festgelegt, bei deren Erfüllung ein solches Risiko besteht. Jede Datenverarbeitung ist vorab daraufhin zu prüfen, ob es voraussichtlich solche Risiken birgt. Das Ergebnis sollten Sie dann im Verfahrensverzeichnis festhalten.

9 Schaffen Sie sich einen **Reaktionsplan für Datenpannen**. Jede **Cyberrisk-Versicherung**, deren Abschluss Sie prüfen sollten, sieht so etwas vor. Halten Sie fest, wer durch wen wann alarmiert wird, welche Sofortmaßnahmen ergriffen werden müssen, was dokumentiert werden muss und wie die Auskunfts- und Meldepflichten an die Behörden realisiert werden. Cyberrisk-Versicherungen bieten gerade bei Datenpannen Schutzkonzepte.

10 Klären Sie, wer bei Ihnen für die **Erfüllung der Betroffenenrechte** zuständig ist. Sorgen Sie für die Ausstattung mit Antwortmustern und Mitarbeiterschulungen. Legen Sie in Zusammenarbeit mit der IT-Abteilung fest, welche Datensätze wie zusammengestellt und in welcher Form zur Übermittlung (vor allem elektronisch) dem Betroffenen auf Verlangen zur Verfügung gestellt werden. Legen Sie dabei fest, welche Daten auf Verlangen einer eingeschränkten Verarbeitung unterliegen, gelöscht oder gesperrt werden und welche archiviert werden müssen. Prüfen Sie die Prozesse und den **Umgang mit Werbewidersprüchen** und dokumentieren Sie das im Verfahrensverzeichnis. Legen Sie fest, wie **die Richtigkeit von Daten** überprüft werden kann.

11 Prüfen Sie die Auswirkungen des neuen **Rechts auf Vergessenwerden**. Wo werden Daten von Betroffenen bei Ihnen an Dritte weitergegeben (Presseerklärung mit Fotos und Namen von Gewinnern eines Gewinnspiels?)? Wer wäre von Ihnen zu informieren, wenn der Betroffene sein Recht geltend machen will? Wie kann man das vermeiden? Gleiches gilt für das Recht auf Datenportabilität, nach dem Sie auf Wunsch des Kunden bestimmte Daten an den Wettbewerb übergeben müssen.

12 Aktualisieren Sie Ihr **Vertragsmanagement**. Alle Verträge mit Dienstleistern, bei denen personenbezogene Daten eine Rolle spielen, müssen rechtlich auf Einhaltung der neuen Datenschutzanforderungen geprüft werden. Das Gesetz verlangt Auftragsdatenverarbeitungsabreden mit ganz bestimmten Mindestinhalten.

13 Gehen Sie schließlich die **Mitarbeiterverpflichtungserklärungen** zum Datengeheimnis an. Die alten stimmen nicht mehr und müssen ohnehin am besten jährlich erneuert werden. Die Mitarbeiter sollten jetzt aus Nachweisgründen auf Vertraulichkeit verpflichtet werden, auch wenn das Gesetz eine ausdrückliche Verpflichtungserklärung außerhalb des öffentlichen Sektors nicht mehr kennt.

14 Implementieren Sie in Zusammenarbeit mit dem Datenschutzbeauftragten regelmäßige Schulungen und Sensibilisierungsmaßnahmen für die Mitarbeiter.

Fazit

Das sind nicht zwingend alle Aufgaben, aber die Darstellung enthält wichtige Schritte, um Ihr Unternehmen fit zu machen und für Sie als Geschäftsführer den Nachweis zu erbringen, dass Sie Ihren Sorgfaltsanforderungen nachgekommen sind. Bußgelder sollen künftig ausdrücklich abschreckende Wirkung haben. Sorgen Sie für Unterstützung durch spezialisierte Unternehmen, die Ihnen auch den Datenschutzbeauftragten stellen, und begleitende anwaltliche Beratung durch spezialisierte Rechtsanwälte.

Docuware

www.docuware.com