

Birgit Pauls und Bernd Sommerfeldt

Basisdatenschutz für Jungunternehmer

Ein Praxisratgeber

Inhaltsverzeichnis

Vorwort

Datenschutzgrundlagen

Technische und organisatorische Maßnahmen

 Zutrittskontrolle

 Zugangskontrolle

 Zugriffskontrolle

 Weitergabekontrolle

 Eingabekontrolle

 Auftragskontrolle

 Verfügbarkeitskontrolle

 Trennungsgebot

 Anpassung an weitere Bestimmungen

 Prüfung der Eignung von Beauftragten bei Dritten

 Dokumentation

 Nachweise Dritter

Verpflichtung und Unterrichtung

Verfahrensübersichten

Überprüfung

Vorabkontrolle / Risiko Folgeabschätzung

Auftragsdatenverarbeitung

Rechte der Betroffenen

Informationspflicht bei der Erhebung

Auskunft

Berichtigung, Löschung und Sperrung

Datenübertragbarkeit

Schadensersatz

Informationspflichten

Internetauftritt und Werbung

Die Aufsichtsbehörde kommt, was tun?

Abkürzungen

Begriffserklärungen

Quellen

Die Autoren

Birgit Pauls

Bernd Sommerfeldt

Vorwort

Datenschutz und IT-Sicherheit sind für jede Unternehmensgröße wichtig und auch rechtlich verbindlich umzusetzen. Im Zuge der schnelllebigen Entwicklung im Informationszeitalter eröffnen sich laufend neue Möglichkeiten, welche von allen Unternehmensgrößen genutzt werden.

Neue Möglichkeiten schaffen auch immer neue Herausforderungen; mit diesen wird das Unternehmen oft allein gelassen und die wichtigsten Schritte werden häufig nicht oder nicht hinreichend vollzogen, wodurch sich unkalkulierbare Risiken für den Unternehmer ergeben.

Dieses Buch wendet sich an alle Unternehmen sowie alle Interessierten und betrieblichen Datenschutzbeauftragten.

Eine vollständige Abhandlung aller Eventualitäten und Sonderfälle ist mit diesem Buch nicht beabsichtigt. Hier wird auf die wichtigsten Punkte eingegangen, die jeder Unternehmer in seinem Betrieb realisieren sollte, unabhängig von der Größe seiner Unternehmung.

Hinweis: Natürlich wendet sich dieses Buch sowohl an Männer als auch an Frauen gleichermaßen, wie auch an das dritte Geschlecht. Auf Formulierungen wie Unternehmer und Unternehmerinnen wurde aus Gründen der Vereinfachung und des besseren Lesens des Buches bewusst verzichtet.

Birgit Pauls und Bernd Sommerfeldt

Tönning / Lübeck im April 2017

Datenschutzgrundlagen

Die wichtigste Grundlage beim Datenschutz ist der gesunde Menschenverstand. Die rechtliche Basis des Datenschutzes in Deutschland wird durch das Grundgesetz gebildet. Auf diesem baut eine Vielzahl weiterer Bestimmungen und Richtlinien auf, z.B. das Bundesdatenschutzgesetz, welches aktuell die wichtigste Norm für Unternehmen und andere private Stellen wie z.B. Vereine darstellt. In anderen Ländern gibt es vergleichbare Anforderungen aus bestehenden Verfassungen sowie Vereinbarungen, welche staatenübergreifend gelten, wie die EU-Datenschutz-Grundverordnung (DS-GVO), die ab 25. Mai 2018 anzuwenden ist.

Unterschiedliche Normen sind für unterschiedliche geografische Zonen herausgegeben worden; die wichtigsten hiervon sind DIN (Deutschland), EN (Europa) sowie ISO (International). Es gibt zahlreiche weitere Normen und Richtlinien, insbesondere in anderen geografischen Zonen. Problematisch wird dies erst, wenn bestimmte Normen, Gesetze und Vorgaben die eigenen Normen nicht berücksichtigen oder sogar zu dessen Bruch verpflichten. Als Beispiel sei hier der Patriot Act zu benennen, bezüglich dessen sich bereits verschiedene Gerichte in den USA und der EU mit Streitfällen beschäftigt haben.

Tatsächlich sind diese unterschiedlichen Handhabungen des Datenschutzes für Unternehmen einer jeden Größe notwendig. Die Globalisierung von Lösungen in der Datenverarbeitung erfordert eine genaue Betrachtung,

welche dieser Lösungen für welchen Bereich einsetzbar ist oder auch ausscheidet.

Als Unternehmer sind Sie dafür verantwortlich, sicherzustellen, dass der Datenschutz lückenlos eingehalten wird und können bei Verletzung des Datenschutzes nicht auf mögliche Bestimmungen in Drittstaaten verweisen.

Was muss ein Unternehmen grundsätzlich tun, um die Mindestanforderungen an den Datenschutz einzuhalten? Die Themen sind recht übersichtlich:

- Überprüfung der Zulässigkeit der Datenverarbeitung und -nutzung
- Mitarbeiterverpflichtung und -unterrichtung
- Technische und organisatorische Maßnahmen zum Datenschutz
- Gesetzeskonforme Auftragsdatenverarbeitung
- Wahrung der Rechte Betroffener
- Verfahrensübersichten erstellen
- Informationspflichten bei Datenschutzpannen
- Ggf. Bestellung eines Datenschutzbeauftragten

Beim Datenschutz geht es immer um den Schutz personenbezogener Daten, d.h. um Angaben über sachliche oder persönliche Verhältnisse einer bestimmten oder bestimmbarer Person. Betriebs- und Geschäftsgeheimnisse ohne Personenbezug fallen nicht unter die Datenschutzgesetzgebung.

Bei der Zulässigkeit der Verarbeitung personenbezogener Daten gilt ein Verbot mit Erlaubnisvorbehalt: Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten ist grundsätzlich verboten, es sei denn