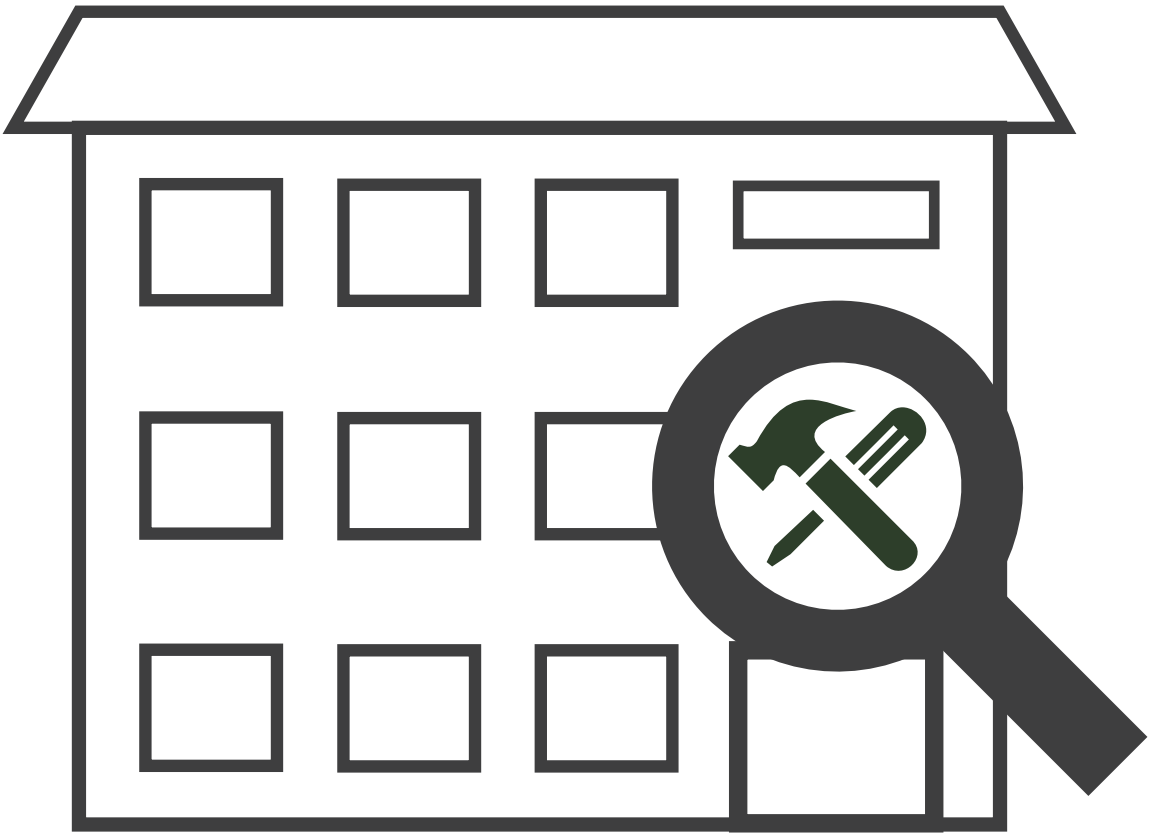
Datenschutz
Einfach
Digital
Gestalten



5 häufige Fehler vermeiden

Der eigene Betrieb

Mit den digitalen Möglichkeiten steigen die administrativen Aufgaben.

Inhaltsverzeichnis

Impressum:

Herausgeber:
Datenschutz | Einfach | Digital | Gestalten
eine Initiative der
Marc Weber Management GmbH

Autor:
Marc Weber

Bezugsquelle:
Marc Weber Management GmbH
Lackerbauerstraße 23
81241 München
www.dedg.de
dedg@marcweber.de
Telefon 089 66 62 86 0
Fax 089 66 62 86 25

Stand:
Februar 2018

Bildnachweis:
Marc Weber Management GmbH

Vorwort

Mit einer weiteren Ausgabe in unserer Reihe „5 häufige Fehler vermeiden“ widmen wir uns diesmal 5 häufig gemachten Fehlern im Unternehmen. Dabei steht die Organisation wie auch die Prozesse und Verfahren auf dem Prüfstand, mit denen personenbezogene Daten verarbeitet werden. Unser Augenmerk legen wir hierbei auf zwei Kernthemen des Datenschutzes. Zum einen beschäftigen wir uns eingangs mit der Bestellung eines Datenschutzbeauftragten und dessen Grundlagen, zum anderen haben wir allgemein die automatisierte Verarbeitung im Blick, wo es in erster Linie um den Einsatz von Computern und Software als Hilfsmittel bei der Verarbeitung von personenbezogenen Daten geht.

Ihr Marc Weber

1. Die Bestellung eines Datenschutzbeauftragten (DSB)

Die Lage

Datenschutz ist eine vielschichtige Angelegenheit, zu der auch die Thematik des Datenschutzbeauftragten als Kernelement in einer Datenschutzorganisation zählt. Entgegen der verbreiteten Annahme, dass Datenschutz erst mit der Bestellung eines Datenschutzbeauftragten beginnt, ist dieser vielmehr eine zusätzliche Anforderung an Unternehmen beim Datenschutzmanagement.
Zahlreiche Unternehmen zeigen neben einer lückenhaften Datenschutzorganisation auch Mängel bei der Bestellung eines betrieblichen Datenschutzbeauftragten. Der Begriff ist dabei noch geläufig, auch die Aufgaben sind halbwegs bekannt, jedoch zeigen sich Wissenslücken bei den Fragestellungen:

Wann ist ein DSB zu bestellen? (Bestellpflicht) und
Welche Voraussetzungen muss der DSB erfüllen? (Qualifikation und Interessenskonflikt).

Diese beiden Kernfragen sind elementar bei der Feststellung einer möglichen Bestellpflicht, sowie der Wahl einer geeigneten Person. In der Praxis macht sich diese Wissenslücke oftmals in einer unsachgemäßen bzw. auch ausbleibenden Überprüfung der Bestellpflicht bemerkbar. Dieses Vorgehen führt zu einer ausbleibenden oder fehlerhaften Bestellung mit weitreichenden Folgen. Mängel bei der Bestellpflicht können zu Bußgeldern und einer Aufforderung zur Bestellung einer geeigneten Person innerhalb kurzer Fristen führen.

Der Ansatz

Die Bestellvoraussetzungen sind im Bundesdatenschutzgesetz (BDSG) eindeutig geregelt. Für einen verbesserten Überblick über die Gesamtthematik halten zahlreiche Aufsichtsbehörden und Institutionen Ratgeber mit den Eckpunkten zu den beiden Kernfragen bereit. Insbesondere die Frage nach den Voraussetzungen der zu bestellenden Person ist von zentraler Bedeutung. Für eine kompetente Ausübung der Tätigkeit ist eine fundierte Fach- bzw. Sachkunde unablässig. Dabei beschränkt sich das Wissen nicht allein auf den juristischen Bereich des Datenschutzes, sondern auch auf den Praktischen. IT und IT-Sicherheitskenntnisse sind in digitalen Zeiten von zentraler Bedeutung um vorliegende Sachverhalte und Prozesse von automatisierter Datenverarbeitung richtig einschätzen und bewerten zu können. Je nach Unternehmen und Prozesse kann es hierbei zu einem umfassenden Anforderungsprofil in der Stellenbeschreibung kommen. Für eine praxisorientierte und kostenoptimale Lösung, gerade auch für kleinere Unternehmen, hält das Bundesdatenschutzgesetzt (BDSG) die Möglichkeit parat, anstatt einer innerbetrieblichen Lösung auch einen externen Datenschutzbeauftragten zu verpflichten.

Tipp:
Auf unserer Website finden Sie einen digitalen Fragebogen zur Feststellung, ob Ihr Unternehmen zur Bestellung eines Datenschutzbeauftragten verpflichtet ist oder nicht.

2. Hard- und Softwarewartung ohne Auftragsdatenverarbeitung

Die Lage

Meist, gerade auch in kleineren Unternehmen, gehört IT-Fachkenntnis nicht zwangsläufig zu den Kernkompetenzen der Belegschaft. Daher hat es sich im Laufe der vergangenen Jahre eingebürgert, externe Dienstleister nach Bedarf mit der Wartung der IT-Infrastruktur zu betrauen oder bei konkreten Problemen zu kontaktieren. Eine gelungene Arbeitsteilung in einer zunehmend komplexer werdenden Technologiewelt mit stetig kürzer werdenden Zyklen an Updates und Neuerungen.

Geht ein Unternehmen mit personenbezogenen Daten um, so ist diese (Fern-)Wartung unter datenschutzrechtlichen Gesichtspunkten zu prüfen und zu bewerten. Ein oftmals außer Acht gelassener Punkt, da im Grunde genommen keine direkte Datenverarbeitung durch den Dienstleister stattfindet. Dennoch für den Datenschutz relevant, da, entsprechend der Vorschrift, durchaus ein Zugriff und eine Einsichtnahme der personenbezogenen Daten möglich ist. Neben technischer und organisatorischer Maßnahmen, ist auch ein entsprechendes Vertragswerk auszuarbeiten, eine Vereinbarung über eine Auftragsdatenverarbeitung (ADV). Derartige Vereinbarungen sind obligatorische Prüfkriterien bei Kontrollen mit eingeleiteten Sanktionen bei Verstößen.

Der Ansatz

Der vertragliche Teil mit der Vereinbarung über eine Auftragsdatenverarbeitung (ADV) ist verhältnismäßig leicht abzudecken. Gut ausgearbeitete Muster und Vorlagen sind bei Aufsichtsbehörden oder datenschutzorientierten Institutionen verfügbar und müssen nur an wenigen Stellen auf den individuellen Sachverhalt hin angepasst werden. Teil einer derartigen Vereinbarung sind auch die technischen und organisatorischen Maßnahmen auf Seiten des Dienstleisters, die auch vom Auftraggeber eine gewisse Kompetenz in der IT und IT-Sicherheit abverlangen. Diese Maßnahmen sind vorab beim Dienstleister zu kontrollieren und zu bewerten. In einer Übersicht werden die Ergebnisse und Maßnahmen festgehalten, die als Anlage der Vereinbarung beizufügen ist. Gerade die Fernwartung, bei der der externe Dienstleister nicht vor Ort tätig wird, sondern sich über Schnittstellen auf das System aufschaltet, ist in einem besonderen Maße von der Auftragsdatenverarbeitung betroffen. Neben einer Erstkontrolle vor der Aufnahme der eigentlichen Tätigkeit, sind regelmäßige Kontrollen der verantwortlichen Stelle (Auftraggeber) beim Dienstleister (Auftragnehmer) vorzunehmen.

Tipp:
Der „Stand der Technik“ ist für die Beurteilung und den zu treffenden Maßnahmen von entscheidender Wichtigkeit. Die stetige Veränderung der Technik sowie der Möglichkeiten ist auch unter Sicherheitsaspekten bei Kontrollen zu berücksichtigen.

3. Lückenhafte Verpflichtung auf das Datengeheimnis

Die Lage

Die Verarbeitung von personenbezogenen Daten findet in den meisten Fällen „noch“ unter der Mitwirkung der Beschäftigten eines Unternehmens statt. Für einen effizienten und prozessorientierten Arbeitsablauf ist es übliche Praxis, die Beschäftigten in die unternehmensspezifischen Besonderheiten einzuweisen und im Umgang mit den vorhandenen Systemen zu schulen. Ein alltägliches Vorgehen, was Unternehmen bereits aus eigenem wirtschaftlichem Interesse verfolgen. Der Fokus liegt meist jedoch auf der Handhabung des Prozesses, wobei Datenschutzaspekte besten Falls am Rande erwähnt werden. Datenschutzrechtliche Details bzw. die Grundsätze des Datenschutzes werden nur selten vermittelt. In der täglichen Praxis spiegelt sich diese Haltung in den Mustern von Arbeitsverträgen und den mitgeltenden Unterlagen wieder. Diese beinhalten häufig eine schriftliche Verpflichtung auf das Datengeheimnis mit Auszügen an Paragraphen aus den betroffenen Gesetzen. Ohne individuelle Betreuung und Schulung des Beschäftigten, mag dies ein erster richtiger Schritt sein, jedoch noch nicht ausreichend, um den gesetzlichen Anforderungen nachzukommen.

Der Ansatz

Unternehmen, die mit personenbezogenen Daten umgehen und Beschäftigte mit der Verarbeitung betrauen, haben diese vor der Aufnahme der Tätigkeit auf das Datengeheimnis zu verpflichten. Diese gesetzliche Forderung ist an keine Form gebunden, jedoch hat es sich in der Praxis bewährt, schriftliche Verpflichtungen aufzusetzen, die entsprechend von den Parteien unterzeichnet werden. Dies ermöglicht zum einen eine eindeutig einheitliche Grundsatzformulierung für alle Beschäftigten, zum anderen lässt sich bei Kontrollen oder späteren Unklarheiten ein Nachweis erbringen. Neben diesen Formalien stehen verantwortliche Stellen in der Pflicht, die Beschäftigten im Umgang mit personenbezogenen Daten und den Datenschutzgrundsätzen zu schulen und regelmäßig zu unterweisen.

Tipp:
Das ADV-Management gehört bei manchen Aufsichtsbehörden zum Standardprüfkatalog und Mängel werden häufig mit Bußgeldern belegt.

4. Lückenhaftes Verfahrensverzeichnis

Die Lage

Der Umgang mit personenbezogenen Daten erfolgt im Unternehmen in aller Regel nach definierten und stets den gleichen Prozessen und Verfahren. Entsprechend dem Bundesdatenschutzgesetz (BDSG) ist jede verantwortliche Stelle, die personenbezogene Daten automatisiert verarbeitet, dazu angehalten, eine Übersicht zu führen. Eine derartige Übersicht ist, im Falle einer Bestellpflicht eines Datenschutzbeauftragten, diesem als Tätigkeitsgrundlage auszuhändigen oder auf Antrag einem Außenstehenden zur Verfügung zu stellen. Zudem ermöglicht die Übersicht eine schnelle Einarbeitung und Orientierung in die Verfahren des Unternehmens. Neben der Problematik, dass keine Übersicht geführt wird, stellt sich in der digitalen Zeit zunehmend die Herausforderung, bestehende Verzeichnisse auf dem aktuellen Stand zu halten.

Der Ansatz

Das Führen von Verfahrensverzeichnissen ist unter diversen Gesichtspunkten ein besonderes datenschutzrechtliches Themengebiet für verantwortliche Stellen. Ausführliche Übersichten sind einem etwaigen bestellten Datenschutzbeauftragten zur Verfügung zu stellen, schlankere Versionen auf Antrag jedem Interessierten auszuhändigen. Dabei sorgen die unterschiedlichen Varianten für die nötige Transparenz der Prozesse und für eine Übersicht über die Rechtmäßigkeit von Verarbeitungstätigkeiten. Das Bundesdatenschutzgesetz (BDSG) hält hierzu eine 8– bzw. 9-Punkte Liste der Pflichtinhalte eines konformen Verfahrensverzeichnisses bereit.

5. Verfahren ohne Vorabkontrolle

Die Lage

Die aktuellen Datenschutzverordnungen und –vorschriften haben im Kern den Blick auf die automatisierte Verarbeitung an personenbezogenen Daten gerichtet. Zahlreiche, von den verantwortlichen Stellen zu bewältigenden Herausforderungen beziehen sich konkret auf diesen Verarbeitungsumstand. Dabei ist in der heutigen softwaregespickten Zeit diese Hürde schnell genommen. So alltäglich und selbstverständlich wie der Einsatz von IT und Software ist, so schnell sind Anforderungen des Datenschutzes aus den Augen verloren. Der Einsatz von neuen Verfahren (Software und Applikationen) ist stets vor der Inbetriebnahme auch unter Datenschutzgesichtspunkten zu prüfen und zu bewerten. Dabei ist zu klären, ob das anstehende Verfahren einer Vorabkontrolle unterzogen werden muss. Vielfach findet in der Praxis weder eine Prüfung zur Vorabkontrolle, noch im Bedarfsfall die eigentliche Vorabkontrolle selbst statt.

Der Ansatz

Automatisierte Verarbeitungsprozesse haben ein deutlich höheres datenschutzrechtliches Risiko für Betroffene als anderweitige Verfahren. Aus diesem Anlass sind verantwortliche Stellen in der Pflicht, geplante Prozesse vor der eigentlichen Inbetriebnahme genauestens zu prüfen und zu bewerten. Dabei sind die Risiken für die Rechte und Freiheiten der Betroffenen ein zentrales Kernelement im Prüfprozess. Im Rahmen der Risikoanalyse ist abzuwägen, ob eine Vorabkontrolle zum Tragen kommt. Besteht ein entsprechendes Risikoniveau bei dem geplanten Verarbeitungsvorgang, führt kein Weg an der eigentlichen Vorabkontrolle vorbei. Eine besondere Herausforderung, denn die Durchführung dieser Kontrolle obliegt alleinig dem bestellten Datenschutzbeauftragten. Verantwortliche Stellen, die bis dato nicht zu einer Bestellung verpflichtet waren, geraten nun in die verbindliche Bestellpflicht. Dabei spielen anderweitige Voraussetzungen, wie bspw. die Beschäftigtenzahl, keine Rolle mehr.

Datenschutz ist die wahre Herausforderung der digitalen Epoche.