# Die 7 „populärsten“ Mythen der DSGVO

von RA Heike Mareck, Externe Datenschutzbeauftragte, Dortmund

|„Wahrheit oder Mythos? Vieles, was zur neuen Datenschutz-Grundverordnung in Blogs und Foren umhergeistert, sind Halbwahrheiten. Wir haben die derzeit 7 populärsten DSGVO-Irrtümer aus Unternehmen, Betrieben und Kanzleien einem Fakten-Check unterworfen. |

**Mythos Nr. 1: Kein Computer im Betrieb = keine DSGVO**

Das stimmt schon einmal nicht. Auch Betriebe, die „nur“ mit einem Kunden-Karteikasten – geordnet nach einem System, zum Beispiel Namen – arbeiten, sind von der DSGVO betroffen. Insbesondere kleine Betriebe sowie Vereine sind hier häufig falsch informiert. Ausgenommen sind lediglich Daten für ausschließlich persönliche und familiäre Tätigkeiten.

**Mythos Nr. 2: Es reicht, wenn ich meine Mandanten mündlich darüber informiere, dass ich den Datenschutz einhalte!**

Nein, das reicht nicht. Denn der Informationsumfang ist dafür einfach zu hoch. Nach Art. 12 DSGVO muss der Kanzleiinhaber geeignete Maßnahmen treffen, um der betroffenen Person alle Informationen zur Verarbeitung „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu übermitteln. Damit haben Mandanten einen Informationsanspruch bei Erhebung der Daten. Kanzleien können diese Hürde elegant lösen, indem sie die Informationen im Steuerberatungsvertrag zur Verfügung stellen (zum Beispiel in einer Anlage zum Vertrag). Diese Pflichten gelten für jede Person, deren personenbezogene Daten durch den Steuerberater verarbeitet werden.

Art. 13 Abs. 1 DSGVO regelt, welche Informationen mitgeteilt werden müssen. Falls die personenbezogenen Daten zu einem anderen als dem ursprünglichen Zweck weiterverarbeitet werden sollen, werden dem Betroffenen vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen zur Verfügung gestellt. Die zuvor genannten Informationspflichten bestehen nicht, wenn und soweit der Betroffene bereits über die Informationen verfügt.

**Mythos Nr. 3: Einer Datenschutz-Verpflichtung für meine Mitarbeiter bedarf es nicht, da dies bereits im Arbeitsvertrag steht**

Jein! In den meisten Arbeitsverträgen findet sich ein Hinweis auf die Geheimhaltung. Meist ist er wie folgt formuliert: „Der Arbeitnehmer ist verpflichtet, für die Dauer der Beschäftigung absolute Geheimhaltung über den Arbeitsvertrag, seine Vergütung, von Arbeits- und Kündigungszeiten sowie von Kündigungsfristen zu wahren. Gleiches gilt für alle

Angelegenheiten und Vorgänge, die ihm im Rahmen seiner Tätigkeit zur Kenntnis gelangen, während und nach Beendigung des Arbeitsverhältnisses."

Bei der Verpflichtung auf das Datengeheimnis geht es nicht nur um die im Arbeitsvertrag stehenden Vorschriften zur Geheimhaltung. Eine Verpflichtung auf das Datengeheimnis geht noch viel weiter. Sie umfasst die Vertraulichkeit von betrieblichen Inhalten, Tätigkeiten und zu schützenden personenbezogenen Daten und Vorgängen – der Mandanten, Kunden, Bewerber und Beschäftigten.

§ 5 BDSG a. F. sah eine sogenannte „Verpflichtung auf das Datengeheimnis" vor. Diese fehlt so explizit in der DSGVO. Aber nach Art. 29 DSGVO dürfen Beschäftigte eines Unternehmens personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten. Ausnahme: Eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor. Ergänzend dazu regelt Art. 32 Abs. 4 DSGVO, dass der Verantwortliche oder Auftragsverarbeiter Schritte unternehmen muss, um sicherzustellen, dass ihm unterstellte Personen (insbesondere seine Beschäftigten), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten (es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor). Wie diese gesetzliche Verpflichtung umzusetzen ist, ist nicht verbindlich geregelt. Auch die Datenschutzkonferenz empfiehlt daher, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen.

Der Kreis der zu verpflichtenden Personen ist weit auszulegen. Insbesondere sind ergänzend zum regulären Mitarbeiterstamm auch Auszubildende, Praktikanten, Leiharbeiter und ehrenamtlich Tätige mit einzubeziehen. Zur Verpflichtung gehört auch eine Belehrung über die sich ergebenden Pflichten.

Weitere Informationen hierzu finden Sie im Kurzpapier der Datenschutzkonferenz unter www.iww.de/s1856.

Selbst wenn die DSGVO keine bestimmte Form der Verpflichtung vorschreibt, sollte aus Nachweisgründen ein Formular verwendet werden. Dabei kann die Verpflichtung schriftlich oder in einem elektronischen Format erfolgen.

**Mythos Nr. 4: Einzelbetriebe brauchen keine Verarbeitungsverzeichnisse**

Nein. Jeder Verantwortliche muss ein Verzeichnis seiner Verarbeitungstätigkeiten führen (Art. 30 Abs. 1 DSGVO). Auch ein Betrieb, der nur aus einem Mitarbeiter besteht, muss ein

Verzeichnis der Verarbeitungstätigkeiten führen, da er in der Regel nicht nur gelegentlich Daten verarbeitet.

**Mythos Nr. 5: Das Verarbeitungsverzeichnis muss auf die Website**

Nein! Das Verarbeitungsverzeichnis bzw. „das Verzeichnis der Verarbeitungstätigkeiten" muss nur gegenüber der Aufsichtsbehörde vorgelegt werden, damit die Verarbeitungsvorgänge anhand des Verzeichnisses kontrolliert werden können (Art. 30 Abs. 4 DSGVO, Erwägungsgrund 82).

**Mythos Nr. 6: Der Datenschutzbeauftragte wird auf der Website benannt**

Jein! Der Betriebs-/Kanzleiinhaber muss die Kontaktdaten des Datenschutzbeauftragten veröffentlichen. Dieses sollte unter anderem auf der Website erfolgen. Hierbei reicht es aus, wenn die Kontaktdaten genannt werden. Art. 37 Abs. 7 DSGVO gibt nicht verpflichtend vor, dass auch der Name zu den zu veröffentlichenden Daten gehört.

In jedem Fall müssen die Kontaktdaten der Aufsichtsbehörde mitgeteilt werden (Art. 37 Abs. 7 DSGVO). Die Mitteilung erfolgt über ein elektronisches Portal in einem automatisierten Meldeverfahren über die Aufsichtsbehörden der jeweiligen Länder. Soweit ersichtlich, haben alle Bundesländer (bis auf Niedersachsen; Stand 22.7.18) dieses bereits umgesetzt.

**PRAXISTIPP |** Da die Aufsichtsbehörden teilweise Fristen (zum Beispiel hat Hessen eine 3-monatige Frist, gültig seit dem 14.5.18) gesetzt haben, sollte man zügig melden. Wo Sie elektronisch melden müssen, erfahren Sie auf der Website der jeweiligen Aufsichtsbehörde. Die Kontaktdaten der Aufsichtsbehörden und deren Websites finden Sie über folgenden Link: www.iww.de/s1857.

**Mythos Nr. 7: Bewerberdaten müssen immer sofort zurückgeschickt, werden, sie dürfen nicht gespeichert werden**

Nein, da nicht ausgeschlossen werden kann, dass es aufgrund einer Ablehnung durch den Personalverantwortlichen im Betrieb bzw. in der Kanzlei zu einem arbeitsgerichtlichen Verfahren nach dem AGG kommt. Werden diese Unterlagen sofort vernichtet, fehlen dem Personalverantwortlichen entscheidende Informationen. Grundsätzlich ist zu beachten, dass Bewerberdaten unter § 26 BDSG n. F. fallen. Bei der Speicherdauer sollte daher beachtet werden, dass diese maximal 4 bis 6 Monate ab Zugang des Ablehnungsschreibens aufbewahrt werden dürfen und danach gelöscht werden müssen.