DATENSCHUTZ

10 „populäre“ Mythen der DS-GVO

von RA Heike Mareck, Externe Datenschutzbeauftragte, Dortmund

„Kein Computer im Betrieb = keine DS-GVO“, „Die TOMs beziehen sich nur auf die Computer im Unternehmen“, „Ein SSL-Zertifikat sorgt lediglich für ein besseres Google-Ranking“. Die derzeit 10 populärsten DS-GVO-Irrtümer aus Unternehmen, Betrieben und Kanzleien im Fakten-Check.

1. Kein Computer im Betrieb = keine DS-GVO

Insbesondere kleine Betriebe und Vereine liegen hier häufig falsch

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

2. Die TOMs beziehen sich nur auf die Computer

Einige Fragen zur Zutrittskontrolle

Nein. Für die Aufsichtsbehörden sind durchaus auch die Maßnahmen der Zutrittskontrolle in das Gebäude wichtig. Hierbei sind unter anderem folgende Fragen interessant:

- Wer hat Zugang zum Bürohaus und auch zu den Büroräumen?
- Erfolgen die Schlüsselvergabe und das Schlüsselmanagement nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt?
- Werden einem Beschäftigten Zutrittsberechtigungen erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung entsprechend angefordert wurde?
- Erhalten Besucher erst Zutritt zum Bürohaus und den Büroräumen, wenn ihnen durch den Empfang oder einen sonstigen Beschäftigten die Tür geöffnet wird?
- Kann der Empfang die Eingangstür einsehen und trägt Sorge dafür, dass jeder Besucher sich beim Empfang meldet?
- Dürfen sich Besucher ohne Begleitung in den Büroräumen frei bewegen?
- Sind die Eingänge und Fenster des Bürohauses und auch der Büroräume eventuell gesichert?

Die TOMs regeln dabei nicht nur den reinen IT-Bereich.

3. Ein SSL-Zertifikat sorgt für ein besseres Google-Ranking

SSL-Zertifikat für das Kontaktformular auf der Website wichtig

Nicht nur, dieses ist lediglich ein weiterer Nebeneffekt. Das SSL-Zertifikat dient vornehmlich der Sicherheit bei der Übertragung von Daten. Webseiten, auf denen Kontaktformulare verwendet werden, müssen anerkannte Verschlüsselungsverfahren implementieren. Seit dem 1.1.16 gilt die Pflicht für

eine SSL-Verbindung („https://“) zu Websites mit Kontaktformularen (§ 13 Abs. 7 TMG). Diese Pflicht gilt allgemein für Websitebetreiber, welche personenbezogene Daten mittels ihrer Website erheben. Das TLS-Protokoll (Transport Layer Security) ist ein Sicherheitsprotokoll, welches auf SSL aufbaut.

Beim Kontaktformular werden Daten nach Art. 4 Nr. 1 DS-GVO verarbeitet

Wird ein Kontaktformular genutzt, werden personenbezogene Daten nach Art. 4 Nr. 1 DS-GVO verarbeitet. Art. 32 Abs. 1 Buchst. a DS-GVO konkretisiert den Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 Buchst. f DS-GVO. Art. 32 Abs. 1, Buchst. a DS-GVO legt fest, dass unter der Berücksichtigung vom Stand der Technik, der Implementierungskosten, Art, Umfang und Zweck der Verarbeitung, sowie Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen vom Website-Betreiber technische und organisatorische Maßnahmen getroffen werden müssen. Art. 32 Abs. 1 Buchst. a DS-GVO benennt ausdrücklich die Verschlüsselung personenbezogener Daten als eine solche technische Maßnahme.

Eine Verschlüsselung mittels eines SSL- oder TLS-Protokolls für Kontaktformulare auf Websites entspricht dem Stand der Technik und wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen.

Weitere Informationen des BSI unter www.iww.de/s1855.

DOWNLOAD
www.iww.de/s1855
SSL-Kriterien

4. Jeder Kunde muss eine Einwilligung unterschreiben

Art. 6 Abs. 1 Buchst. b DS-GVO ist wichtig

Nein. Für die Verarbeitung der Daten von Kunden/Mandanten zum Zwecke eines Angebots oder eines Vertrags muss von ihnen keine Einwilligung eingeholt werden. Das Gesetz erlaubt die Verarbeitung zum Zwecke der Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen auch ohne Einwilligung (Art. 6 Abs. 1 Buchst. b DS-GVO). Die Kunden müssen aber bei der Erhebung ihrer Daten über die Verarbeitung ihrer Daten durch das Unternehmen/die Kanzlei informiert werden (hierzu mehr im 5. Mythos).

5. Es reicht, wenn ich meine Kunden/Mandanten mündlich darüber informiere, dass ich den Datenschutz einhalte!

Informationsanspruch des Kunden/Mandanten

Nein, das reicht nicht. Denn der Informationsumfang ist dafür einfach zu hoch Nach Art. 12 DS-GVO muss der Betriebs-/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 Kunden bzw. Mandanten einen Informationsanspruch bei Erhebung der Daten. Kanzleien können diese Hürde elegant lösen, indem sie die Informationen im Mandatsvertrag zur Verfügung stellen (zum Beispiel in einer Anlage zum Vertrag). Diese Pflichten gelten für jede Person, deren personenbezogene Daten durch den Rechtsanwalt verarbeitet werden.

Art. 13 DS-GVO regelt, welche Informationen mitgeteilt werden

Art. 13 Abs. 1 DS-GVO 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 gem. Abs. 2 zur

Verfügung gestellt (Art. 13 Abs. 3 DS-GVO). Die zuvor genannten Informationspflichten bestehen nicht, wenn und soweit der Betroffene bereits über die Informationen verfügt (Art. 13 Abs. 4 DS-GVO).

6. Eine Datenschutz-Verpflichtung für meine Mitarbeiter braucht 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, seiner 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."

Es geht um mehr als das, was im Arbeitsvertrag steht

Bei der Verpflichtung auf das Datengeheimnis geht es nicht nur um die im Arbeitsvertrag bestehenden 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 DS-GVO. Aber nach Art. 29 DS-GVO 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 DS-GVO, 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.

Kreis der Personen ist groß: Azubis, Praktikanten, Leih-ArbN

Der Kreis der zu verpflichtenden Personen (die DS-GVO spricht insoweit von „unterstellten natürlichen 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.

DOWNLOAD
www.iww.de/s1856

Selbst wenn die DS-GVO keine bestimmte Form der Verpflichtung vorschreibt, sollte aus Nachweisgründen ein Formular verwendet werden. Dabei kann die Verpflichtung schriftlich oder in einem elektronischen Format erfolgen. Ein Muster der Verpflichtung zur Vertraulichkeit finden Sie unter ak.iww.de (unter Downloads).

DOWNLOAD
ak.iww.de

7. Einzelbetriebe brauchen keine Verarbeitungsverzeichnisse

Nein. Jeder Verantwortliche muss ein Verzeichnis seiner Verarbeitungstätigkeiten führen (Art. 30 Abs. 1 DS-GVO). 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.

Jeder Verantwortliche muss Verzeichnis führen

8. 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 DS-GVO, Erwägungsgrund 82).

Nur der Aufsichtsbehörde vorzulegen

9. 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 DS-GVO 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 DS-GVO). 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.

Kontaktdaten an die Aufsichtsbehörde

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.

Melden Sie zeitnah

10. 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 4-6 Monate ab Zugang des Ablehnungsschreibens aufbewahrt werden dürfen und danach gelöscht werden müssen.

Nach 4-6 Monaten löschen