BVIK-TOOLS / FEB. 2018

Bundesverband Industrie Kommunikation e.V.

CHECKLISTE DATENSCHUTZ

ZUR SCHNELLEN „STATUS QUO“-ÜBERPRÜFUNG DES UNTERNEHMENS HINSICHTLICH EU-DSGVO 2018

VORBEMERKUNG

Ausgangslage

Am 25.05.2018 läuft die Frist zur Umsetzung der Vorgaben in der europäischen Datenschutz-Grundverordnung (DSGVO) und im neuen Bundesdatenschutzgesetz (BDSG-neu) ab. Ab diesem Zeitpunkt muss jedes Unternehmen – egal ob Kleinunternehmen, Freiberufler, KMU, Verein, Mittelstand oder Konzern – die neuen Regelungen umgesetzt haben. Wichtig für Sie zu wissen: Die DSGVO regelt den Schutz personenbezogener Daten und ist bereits seit Mai 2016 verabschiedet, die Übergangsfrist endet am 25.05.2018.

Jetzt zu handeln ist das Gebot der Stunde.

Personenbezogene Daten dürfen künftig nur verwendet werden, wenn eine der Voraussetzungen des Art. 6 DSGVO die jeweilige Verarbeitung explizit legitimiert. Bei der Flut an Daten, die heutzutage an verschiedensten Stellen im Unternehmen erfasst, gespeichert, genutzt oder auch gelöscht werden, ist es das Gebot der Stunde, vor allem die Prozesse in Marketing und Vertrieb rechtlich an die geforderten Datenschutzrichtlinien anzupassen. Bei Verstößen gegen das europaweit geltende Gesetz drohen empfindliche Strafen in Höhe von bis zu 4 Prozent des Jahresumsatzes.

Viele Hürden sind zu nehmen.

Marketer stehen vor der großen Herausforderung, geeignete Maßnahmen zum technisch-organisatorischen Schutz der Daten und zur rechtskonformen Nutzung zu ergreifen, ohne sich jeglichen Handlungsspielraum in ihrer Kundenkommunikation zu nehmen. Eine nachhaltig erfolgreiche Strategie erfordert in jedem Fall die intensive Zusammenarbeit von Datenschutzbeauftragten, IT, Marketing und Vertrieb.

e-Privacy Verordnung

Es kommt erschwerend hinzu, dass auch unter Datenschutz-Profis eine gewisse Unsicherheit in der genauen Auslegung der Richtlinien besteht, da es noch keine Rechtsprechung zur neuen Gesetzeslage mit eindeutigen Präzedenzfällen gibt. Auch die sog. zusätzlich diskutierte „e-Privacy Verordnung“ zur Verarbeitung und Speicherung elektronischer Kommunikationsdaten (z.B. Cookies) ist noch nicht verabschiedet. Änderungen bis zum Inkrafttreten (vermutlich nicht vor 2019) sind zu erwarten.

Hinweis: Die Checkliste wurde auf Grundlage sorgfältiger Recherche erstellt. Dennoch können der Autor oder der bvik keine Haftung für die Richtigkeit und Vollständigkeit der Informationen übernehmen.

CHECKLISTE

In der folgenden Checkliste können Sie schnell und einfach selbst überprüfen, wie der Status quo in Ihrem Unternehmen ist und wo noch Lücken vorhanden sind. Das Ergebnis ist eine gute Vorbereitung für die anschließende Umsetzung der notwendigen Schritte.

1. Verantwortlichkeit im Unternehmen

Die verantwortliche Stelle im Unternehmen ist immer die Geschäftsführung. Diese Verpflichtung kann auch nicht vertraglich z.B. auf einen Mitarbeiter übertragen werden.

	ja	nein
■ Wurden die Geschäftsleitung, das Management und die Mitarbeiter für das Thema sensibilisiert?	☐	☐
■ Gibt es bereits im Unternehmen jemanden, der für Datenschutzthemen zuständig ist?	☐	☐
■ Gibt es bereits einen bestellten Datenschutzbeauftragten?	☐	☐
■ Haben Sie im Unternehmen für jede Verarbeitung einen Nachweis über die Rechtmäßigkeit?	☐	☐
■ Gibt es im Unternehmen ein Datenschutz-Managementsystem?	☐	☐

2. Status quo feststellen

	ja	nein
■ Gibt es bereits ein Verzeichnis der Verarbeitungstätigkeiten?	☐	☐
■ Falls ja, wer ist für das Verzeichnis verantwortlich? Wird es regelmäßig aktualisiert?	☐	☐
■ Falls nein, wurde eine Bestandsaufnahme aller Verfahren und Prozesse gemacht, in denen personenbezogene Daten verarbeitet werden?	☐	☐
■ Haben Sie bereits einen Abgleich des Ist-Zustandes mit dem Soll-Zustand (nach DSGVO) erstellt (GAP-Analyse)?	☐	☐

3. Externe Dienstleister / Cloud-Services

	ja	nein
■ Gibt es externe Dienstleister, die im Auftrag personenbezogene Daten verarbeiten? Dies kann z. B. auch ein Lettershop sein, der ein Briefmailing produziert.	☐	☐
■ Werden Cloud-Services im Unternehmen genutzt?	☐	☐
■ Falls ja, haben Sie mit allen Auftragsverarbeitern eine erforderliche Vereinbarung abgeschlossen?	☐	☐

4. Rechtsgrundlage für die Verarbeitung personenbezogener Daten

	ja	nein
■ Haben Sie alle Verarbeitungen von personenbezogenen Daten in Ihrem Unternehmen auf die Zulässigkeit überprüft?	☐	☐
■ Ist für alle Verarbeitungen eine Rechtsgrundlage nach neuem Recht vorhanden?	☐	☐
■ Existiert bereits eine Dokumentation der Rechtsgrundlage?	☐	☐
■ Sind Ihre Einwilligungserklärungen für Betroffene an die Anforderungen der DSGVO angepasst, vor allem z.B. die erweiterten Informationspflichten und die Möglichkeit des jederzeitigen Widerrufs der Einwilligung (z.B. für E-Mail-Werbung)?	☐	☐
■ Sind Ihre Datenschutzerklärungen (z.B. auf der Webseite) an die neuen Anforderungen angepasst?	☐	☐

5. Transparenz

	ja	nein
■ Werden die Betroffenen vor der geplanten Verarbeitung ihrer Daten umfassend und rechtzeitig informiert?	☐	☐
■ Werden z.B. Zweck und Zweckänderung der erstmaligen Erhebung oder der geplanten Datenverarbeitung transparent kommuniziert?	☐	☐
■ Ist ein Löschkonzept mit entsprechenden Löschfristen vorhanden?	☐	☐

6. Informationspflichten und Betroffenenrechte

	ja	nein
■ Informieren Sie die Betroffenen über die beabsichtigte Verarbeitung ihrer Daten? Diese Information muss in einer klaren und einfachen Sprache und in leicht zugänglicher Form erfolgen.	☐	☐
■ Haben Sie die Betroffenenrechte sichergestellt?	☐	☐

Folgende Informationen sind besonders wichtig:

- Kontaktdaten des Datenschutzbeauftragten (wenn ein DSB erforderlich ist)
- Speicherdauer der Daten
- Zweck der Verarbeitung
- Datenherkunft
- Recht auf Widerruf der Einwilligung
- Recht auf Beschwerde bei der Aufsichtsbehörde

7. Umgang mit Risiken

	ja	nein
■ Sind TOMs (Technische und Organisatorische Maßnahmen) vorhanden und ausreichend dokumentiert?	☐	☐
■ Gibt es eine regelmäßige Überprüfung und Verbesserung der Sicherheitsmaßnahmen im Unternehmen?	☐	☐

8. Privacy by Design

	ja	nein
■ Sind Ihre IT-gestützten Prozesse und IT-Systeme durch geeignete technische und organisatorische Maßnahmen daten-schutzfreundlich gestaltet?	☐	☐

9. Privacy by Default

	ja	nein
■ Werden bei Ihren eingesetzten IT-Systemen so wenig Daten wie nötig erhoben?	☐	☐

10. Verträge mit Auftragsarbeitern

	ja	nein
■ Sind mit allen Auftragsverarbeitern (AV) Verträge vorhanden?	☐	☐
■ Gibt es bei Auftragsverarbeitern, bei denen Daten in ein Dritt-land übermittelt werden, erweiterte Vertragsvereinbarungen (EU-Standardvertragsklauseln, Binding Corporate Rules, Privacy Shield bei US-Unternehmen)?	☐	☐
■ Wurden die bestehenden Verträge mit Ihren externen Partnern, die in Ihrem Auftrag personenbezogene Daten verarbeiten (Auftragsverarbeiter), an die DSGVO angepasst?	☐	☐

11. Meldepflichten

	ja	nein
■ Gibt es einen dokumentierten Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde?	☐	☐

12. Datenschutz-Managementsystem

	ja	nein
■ Haben Sie die Einhaltung aller Pflichten und die umgesetzten Anforderungen der DSGVO schriftlich und nachweisbar dokumentiert?	☐	☐
■ Ist sichergestellt, dass die Dokumentation regelmäßig geprüft und auf den aktuellen Stand gebracht wird?	☐	☐

GESETZESTEXTE

- Amtsblatt der Europäischen Union
  Veröffentlichung der DSGVO (deutsch, PDF-Download) — **Download**
- Amtsblatt der Europäischen Union
  Veröffentlichung der DSGVO (englisch, PDF-Download) — **Download**
- Veröffentlichung des BDSG-neu
  im Bundesgesetzblatt (PDF-Download) — **Weblink**

WEBLINKS

- IT-Sicherheit in kleinen und mittleren Unternehmen (KMU)
  BSI-Studie zum Grad der Sensibilisierung des Mittelstandes in DE — **Weblink**
- IT-Grundschutz kompakt
  BSI - Leitfaden Informationssicherheit — **Weblink**
- Verarbeitung personenbezogener Daten in Drittländern
  Bitkom Leitfaden — **Weblink**
- Datenschutz-Wiki
  Der Ruhr-Universität Bochum und des BvD e.V. — **Weblink**

Hinweis: Die oben genannten weiterführenden Links wurden sorgfältig recherchiert. Für die Inhalte und Richtigkeit der bereitgestellten Informationen ist der jeweilige Anbieter der verlinkten Webseite verantwortlich. Zum Zeitpunkt der Verlinkung waren keine Rechtsverstöße erkennbar.

Impressum

Herausgeber: Bundesverband Industrie Kommunikation e.V. (bvik)
Am Mittleren Moos 48
86167 Augsburg
Tel: 0821 650 537-0
E-Mail: geschaeftsstelle@bvik.org
www.bvik.org

Autor: Thorsten Wälde, Büro für Datenschutz und Inbound Marketing, thorstenwaelde.com
Redaktion: Tanja Auernhamer, bvik
Satz: aia orange – büro für gestaltung
Stand: Februar 2018