CHECKLISTE

Der Mittelstand. BVMW
Bundesverband mittelständische Wirtschaft
Unternehmerverband Deutschlands e.V.

12 FRAGEN ZUM DATENSCHUTZ, DIE SIE SICH STELLEN SOLLTEN!
ANSONSTEN KANN ES TEUER WERDEN!

BEGRIFFE ZUM DATENSCHUTZ:

Personenbezogene Daten: Alle Daten, mit denen eine natürliche Person identifiziert werden kann. Das kann ein Name, eine Adresse, eine Sozialversicherungsnummer, eine E-Mail-Adresse oder eine IP-Adresse sein.

Datenverantwortlicher: Eine natürliche Person, eine Gemeinschaft, eine Stiftung oder eine andere Einrichtung, die das Recht hat, die Daten zu nutzen.

Datenverarbeiter: Eine natürliche Person, ein Büro oder ein Unternehmen, welche Daten im Auftrag des Datenverantwortlichen bearbeitet, wie beispielsweise ein Anbieter von E-Mail-Marketing-Software.

HINWEIS: Kennen Sie Ihre Rolle – sind Sie Datenverantwortlicher oder Datenverarbeiter? Stellen Sie sicher, dass Sie wissen, welche Rolle Ihr Unternehmen beim Umgang mit personenbezogenen Daten spielt: davon hängen auch Ihre Pflichten und Verantwortlichkeiten ab.

Folgend möchten wir Ihnen ein paar grundsätzliche Maßnahmen vorstellen, auf die Sie den Datenschutz in Ihrem Unternehmen prüfen sollten.*

1. Haben Sie Ihre Dokumente, insbesondere Ihre AGB und Ihre Datenschutzerklärung, auf Transparenz und Verständlichkeit überprüft?

Nach Erwägungsgrund 58 der EU-DSGVO sollen alle für die Öffentlichkeit oder für betroffene Personen bestimmte **Informationen präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache** abgefasst sein. Werden Kinder angesprochen, sollen die Informationen und Hinweise in einer derart klaren und einfachen Sprache verfasst sein, dass auch ein Kind sie verstehen kann.

2. Haben Sie Ihre Verträge zur Auftragsdatenverarbeitung an die EU-DSGVO angepasst?

Bisher war nach § 11 BDSG ein Vertrag zur Auftragsdatenverarbeitung erforderlich, wenn ein Dienstleister in Ihrem Auftrag personenbezogene Daten erhoben, verarbeitet oder genutzt hat. Dieser wird nun durch zwei neue Artikel (28,29) der EU-DSGVO ersetzt. **Verträge zur Auftragsdatenverarbeitung sind damit an die Vorgaben der neuen Verordnung anzupassen.**

3. Ist Ihr Internetauftritt an die EU-DSGVO angepasst?

Nach Art. 25 EU-DSGVO ist Datenschutz durch die Gestaltung technischer Abläufe (privacy by design) und durch **datenschutzfreundliche Voreinstellungen** (privacy by default) zu gewährleisten. Konkret heißt dies, dass der Schutz der Privatsphäre in allen Stufen der Produktentwicklung zu beachten ist (privacy by design), und die Voreinstellungen von Online-Diensten so zu wählen sind, dass möglichst wenig personenbezogene Daten erhoben werden (privacy by default).

Stand: Dezember 2017

Der Mittelstand. BVMW
Bundesverband mittelständische Wirtschaft
Unternehmerverband Deutschlands e.V.

4. Haben Sie Ihr Verfahrensverzeichnis an die EU-DSGVO angepasst und ein Verzeichnis Ihrer Verarbeitungstätigkeiten (VVT) erstellt?

Bisher hatten Unternehmen nach §§ 4e und 4g BDSG ein Verfahrensverzeichnis zu führen. Mit der EU-DSGVO (Art. 30) wird dieses Verfahrensverzeichnis durch ein Verzeichnis der Verarbeitungstätigkeiten (VVT) abgelöst. Das Verfahrensverzeichnis ist also hinsichtlich Inhalt und Umfang an diesen anzupassen. **Unternehmen mit weniger als 250 Mitarbeitern benötigen kein Verarbeitungsverzeichnis, sofern die Datenverarbeitung nur ein geringes Risiko für die Rechte und Freiheiten betroffener Personen birgt, keine sensiblen Daten verarbeitet werden und die Datenverarbeitung nur gelegentlich erfolgt.** In den allermeisten Fällen wird jedoch von einer regelmäßigen Datenverarbeitung auszugehen sein, sodass ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen ist.

5. Denken Sie Datenschutz bereits als Teil Ihres Betriebsführungssystems?

Nach der Datenschutz-Grundverordnung sind Unternehmen verpflichtet, bei der Verarbeitung personenbezogener Daten geeignete und wirksame Maßnahmen zu treffen, damit diese Verarbeitungen im Einklang mit der EU-DSGVO stehen. **Die Datenschutzkonformität muss durch das Unternehmen jederzeit nachgewiesen werden können.** Die beständige Überprüfung und Aktualisierung macht eine Integration des Datenschutzes in das Betriebsführungssystem erforderlich.

6. Müssen Sie in Ihrem Unternehmen einen Datenschutzbeauftragten benennen?

Ja, wenn
- umfangreiche, regelmäßige und systematische Überwachung von betroffenen Personen besteht oder
- eine umfangreiche Verarbeitung besonderer Kategorien personenbezogenen Daten (z.B. Religion, ethnische Zugehörigkeit etc.) besteht. (EU-DSGVO Art. 37)

und/oder wenn
- in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind,
- Sie Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung unterliegen, oder
- Sie geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung personenbezogene Daten verarbeiten (BDSG (neu) §38).

ACHTUNG: Die Sanktionen sind erheblich, **wenn sich ein Unternehmen nicht daran hält: 10.000.000,00 € oder 2 % des weltweiten gesamten Vorjahresumsatzes.**

Hatte der Datenschutzbeauftragte bislang nur die Aufgabe auf die Einhaltung des Datenschutzes hinzuwirken, obliegt ihm zukünftig die Aufgabe, die Einhaltung des Datenschutzes zu überwachen.

Die Kontaktdaten des Datenschutzbeauftragten müssen nach Art. 37 Abs. 7 EU-DSGVO veröffentlicht und der Aufsichtsbehörde mitgeteilt werden.

ACHTUNG: Bei Verstößen steigt nun das **Haftungsrisiko nicht nur für Unternehmen, sondern auch für Geschäftsführer, Mitarbeiter und interne Datenschutzbeauftragte.** Bei Verstößen im Umgang mit personenbezogenen Daten drohen über Geldbußen hinaus gar strafrechtliche Sanktionen wie eine Freiheitsstrafe (§42 DSAnpUG).

Stimmen Sie sich mit Ihrem Datenschutzbeauftragten und Ihren Mitarbeitern zu dem Thema unbedingt ab, um Konsequenzen dieser Art zu vermeiden.

7. Haben Sie Ihre Verpflichtung auf das Datengeheimnis an die EU-DSGVO angepasst?

Nach dem alten Bundesdatenschutzgesetz (§ 5) waren die mit der Datenverarbeitung beschäftigten Personen auf das Datengeheimnis zu verpflichten. Diese Pflicht wird sich in der neuen Verordnung (Art. 28) und dem neuen Bundesdatenschutzgesetz (§ 53) wiederfinden. Die Verpflichtungen sind dementsprechend anzupassen.

8. Wurde die Einwilligungserklärung an die EU-DSGVO angepasst?

Mit der EU-DSGVO werden deutlich erhöhte Anforderungen an die Einwilligung gestellt. So ist der Betroffene insbesondere nach Art. 7 Abs. 3 EU-DSGVO über die **freie Widerruflichkeit seiner Einwilligung vorab zu unterrichten.**

Zudem muss im Rahmen der neuen Verordnung in der Datenschutzerklärung auf dieses Widerrufsrecht hingewiesen werden. Einwilligungs- und Datenschutzerklärungen sind also insoweit anzupassen.

ACHTUNG: Eine nach bisher geltendem Recht rechtswirksame eingeholte Einwilligung gilt auch nach dem 25.05.2018 fort. Soll jedoch nach dem 25.05.2018 eine Einwilligung beim Betroffenen eingeholt werden, muss die Einwilligungserklärung den oben dargestellten Grundsätzen entsprechen.

9. Haben Sie einen Prozess zur Datenschutz-Folgeabschätzung (DSFA) definiert inkl. eines Musters für die dazugehörige Risikobewertung?

Soll ein neues Verfahren der Datenverarbeitung eingesetzt werden, das mit einem hohen Risiko für die Betroffenen verbunden ist, ist **künftig eine Folgenabschätzung vorzunehmen** (Art. 35 EU-DSGVO). Diese ist mit dem Datenschutzbeauftragten abzustimmen und ersetzt die bisherige Vorabkontrolle. Stellt sich ein hohes Risiko für die Betroffenen heraus und werden keine Maßnahmen zur Risikoeindämmung getroffen, **ist die zuständige Aufsichtsbehörde zu informieren.**

HINWEIS: Art. 35 Abs. 7 EU-DSGVO regelt den typischen Ablauf einer DSFA. Im Unternehmen sollte also ein entsprechendes Muster für einen Meldeprozess im Sinne der DSFA vorliegen, um die Risikobewertung durchzuführen, ebenso wie ein Meldebogen für die Behörde.

10. Kennen Sie den vorgeschriebenen Ablauf bei einer Datenpanne?

Sie sind als Unternehmer verpflichtet, **eine Datenpanne innerhalb von 72 Stunden der Aufsichtsbehörde zu melden.** Diese Meldung muss nach Art. 33 Abs. 3 EU-DSGVO bestimmte Informationen zur Art und den wahrscheinlichen Folgen der Verletzung beinhalten. Zudem sind Sie **verpflichtet betroffene Personen über Datenpannen zu informieren.**

11. Können Sie das „Recht auf Vergessenwerden“ gewährleisten?

Personenbezogene Daten müssen unverzüglich gelöscht werden können (Art. 17 EU-DSGVO). Das heißt, Sie müssen einen Prozess entwickeln, um dieses „Recht auf Vergessenwerden“ zu gewährleisten.

Tipp: Legen Sie Prozesse und Zuständigkeiten direkt im Unternehmen fest, um den entsprechenden Rechten und Wünschen von Betroffenen gerecht werden zu können.

12. Haben Sie Ihre Betriebsvereinbarung an die Vorgaben der EU-DSGVO angepasst?

In der neuen Verordnung (Art. 88) wird auch die Datenverarbeitung im Beschäftigungskontext geregelt. Damit betrifft **diese Regelung insbesondere Betriebsvereinbarungen.** Dabei wird klargestellt, dass Betriebsvereinbarungen zwar über das Datenschutzniveau der EU-DSGVO hinausgehen können, dieses aber nicht unterschreiten dürfen.

Des Weiteren ist die Transparenz der Verarbeitung zu berücksichtigen. So muss in den Betriebsvereinbarungen nun ausdrücklich auf die Rechte der betroffenen Arbeitnehmer eingegangen werden.

ACHTUNG: Diese Punkte machen eine **Anpassung aktueller Betriebsvereinbarungen erforderlich.**

Der BVMW stellt Ihnen auf schriftliche Anfrage unter politik@bvmw.de sowie im BVMW-Mitgliederbereich Muster für Vorlagen, Verträge und Meldebögen im Sinne der EU-DSGVO zur Verfügung.

Die Checkliste und die dazugehörigen Muster wurden mithilfe der BVMW-Unternehmerkommissionen Internet und Digitales, Unternehmenssicherheit sowie Recht nach bestem Wissen und mit größter Sorgfalt zusammengestellt.

***Diese Ausarbeitung ist nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen der BVMW bzw. die Autoren nicht. Die in den vorliegenden Dokumenten gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen von der verantwortlichen Stelle für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.**

Kontakt:
Bundesverband mittelständische Wirtschaft (BVMW) e. V.
Bereich Volkswirtschaft & Politik
Potsdamer Straße 7, 10785 Berlin
Tel.: +49 (0)30 533206-47, Fax: +49 (0)30 533206-50
politik@bvmw.de, www.bvmw.de