DSGVO: Das müssen Kleinunternehmer jetzt tun!

Wenn die EU-Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018 ihre volle Wirkung entfaltet, wird es keine Übergangsfrist geben. Datenschutzrecht gilt zwar „nur“ für personenbezogene Daten, da dieser Begriff jedoch sehr weit ausgelegt wird, sollten Sie im Zweifel davon ausgehen, dass Daten Personenbezug aufweisen. Alle datenschutzrechtlichen Vorgaben müssen also spätestens zum 25. Mai umgesetzt sein – das gilt auch für Kleinunternehmer. Denn die DSGVO gilt grundsätzlich für alle Unternehmen jeder Branche, Größe, Gesellschaftsform, Umsatz- oder Beschäftigtenzahlen.

Es gibt zwar die eine oder andere Erleichterung für Kleinstunternehmen und Einzelunternehmer, aber trotzdem gibt es einiges zu tun. Wenn Sie die bislang gemäß Bundesdatenschutzgesetz (BDSG) vorgesehenen Regelungen schon umgesetzt haben, über ein Qualitätsmanagement verfügen oder gar ISO-zertifiziert sind, dann haben Sie schon eine recht gute Basis, die Sie jetzt „nur“ noch um die speziellen Vorgaben der DSGVO ergänzen müssen. Allerdings zeigt die Erfahrung, dass viele Unternehmen – gerade auch viele Kleinunternehmer – sich bislang zwar an Datenschutzregeln gehalten haben, dies aber wenig bis gar nicht dokumentiert ist.

Leider ist es so, dass es nach Maßgabe der DSGVO nicht mehr ausreicht, Datenschutz im Unternehmen umzusetzen, im Zweifel muss hierüber auch ein tauglicher Nachweis erbracht werden können. Und dies geschieht idealerweise mit Hilfe einer entsprechenden Dokumentation, sozusagen einem ausführlichen und aktuellen „Datenschutzhandbuch“.

Auch wenn die Zeit knapp ist und Sie vielleicht nicht mehr bis zum 25. Mai alle erforderlichen Unterlagen zusammenstellen können – es ist auf jeden Fall besser, mit dem Projekt DSGVO erst halb fertig zu sein, als zugeben zu müssen, dass man noch nicht einmal damit begonnen hat. Deshalb zeigen wir Ihnen, welche Schritte Sie als Kleinunternehmer auf jeden Fall so bald wie möglich angehen sollten.

1. Zeit und Geld einplanen, Verantwortung verteilen

Die Erstellung der erforderlichen Unterlagen für die DSGVO erfordert zunächst einmal die Analyse der Geschäftsabläufe / Prozesse im eigenen Kleinunternehmen – und das wiederum erfordert ein gewisses Budget an Zeit und Geld. Als Einzelunternehmer müssen Sie sich selbst um alles kümmern. Wenn Sie Beschäftigte haben, dann können Sie zumindest manche Aufgaben auf sie delegieren.

Oftmals ist es aber notwendig, externen Fachverstand mit ins Boot zu holen, was zwar weniger Zeit, dafür aber Geld kostet. Wichtig ist, dass irgendjemand „den Hut aufhat“ und die Umstellung bzw. Vorbereitung auf die DSGVO federführend übernimmt.

2. Analyse des eigenen Kleinunternehmens

Was mache ich eigentlich im beruflichen Alltag? Wie gehe ich vor, wenn mich ein Kundenauftrag erreicht? Welche Schritte führe ich aus, um eine Rechnung zu erstellen? Diese Fragen und noch mehr sollten Sie sich als Kleinunternehmer stellen, wenn Sie Ihre Geschäftsabläufe (auch „Prozesse“ oder „Verfahren“ genannt) in Hinblick auf die DSGVO genauer unter die Lupe nehmen.

Typische Prozesse in Unternehmen sind etwa das Führen von Personalakten, die Buchhaltung, das Durchführen von Bewerbungsverfahren, der Versand von Werbung, das Nutzen von Cloud-Dienstleistungen oder auch die Vernichtung von Papierunterlagen. Die in Ihrem Kleinunternehmen bestehenden Prozesse sollten Sie zumindest stichpunktartig beschreiben, Sie können sie auch in einem Ablaufdiagramm skizzieren. Zusätzlich müssen Sie alle technischen und organisatorischen Maßnahmen (TOM) niederschreiben, die Sie treffen, um die durch Sie verarbeiteten personenbezogenen Daten zu schützen.

Es geht hier also primär um Fragen der IT-Sicherheit, aber nicht nur. Auch eine Arbeitsanweisung an die Mitarbeiter, dass alle Schreibtische vor dem Verlassen des Büros aufzuräumen sind, damit keine Unterlagen mit sensiblen Daten mehr offen herumliegen, kann beispielsweise eine organisatorische Maßnahme zur Verbesserung des Datenschutzes sein. Zu TOM zählen alle möglichen Dinge, u.a. eine Zutrittskontrolle zum Gebäude bzw. Büro, die Sicherung des Servers, die Pflicht zum Anmelden am Computer mittels Kennung und Passwort, der Einsatz von Antiviren-Software und Firewall usw.

Die Beschreibung der einzelnen Prozesse und die TOMs ergeben zusammen das sogenannte Verarbeitungsverzeichnis, das Sie gemäß DSGVO führen müssen. Eine kostenfreie Vorlage nebst erläuternden Hinweisen können Sie sich hier herunterladen:
www.lexware.de/dsgvo/mustervorlagen

In der DSGVO gibt es zwar Ausnahmen für Kleinunternehmen mit weniger als 250 Mitarbeitern. Zu diesem Grundsatz existieren aber auch Einschränkungen, die letztlich dazu führen, dass lediglich nur

›››

diejenigen Kleinunternehmer von der Pflicht zur Führung des Verarbeitungsverzeichnisses befreit sind, die bei ihrer Arbeit keinen Computer verwenden und auch keine Kunden- oder Lieferantenkartei in Papierform führen. Unter dem Strich besteht die Pflicht also dann doch für so ziemlich jedes Unternehmen.

Weiterhin ist es sinnvoll, dass Sie eine Liste anfertigen, in der Sie alle Dienstleister aufführen, deren Dienste Sie in Anspruch nehmen. Hier kommen u.a. Cloud-Anbieter, E-Mail- bzw. Web-Hoster, Drucker-/Kopierer-Wartung, externe Lohnbuchhaltung, Entsorgungsunternehmen o.ä. in Frage. Aus dieser Liste ergibt sich, welcher dieser Dienstleister die personenbezogenen Daten aus Ihrem Unternehmen in Ihrem Auftrag sozusagen als „ausführendes Organ" für Sie verarbeitet. In diesen Fällen müssen Sie dann gemäß DSGVO mit dem betreffenden Dienstleister – zusätzlich zum eigentlichen Dienstleistungsvertrag – einen sog. Auftragsverarbeitungsvertrag abschließen, der speziell den Umgang mit den betreffenden Daten regelt.

Da es diese Pflicht auch schon nach der bisherigen Regelung im BDSG gab, bestehen derartige Verträge unter Umständen schon, müssen aber an die DSGVO angepasst werden. Hier können Sie sich von einem Rechtsanwalt einen Mustervertrag anfertigen lassen und diesen dann für all Ihre Dienstleister verwenden; insbesondere die größeren Dienstleistungsunternehmen haben aber auch ihre eigenen Verträge, die von Ihnen als Kunde dann nur noch unterzeichnet werden müssen.

3. DSGVO-Maßnahmen mit Außenwirkung

Es gibt zwei Dinge, die Sie als Kleinunternehmer auf jeden Fall bis zum 25. Mai erledigt haben sollten, denn diese besitzen eine Außenwirkung. Daran lässt sich dann sehr leicht erkennen, ob Sie die Vorgaben der DSGVO beachten oder nicht. Hierbei handelt es sich zum einen um die Bestellung eines Datenschutzbeauftragten und zum anderen um die Erfüllung Ihrer Informationspflichten.

Gemäß DSGVO müssen Sie als Kleinunternehmer nur dann einen Datenschutzbeauftragten bestellen, wenn zu Ihren Kerntätigkeiten die regelmäßige und systematische Überwachung von Personen oder die umfangreiche Verarbeitung besonders sensibler Daten (z.B. Gesundheitsdaten) zählt. Wenn Sie Angestellte haben, dann verarbeiten Sie zwar auch sensible Daten, nämlich beispielsweise die Religionszugehörigkeit und ggf. auch Gesundheitsdaten, dies zählt dann allerdings nicht zu Ihrer Kerntätigkeit. In diesem Sinne wären nur z.B. Detektive, Auskunfteien, Krankenhäuser oder Online-Werbenetzwerke betroffen.

Allerdings müssen auch die ergänzenden Regelungen des neuen BDSG herangezogen werden, der die Hürde noch etwas höher legt als die DSGVO. Der deutsche Gesetzgeber verlangt in Ergänzung der DSGVO dann einen Datenschutzbeauftragten, wenn sich in Ihrem Kleinunternehmen insgesamt 10 oder mehr Beschäftigte ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen oder Sie personenbezogene Daten geschäftsmäßig übermitteln (wie z.B. Adresshändler oder Marktforschungsinstitute). Sie können also als Kleinunternehmer nur dann auf einen Datenschutzbeauftragten verzichten, wenn sich weniger als 10 Beschäftigte in Ihrem Unternehmen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen und Ihr Hauptgeschäftszweck nicht in der Verarbeitung sensibler Daten bzw. in der geschäftsmäßigen Übermittlung von Daten mit Personenbezug besteht.

Kommen Sie zum Ergebnis, dass Sie einen Datenschutzbeauftragten benötigen, können Sie entweder einen Ihrer Mitarbeiter dazu ernennen (sofern er dem zustimmt) oder Sie können diese Aufgabe einem externen Fachmann übertragen. Wofür Sie sich auch entscheiden, Ihr Datenschutzbeauftragter muss in jedem Fall spätestens zum 25. Mai der für Sie zuständigen Datenschutzaufsichtsbehörde gemeldet werden. Melden Sie nicht, obwohl Sie eigentlich müssten, so ist das schon ein Datenschutzverstoß, der mit empfindlichen Bußgeldern geahndet werden kann.

Wenn Sie einen Webshop oder eine sonstige geschäftliche Internetseite betreiben, müssen Sie dort eine Datenschutzerklärung bereitstellen. Das ist keine neue Pflicht, aber die Inhalte müssen an die DSGVO angepasst werden. Außerdem sind Sie auch als Kleinunternehmer verpflichtet, bei jedem Erstkontakt mit Kunden, neuen Mitarbeitern, Vertragspartnern etc. diesen Ihre allgemeinen Datenschutzhinweise zur Verfügung zu stellen. Dies kann z.B. als PDF-Anhang per E-Mail erfolgen, durch Übergabe bei einem persönlichen Treffen oder auch mit kurzem Hinweis bei Telefonaten bzw. durch entsprechende Änderung Ihres Anrufbeantworter-Textes.

Wie genau diese Informationspflichten „offline" nun genau erfüllt werden müssen, ist leider noch nicht abschließend geklärt – fest steht jedoch, dass die Pflicht zur Information über die Verarbeitung von personenbezogenen Daten über die Online-Datenschutzerklärung hinausgeht.

4. Interne Abläufe

Im Hinblick auf die Rechte von betroffenen Personen, deren Daten Sie verarbeiten, ist es wichtig, dass Sie Abläufe festlegen, wie z.B. im Falle einer Auskunftsanfrage verfahren werden soll. Sie müssen gemäß DSGVO auch als Kleinunternehmer auf eine entsprechende Anfrage zeitnah reagieren und der betreffenden Person mitteilen, ob Sie personenbezogene Daten von ihr verarbeiten, und wenn ja, welche das sind. Hierzu sollten Sie ein Muster-Antwortschreiben entwerfen, das dann noch um die individuellen Daten der anfragenden Person ergänzt und an diese verschickt wird.

Ebenso sollten Sie auf etwaige Datenpannen vorbereitet sein. Verlieren Sie beispielsweise einen USB-Stick mit wichtigen Mitarbeiterdaten oder wird die Kundendatenbank auf Ihrem Server gehackt, müssen Sie im Regelfall die zuständige Aufsichtsbehörde und – bei einem voraussichtlich hohen Risiko – auch die von der Datenpanne betroffenen Personen darüber in Kenntnis setzen. Auch dieser Ablauf muss dokumentiert und schon mit entsprechenden Musterschreiben vorbereitet werden.

Insgesamt müssen Sie Ihre Beschäftigten in Bezug auf den Umgang mit personenbezogenen Daten sensibilisieren. Diese müssen also zumindest Informationen über die grundlegenden Dinge im Datenschutz erhalten. Ob Sie dies per Arbeitsanweisung, ausführlicher Literatur oder dem „Zwangsbesuch" einer Fortbildungsveranstaltung umsetzen, bleibt Ihnen überlassen. Irgendeine Maßnahme sollten Sie jedoch ergreifen.

Autor: Michael Rohrlich, Rechtsanwalt und zertifizierter Datenschutzbeauftragter (DSB-TÜV)

Mehr Informationen zur DSGVO finden Sie online unter:
www.lexware.de/dsgvo