Axel Voss
Mitglied des Europäischen Parlaments

Die neue Datenschutz-Grundverordnung:
Auf was müssen Mittelständler jetzt achten?

Mit dieser Aufstellung möchte ich Ihnen einen allgemeinen Überblick über die neuen Pflichten von kleinen und mittleren Unternehmen bei der Verarbeitung von persönlichen Daten geben. Da Unternehmen sehr unterschiedlich strukturiert sind, sind alle Angaben ohne Gewähr, erheben keinen Anspruch auf Vollständigkeit und ersetzen keine juristische Einzelfall-Beratung.
Leider führt die Anwendung der Datenschutzgrundverordnung (DSGVO) zurzeit zu großen Verunsicherungen, insbesondere bei kleinen und mittelständischen Unternehmen. Dies wird noch dadurch bestärkt, dass der ein oder andere nationale Datenschützer versucht, Standards im Markt unterzubringen, die europarechtlich keine Grundlage haben. Sie interpretieren das europäische Recht dabei bewusst in einer Weise, dass der Datenschutz zur Innovationsbremse wird. Wir als CDU/CSU-Gruppe im Europäischen Parlament hätten uns eine zukunftsorientiertere Balance zwischen dem Schutz der Rechte des Einzelnen und praktikablen Regeln für die europäische Wirtschaft gewünscht. Mit gezielteren Regelungen und mehr Ausnahmen für die alltägliche Datenverarbeitung durch Bürger, Vereine und kleine Unternehmen hätte dies verhindert werden können, was die anderen Fraktionen im Europäischen Parlament aber nicht zugelassen haben.

ALLGEMEINES

Mit der DSGVO werden die Regeln zur Verarbeitung personenbezogener Daten innerhalb der Europäischen Union vereinheitlicht. Da es sich um eine europäische Verordnung handelt, gelten die neuen Regeln direkt in allen Mitgliedstaaten. Der nationale Gesetzgeber kann darüber hinaus in bestimmten Bereichen (bei den sog. Öffnungsklausel) eigene konkretisierende Vorschriften erlassen. Das bisher in Deutschland geltende Bundesdatenschutzgesetz (BDSG) wurde daher entsprechend angepasst und wird in Teilen fortbestehen. Die DSGVO wird ab dem **25. Mai 2018** angewendet.

GILT DIE DSGVO AUCH FÜR UNTERNEHMEN?

Ja, sobald das Unternehmen / der Betrieb personenbezogene Daten (meist Name, Anschrift, Telefon, E-Mail) ganz oder teilweise automatisiert (z.B. über PC, Smartphone, Kamera, Kopierer) in einer strukturierten Ablage wie beispielsweise in einem Kundenverzeichnis verarbeitet. Ausgenommen sind lediglich der rein private Schriftverkehr einer natürlichen Person, ein privates Anschriftenverzeichnis oder die private Nutzung von sozialen Netzwerken.

WELCHE PERSONENBEZOGENEN DATEN SIND GEMEINT?

Personenbezogene Daten sind all jene Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Darunter fallen u.a. der Name, der Aufenthaltsort, eine Mail-Adresse, eine Kundennummer. Für die Verarbeitung von besonders sensiblen persönlichen Daten wie Gesundheitsdaten, Daten zur

ethnischen Herkunft, politischen Meinungen dürfen nur unter bestimmten Anforderungen nach Art. 9 Abs. 2 verarbeitet werden.
Wenn also ein Unternehmen eine Liste über die Gewerkschaftszugehörigkeit aller Mitarbeiter führt, braucht es dazu die ausdrückliche Einwilligung der Betroffenen.

RECHTMÄßIGE VERARBEITUNG UND EINWILLIGUNG
Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Kunden kommt für Unternehmen insbesondere Art. 6 Abs. 1 b („Vertragserfüllung“) in Betracht, d.h. die Datenverarbeitung findet im Rahmen einer vertraglichen Beziehung (=Geschäftsbeziehung) statt, manchmal auch nach Art. 6 Abs. 1 f („berechtigtes Interesse des Unternehmens“). Die Daten von Kunden (u.a. Name, Anschrift, Geburtsdatum, Bankverbindung) können ohne Einwilligung aber nur für Vertragszwecke sowie zur Kundenbetreuung/-verwaltung verarbeitet werden. Wofür diese verarbeitet werden, ergibt sich aus dem Vertrag, der die Ziele bestimmt, für welche wiederum die Kundendaten genutzt werden können. Man darf dabei aber nur die Daten verarbeiten, die für eine Kundenbeziehung unbedingt nötig sind. Es gilt der Grundsatz der Datenminimierung. Vor dem 25. Mai 2018 eingeholte Einwilligungserklärungen sind auch nach diesem Stichtag gültig.
Unternehmen, die einen Newsletter an minderjährige Kunden senden wollen, müssen ggf. kleine Anpassungen vornehmen, da Jugendliche nach Art. 8 Abs. 1 nun erst mit 16 Jahren in die Verarbeitung ihrer Daten einwilligen können. Wollen Kinder ihre Mailadressen zur Anmeldung für Newsletter verwenden, müssen also die Eltern dem zustimmen.
Zudem müssen die Datenschutzerklärungen in einfacher und verständlicher Sprache auf der Homepage des Unternehmens aktualisiert werden.
1) Enthalten sein muss nun ein Hinweis, welche personenbezogenen Daten erhoben werden,
2) wie lange sie gespeichert werden,
3) wie ein Eintrag auf Datenlöschung gestellt werden kann und
4) welche Daten an Dritte oder an Staaten außerhalb der EU weitergegeben werden.

Wenn Unternehmen mit anderen Dienstleistern, Partnerunternehmen etc. zusammenarbeiten und deshalb Daten transferieren, dann ergeben sich daraus, weitere Informations- und Dokumentationspflichten. Dies trifft aber für kleine Handwerksunternehmen in der Regel nicht zu.
Falls es eine solche Kooperation mit solchen Partnern gibt, die ausserhalb der EU ihren Sitz haben, gibt es hier zusätzlichen Anforderungen, die auf einen gleichartigen Datenschutz im Ausland zielen.

Kleine Handwerksbetriebe, die die Daten ihrer Kunden nur für eigene Geschäftszwecke nutzen (Rechnung, Mahnung, Geburtstagsschreiben, Werbung etc.) und nicht an jemand anderen weitergeben, benötigen keine Datenschutzfolgeabschätzung, keinen Datenschutzbeauftragten, kein Verzeichnis von Verarbeitungstätigkeiten.

DOKUMENTATION UND DATENSCHUTZBEAUFTRAGTER

Das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 gilt nicht für kleine und mittelständische Unternehmen, die **weniger als 250 Mitarbeiter** beschäftigen.
Ein Unternehmen muss nur dann einen Datenschutzbeauftragten benennen, wenn **mindestens 10 Personen** im Unternehmen mit der **regelmäßigen und systematischen Verarbeitung** von personenbezogenen Daten beschäftigt sind.
Der betriebliche Datenschutzbeauftrage war bereits vor der DSGVO in Deutschland geregelt.

ZWECK DER DATENERHEBUNG

Schließt ein Kunde mit einem Unternehmen einen Vertrag ab, können die hierfür erhobenen Daten auch weiterverwendet werden. Die Weiterverwendung muss allerdings mit dem ursprünglichen Zweck vereinbar sein, es müssen Garantien gegen Missbrauch vorliegen und der Betroffene muss informiert werden. Bei Belangen, welche keine Zweckbindung aufweisen, ist eine Einwilligung des Kunden notwendig. Nach dem Bundesdatenschutzgesetz ist eine Übermittlung und Nutzungen für andere Zwecke zulässig, wenn dies zur Wahrung eines berechtigen Interesses (Art. 6 Abs.1 f DSGVO) erforderlich ist.
Erlaubt ist also die Nutzung der Daten zur Kundenbindung durch die Sendung von Geburtstagsgrüßen oder der Direktwerbung per Post.

AUSKUNFTS- UND INFORMATIONSPFLICHTEN

Die DSGVO erweitert und ergänzt die datenschutzrechtlichen Ansprüche der Kunden. Die Informationspflichten werden gemäß Art. 12-15 erheblich ausgebaut, sodass der Kunde nun eine unentgeltliche Kopie der verarbeiteten Daten verlangen kann und über seine Auskunfts- und Interventionsrechte informiert werden muss.

Aus Art. 13 Abs. 1 und Abs. 2 folgt, dass das Unternehmen in jedem Formular zur Erhebung personenbezogener Daten auf Folgendes hinweisen muss:

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten, wenn das Unternehmen einen haben muss
- die Zwecke der Verarbeitung, am besten im Einzelnen aufzählen
- die Rechtsgrundlage der Verarbeitung
- Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an andere Unternehmen, an alle Mitarbeiter, im Internet)
- die Absicht über Drittlandtransfers (z.B. bei Mitarbeiterverwaltung in der Cloud), sowie Hinweis auf Garantien zur Datensicherheit
- die Speicherdauer der personenbezogenen Daten
- die Belehrung über die Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- den Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- den Hinweis auf das Beschwerderecht bei einer Aufsichtsbehörde

Das Unternehmen hat auch die Pflicht, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich entweder in der Unternehmenssatzung oder auch in einer vom Vorstand beschlossenen Datenschutzerklärung festzulegen.

Kurze Checkliste für kleine Betriebe

1) Machen Sie sich Gedanken darüber, welche Daten Sie erheben, zu welchem Zweck Sie sie gebrauchen wollen oder müssen und ob Sie Dritte miteinbeziehen.
2) Homepage: a) Aktualisieren Sie den Disclaimer und/oder die Datenschutzerklärung mit den geforderten Informationen; b) Wenn Sie Daten über die Homepage beziehen, dann muss auf dieser Seite auch der Hinweis auf die Datenschutzerklärung installiert werden, mit der Möglichkeit der Erklärung des Kunden, die Datenschutzerklärung gelesen zu haben und sich damit einverstanden zu erklären.
3) Machen Sie sich Gedanken darüber, wie Sie dieses dokumentieren wollen.
4) Entwickeln Sie eine Einverständniserklärung (wie auf der Homepage) in Papierform, auf dem der Kunde unterzeichnen kann, dass er Kenntnis von der Datenschutzerklärung erhalten hat und sich damit einverstanden erklärt.
5) Regeln Sie innerhalb des Betriebes den Zugang zu den Kundendaten über den Computer.
6) Sichern Sie Ihren Computer so, dass nicht jeder darauf Zugriff hat und halten Sie die Software und Sicherheitssoftware auf dem aktuellen Stand.
7) Nur für den Fall, dass Sie externe Dienstleister zur Verarbeitung von Daten in Anspruch nehmen: Treffen Sie mit diesen eine Vereinbarung nach Art. 28 Abs. 3 der DSGVO.
8) Halten Sie die o.a. Datenschutzerklärung auch in Papierform bereit, falls Sie persönlich die Kundendaten erheben.
9) Machen Sie sich Gedanken darüber, wie Sie vorgehen, wenn der Kunde vom seinem Auskunftsrecht, Löschrecht etc. Gebrauch macht und wie Sie Vorgehen, wenn es zu einer Datenschutzverletzung kommt oder die Daten auf Anfrage des Kunden in einem maschinenlesbaren Format übertragen werden können. In einem kleineren Handwerksbetrieb bedarf es hierzu i.d.R. keinerlei großen Aufwand.

Auch wenn man beim ersten Lesen der neuen Pflichten den Eindruck bekommen hat, dass die neuen Aufgaben sehr umfassend sind, so wird sich in der Praxis sicher so manches bald ergeben. In der Regel ist es für jeden einzelnen von uns wichtig, dass seine personengezogenen Daten bestmöglich geschützt werden und in der Regel handelt es sich hierbei um einen einmaligen Aufwand.

Ihr

Axel Voss MdEP

Europabüro Bonn
Prinz-Albert-Str. 73
53113 Bonn
Tel. 0228 95596200
info@axel-voss-europa.de
www.axel-voss-europa.de