Datenschutzgrundverordnung: Handlungsempfehlungen für KMU

Die Datenschutzgrundverordnung (DSGVO), die ab dem 25. Mai 2018 ihre Wirkung entfaltet, stellt für alle Anwender eine besondere Herausforderung dar.

Unternehmen sowie Behörden sehen sich neuen und nicht unerheblichen Anforderungen ausgesetzt. Um den Umgang mit diesen Anforderungen zu erleichtern, finden Sie im Folgenden Handlungsempfehlungen insbesondere für kleinere und mittelständische Unternehmen.

Zu dem Zeitalter der Digitalisierung gehört der Schutz personenbezogener Daten als wesentliche Komponente dazu. Durch die Harmonisierung des Datenschutzrechtes bestehen gleiche Wettbewerbsbedingungen für alle Unternehmen in der Europäischen Union. Die Unterschiede beim Datenschutzniveau in den Mitgliedstaaten sowie Barrieren für den freien Datenverkehr im Binnenmarkt werden beseitigt.

Handlungsempfehlungen für den Umgang mit der DSGVO:

1. Sollen personenbezogene Daten genutzt werden, muss hierfür eine „Berechtigung“ vorliegen. Dies kann beispielsweise aufgrund einer gesetzlichen Ermächtigung der Fall sein. Fehlt eine solche gesetzliche Grundlage, bedarf es der **Einwilligung** der betroffenen Person. Auch die Erfüllung eines Vertrages oder das anderweitige berechtigte Interesse der Person an der Verarbeitung kann eine „Berechtigung“ begründen.

   Beispiel: Bei der Entgegennahme von Visitenkarten sollte künftig darauf geachtet werden, zu welchem konkreten Zweck die Visitenkarte überreicht wird. Es kann nicht immer unterstellt werden, dass die Aushändigung der Visitenkarte konkludent als Einwilligung in die Aufnahme in einen Adressverteiler zu werten ist, ggf. mit der Folge, dass die betroffene Person ungefragt informatorische Emails (z.B. Newsletter), Einladungen zu Veranstaltungen u.Ä. erhält. Hierfür bedarf es der Einwilligung der Person.

2. Sofern personenbezogene Daten in Ihrem Unternehmen erhoben werden, obliegen Ihnen **Informationspflichten** gegenüber Ihren Kundinnen und Kunden. Erheben Sie Daten, die Rückschlüsse auf eine bestimmte Person zulassen, so sind Sie verpflichtet, dieser betroffenen Person - zum Zeitpunkt der Erhebung - bestimmte Informationen zukommen zu lassen (wie bspw. die Kontaktdaten des Datenschutzbeauftragten; die Zwecke, für die Sie die personenbezogenen Daten verarbeiten; sowie die Rechtsgrundlage für die Verarbeitung).

3. Kundinnen und Kunden haben ein **Recht auf Datenübertragbarkeit**.

Beispiel: Eine Kundin / Ein Kunde möchte zu einem anderen Anbieter wechseln oder den Vertrag kündigen und bittet Sie ihr / ihm bzw. dem neuen Anbieter die personenbezogenen Daten zu übermitteln, die Sie über die Person vorhalten. Das bedeutet, Sie müssen ein System vorhalten, welches die Übermittlung der Daten ermöglicht.

4. Um ein angemessenes Schutzniveau der Daten zu gewährleisten, sind alle Unternehmen verpflichtet, geeignete aber auch angemessene **technische und organisatorische Maßnahmen** zu treffen. Diese Maßnahmen können u.a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten, die Vertraulichkeit und Integrität der Systeme und Dienste sowie ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit, einschließen.

5. Vor Verwendung neuer Technologien, z.B. der Einführung neuer Programme, die personenbezogene Daten verarbeiten, kann es erforderlich sein, eine **Datenschutz-Folgenabschätzung** durchzuführen. Dabei soll festgestellt werden, welche Risiken das Programm für personenbezogene Daten birgt.

6. Ihr Unternehmen ist verpflichtet, ein **Verzeichnis über Verarbeitungstätigkeiten** zu führen. Hierin werden alle Prozesse erfasst, die im Unternehmen zur Verarbeitung personenbezogener Daten Anwendung finden. Die LDI stellt hierfür ein Muster zur Verfügung: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten/Inhalt/Verarbeitungstaetigkeiten/Muster-Verarbeitungsverzeichnis-Verantwortlicher.pdf

   Ausgenommen von dieser Verpflichtung sind Unternehmen mit weniger als 250 Mitarbeitern, wenn die Datenverarbeitung kein Risiko für Rechte und Freiheiten der betroffenen Personen birgt, wenn die Verarbeitung nicht nur gelegentlich erfolgt oder wenn eine Datenverarbeitung der Kategorien gemäß der Artikel 9 und 10 erfolgt (vgl. Art. 30 Abs.5 DSGVO).

7. Die DSGVO sieht Grundsätze für die Verarbeitung personenbezogener Daten vor. Sie sollten die Einhaltung dieser Grundsätze dokumentieren, da Sie die Einhaltung nachweisen können müssen (sog. „**Rechenschaftspflicht**“).

8. Auch die DSGVO sieht – wie zuvor das Bundesdatenschutzgesetz (BDSG) – die Verpflichtung zur **Benennung eines Datenschutzbeauftragten** vor. Diese Verpflichtung besteht nach BDSG, soweit mindestens zehn Mitarbeiter personenbezogene Daten verarbeiten.

9. Sollte es trotz aller Vorkehrungen zu einem **Datenschutzverstoß** kommen, muss Ihr Unternehmen diesen der Aufsichtsbehörde, also der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI), unverzüglich **melden**.

10. Alle Beschäftigten im Unternehmen sollten auf die Geltung der neuen Datenschutzregelungen hingewiesen werden.

Weitergehende Informationen erhalten Sie über folgende Links zur LDI:

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Checkliste-fuer-KMU-zur-DS-GVO_LDI-NRW.pdf

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Kurzpapiere-der-Datenschutzkonferenz-zur-DS-GVO.html

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/KP_8_Massnahmenplan.pdf

Einen guten Überblick erhalten Sie auf der Webseite des Deutschen Industrie- und Handelskammertages (DIHK) und des Westdeutschen Handwerkskammertages (WHKT):

https://www.dihk.de/themenfelder/recht-steuern/oeffentliches-wirtschaftsrecht/datenschutzrecht/eu-datenschutz-gvo

Bei konkreten Einzelfragen können Ihnen die Industrie- und Handelskammern (IHK) vor Ort weiterhelfen. Die jeweils zuständige IHK finden Sie über www.ihk.de/ihk-finder.

https://www.whkt.de/fachliches/datenschutzgrundverordnung/