



23.05.2018

DATENSCHUTZ: DAS IST JETZT WICHTIG!

Die Datenschutzgrundverordnung steht unmittelbar vor bevor. „Was sich zunächst unspektakulär anhört, hat es aber tatsächlich in sich“, ist Wolf-Henning Hammer, Rechtsanwalt bei der Kanzlei Voigt, überzeugt und betont, dass dies auch direktauswirkungen auf K&L-Betriebe habe. Zu den neu geregelten Bereichen der Datenschutzgrundverordnung (DSGVO) zählen unter anderem der Arbeitnehmerdatenschutz, die Videoüberwachung im öffentlichen Raum oder die individuelle Einstufung eines Kunden in ein Kundenranking.

Worauf Sie achten sollten, wenn es bei Ihnen zu einer Datenschutz-Panne gekommen ist, [können Sie hier nachlesen, inklusive detailliertem Maßnahmenplan zum Download](#).

Die Kanzlei Voigt hat zum Thema verschiedene hilfreiche Dokumente erstellt, die Sie hier herunterladen können.

- [Schnell-Check-Liste](#)
- [umfassender Überblick und Erklärung der wesentlichen Fachbegriffe](#)

BUSSGELDER VON BIS ZU 20 MILLIONEN EURO!

Besonders pikant: Die Neuregelung ist mit einer erheblichen Anhebung der Bußgelder verbunden. „Wo heute noch vergleichsweise moderate 300.000 Euro drohen, können die Bußgelder künftig bis zu 20 Millionen Euro oder bis zu vier Prozent des weltweiten jährlichen Umsatzes des Unternehmens betragen“, erklärt Rechtsexperte Wolf-Henning Hammer. Schon allein deshalb sollte die betriebliche Praxis – wo bislang noch nicht geschehen – schnellstmöglich an die Anforderungen der DSGVO angepasst werden.

WO LIEGEN POTENZIELLE RISIKEN FÜR WERKSTÄTTEN?

Im Betriebsalltag vieler Werkstätten erkennt Wolf-Henning Hammer einige Risikopotenziale, zum Beispiel:

- Bildschirme am Empfangstresen, auf denen Kundendaten angezeigt werden
- Arbeitsplätze der Servicemeister mit offen liegenden Kundenakten
- fehlende Zutritts- und Zugangskontrollen
- ungesicherte Serverschränke in für betriebsfremde Personen zugänglichen Bereichen

Ebenfalls wichtig zu wissen: Die DSGVO bezieht sich auch auf betriebsinterne Daten zu Arbeitsverhältnissen. Es sei daher ebenfalls sicherzustellen, dass die Datenverarbeitung und - weiterleitung auch die Arbeitnehmerinteressen ausreichend berücksichtige. **Weitere Informationen dazu, welche Daten betroffen sind, wann die Verarbeitung erlaubt ist und welche Rechte Betroffene haben, können Sie hier nachlesen.**

WELCHE ORGANISATORISCHEN MASSNAHMEN SOLLTE DER BETRIEB TREFFEN?

Zur Umsetzung der neuen Anforderungen sollte der Betrieb die folgenden Themen anpacken:

- **Bestellung eines qualifizierten Datenschutzbeauftragten.** Dies könnte sowohl ein Mitarbeiter als auch ein externer Dienstleister sein. Angesichts der Haftungsrisiken und der unverzichtbaren Unabhängigkeit, kann die Bestellung eines externen Dienstleisters mitunter die geeignete Alternative sein, da dieser die Situation unabhängig von den vorhandenen unternehmensinternen Strukturen und Beziehungsgeflechten betrachtet.
- **Durchführung einer Risikoanalyse.** Diese sollte mit der Bestandsaufnahme beginnen und nach einem Soll-Ist-Vergleich in der Behebung etwaiger Mängel münden.
- Erstellung eines **Verzeichnisses der Verarbeitungstätigkeiten**
- **Dokumentation der vorhandenen technischen und organisatorischen Maßnahmen** zum Datenschutz.
- **Gegebenenfalls Änderung bestehender Betriebsvereinbarungen und Einbeziehung des Betriebsrates**, falls ein solcher existiert.
- Darüber hinaus seien auch die **datenschutzrechtliche Sensibilisierung und ggf. Schulung der Mitarbeiter** sind unverzichtbar.

WORAUF ACHTEN BEIM WEBAUFTRETT?

Darüber hinaus sollte jeder Betrieb, der einen Internetauftritt betreibt, auch weiterhin sicherstellen,

- dass die Einwilligung des Betroffenen vorliegt,

- dass sich die Datenverarbeitung auf das notwendige Maß beschränkt sowie
- dass ein legitimes Interesse an der Datenerhebung dasjenige des Betroffenen überwiegt. Wer die Grundsätze der **Datenschutzrichtlinie 95/46/EG** beachtet, dürfte auf der sicheren Seite sein. Wer Dritte mit der Datenverarbeitung oder der Unterhaltung des Internetauftritts beauftragt hat, sollte auch diese kontrollieren und ggf. anpassen.

WAS IST BEI EINER DATENSCHUTZRECHTLICHEN PANNE ZU TUN?

Sollte es zu datenschutzrechtlich relevanten Vorfällen kommen oder gekommen sein, sind diese der für den Sitz des Unternehmens zuständigen Aufsichtsbehörde unverzüglich, spätestens aber innerhalb von 72 Stunden zu melden, heißt es in der DSGVO. Zuständig sei in aller Regel der bzw. die Landesbeauftragte oder das Landesamt für Datenschutz. Im Gegensatz zur bisherigen Regelung, bei der die Aufsichtsbehörde nur dann informiert werden musste, wenn eine schwerwiegende Beeinträchtigung der Betroffenen zu befürchten war (z.B. wenn Dritte unberechtigt Bank-, Kreditkarten- oder Gesundheitsdaten in ihren Besitz gebracht hatten), **besteht die Meldepflicht künftig bei jeder Verletzung personenbezogener Daten**. Gemäß Art. 33 DSGVO kann die Meldung unterbleiben, wenn „die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.“ Eine genaue Übersicht darüber, [was konkret im Fall einer Datenschutz-Panne zu beachten ist, finden Sie hier](#).