



BRING YOUR OWN DEVICE UND DATENSCHUTZ

BYOD ist ein zunehmend wichtiger Faktor im Wettbewerb um Mitarbeiter, die gerne ihr schickes neues Notebook oder ihr multifunktionales Smartphone für die Erledigung ihrer beruflichen Aufgaben hernehmen möchten. Immer mehr Unternehmen geben diesen Forderungen nach und nehmen dafür rechtliche Risiken in Kauf. Ein wesentlicher Aspekt ist in diesem Zusammenhang der Datenschutz, da das Unternehmen als verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes (BDSG) auch dann für die Einhaltung der Datenschutz-Standards haftet, wenn im geschäftlichen Umfeld personenbezogene Daten auf dem privaten Endgerät des Mitarbeiters verarbeitet werden.

Doch wie will das Unternehmen diese Standards auf einem Privatgerät durchsetzen oder gar kontrollieren, ohne dabei seinerseits die datenschutzrechtlichen Belange seines Mitarbeiters (Fernmeldegeheimnis) z.B. in Bezug auf seine privaten E-Mails zu verletzen?

Schon wird deutlich, dass BYOD ohne hinreichende technische Implementierung kaum praktikabel ist. Um zudem eine aus Sicht des Unternehmens (haftungs)rechtlich vertretbare Umsetzung von BYOD zu ermöglichen, ist die Schaffung eines gewissen rechtlichen Rahmens unter datenschutzrechtlichen Gesichtspunkten unerlässlich. In diesem Zusammenhang ist BYOD im Falle eines Mitarbeiters der Personalabteilung, der überwiegend personenbezogene Daten bearbeitet, sicherlich anders zu beurteilen als bei einem Mitarbeiter der Pressestelle, der eher unternehmensbezogene Informationen bearbeitet, die – mangels Personenbezug – keinen Datenschutz genießen.

Ein einheitlicher Rechtsrahmen müsste sich gleichwohl am strengsten Maßstab orientieren. Wenn man sich nun noch vor Augen führt, dass der Mitarbeiter sein Smartphone oder Notebook mit personenbezogenen Daten mit ins Ausland (z.B. nach Kuba) nimmt, wo dann lokales Datenschutzrecht gilt, dann wird schnell deutlich, welche Komplexität BYOD haben kann.