

von Dr. Sebastian Kraska

# Arbeitnehmerdatenschutz: Überblick über die Datenschutz-Regelungen im Arbeitsverhältnis

Der Arbeitnehmerdatenschutz ist in Deutschland nicht übersichtlich in einem eigenen Arbeitnehmerdatenschutzgesetz geregelt, auch wenn dies verfassungs- und europarechtlich an sich gefordert wäre. Vielmehr ergeben sich die gesetzlichen Rahmenbedingungen aus der Anwendung des allgemeinen Bundesdatenschutzgesetzes (BDSG) und einer Reihe bereichsspezifischer Vorschriften.

## Überblick

Im Grundsatz orientiert sich Arbeitnehmerdatenschutz und damit die Erfassung und Verarbeitung von Beschäftigtendaten an den Vorschriften des BDSG. Die Verarbeitung von personenbezogenen Daten der Beschäftigten darf danach nur dann erfolgen, wenn diese entweder durch eine Rechtsvorschrift ausdrücklich erlaubt ist oder der betroffene Arbeitnehmer der Datenverarbeitung zugestimmt hat (§ 4 Abs. 1 BDSG). Die Vorschriften des BDSG sind Generalklauseln, welche nur dann zur Anwendung kommen, wenn sie nicht durch vorrangige gesetzliche Regelungen verdrängt werden.

Daneben gibt es eine Reihe von bereichsspezifischen Gesetzen, d.h. auf bestimmte Lebensbereiche und Personen begrenzte Vorschriften. Diese existieren beispielsweise im Bereich des Telekommunikationssektors (Telemediengesetz TMG und Telekommunikationsgesetz TKG) oder im Anwendungsbereich des Arbeitssicherheitsgesetzes oder des vor kurzem in Kraft getretenen Gendiagnostikgesetzes.

## Das Bundesdatenschutzgesetz

Im Unterschied zu den zahlreichen Datenschutzgesetzen der Länder, welche lediglich den Datenumgang in Behörden und öffentlichen Körperschaften des jeweiligen Landes regeln, erfasst das BDSG neben Behörden des Bundes auch die Privatwirtschaft. Privatwirtschaftliche Beschäftigungsverhältnisse sind erfasst, wenn die Datenverarbeitung automatisiert, d.h. insbesondere unter Verwendung von Datenverarbeitungsanlagen (z.B. PCs) stattfindet. Es regelt die Erhebung, Verarbeitung (hierunter fällt Speichern, Verändern, Übermitteln, Sperren und Löschen von Daten) und Nutzung von Daten der Beschäftigten. Dies setzt allerdings voraus, dass es sich um personenbezogene Daten handelt. Dies sind solche Daten, die sich auf eine bestimmte einzelne Person beziehen oder zumindest dazu geeignet sind, einen Bezug zu ihr herzustellen (z.B. Name, Anschrift, Familienstand, Geburtsdatum, Krankheiten, Vorstrafen, Beruf, Internetsurfverhalten, Foto etc.).

## § 3 BDSG - Weitere Begriffsbestimmungen

“

*(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). (...)*

”

In seinem Geltungsbereich unterscheidet das BDSG also verschiedene Phasen im Umgang mit personenbezogenen Daten (§ 1 Abs. 1 BDSG – Erheben, Verarbeiten und Nutzen) und ordnet in § 4 Abs. 1 BDSG ein „Verbot mit Erlaubnisvorbehalt“ an. Der Umgang mit personenbezogenen Beschäftigtendaten ist damit nur dann zulässig, wenn eine gesetzliche Norm dies erlaubt oder der Beschäftigte den Umgang mit den Daten ausdrücklich gestattet.

### Erlaubnisnorm § 32 BDSG

Das BDSG selbst stellt Erlaubnistatbestände in den §§ 28, 32 BDSG auf. Die Spezialvorschrift des § 32 BDSG wurde erst im Jahr 2009 in das BDSG eingefügt und regelt den Umgang mit Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses. Der bisher in diesem Zusammenhang anwendbare § 28 Abs. 1 BDSG wird damit in vielen Fällen verdrängt. § 32 BDSG kann wohl als legislative Reaktion auf die jüngsten Datenschutzskandale bezeichnet werden, denn er ist erst mit der Entwurfsfassung vom 1.7.2009 kurzfristig in die BDSG-Novelle II eingefügt worden. Während § 32 Abs. 1 S.2 BDSG eine Regelung zur Aufdeckung von durch Beschäftigte begangene Straftaten enthält und damit an eine bereits begangene Straftat anknüpft, soll § 32 Abs. 1 S. 1 BDSG den „präventiven“ Umgang mit Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses regeln und insofern die Rechtsprechung zur verdeckten Überwachung von Beschäftigten berücksichtigen.

In einer im Rahmen von § 32 Abs. 1 S. 1 BDSG erforderlichen Abwägung sind die Rechte des Betroffenen umfassend zu berücksichtigen und die Eingriffsintensität in das Persönlichkeitsrecht des Beschäftigten dem Interesse des Arbeitgebers an der Verarbeitung der Daten gegenüber zu stellen.

### Einwilligung des Arbeitnehmers

Sofern eine Erlaubnisnorm zum Umgang mit den Daten des Arbeitnehmers nicht zur Verfügung steht, ist die Verarbeitung, Nutzung etc. nur zulässig, wenn der Betroffene sein Einverständnis zur Verarbeitung seiner Daten erteilt (Einwilligung). Voraussetzung dafür ist, dass dem Betroffenen hinreichende Informationen über die Art der vorgesehenen Datenverarbeitung und ihren Zweck zugänglich gemacht werden. Eine Erklärung dergestalt, dass pauschal in jede Form der Datenverarbeitung eingewilligt wird, genügt den rechtlichen Vorgaben nicht und ist damit für eine Datenverarbeitung unzureichend. Gerade im Arbeitsverhältnis ist die Einwilligung eine problematische Grundlage, da fraglich sein kann, ob die Einwilligung des Beschäftigten gänzlich ohne „Zwang“ erfolgen und der Beschäftigte die Zustimmung sanktionslos verweigern kann. § 4a Abs. 1 BDSG verlangt jedoch, dass die Einwilligung auf „der freien

Entscheidung des Betroffenen“ beruht. Zudem kann eine Einwilligung auch nach Erteilung widerrufen werden. Aus Arbeitgebersicht sollte in der betrieblichen Praxis daher nach Möglichkeit auf Arbeitnehmereinwilligungen verzichtet werden.

## Vorrangige gesetzliche Regelungen / Betriebliche Kommunikationstechnik

Dort wo Beschäftigten Telekommunikationsgeräte und -techniken (z.B. Telefon, PC, Internet und E-Mail, Mobiltelefon etc.) vom Arbeitgeber zur Verfügung gestellt werden stellt sich die Frage, auf welcher gesetzlichen Grundlage die dabei entstehenden Daten vom Arbeitgeber überwacht werden können. Im Grundsatz ist hier zwischen privater und dienstlicher Nutzung zu unterscheiden. Während es bei der rein dienstlichen Nutzung des Büro-PCs bei der Anwendung des BDSG bleibt, wird dieses bei der (auch stillschweigend) erlaubten Privatnutzung von Spezialvorschriften verdrängt. Konsequenz einer vom Arbeitgeber gestatteten Privatnutzung ist ein weitgehender Verlust von Kontrollmöglichkeiten über den Datenverkehr betrieblicher Telekommunikationsanlagen. Gestattet ist nach dem TKG zwar die Speicherung anfallender Kommunikationsdaten, die der Datensicherheit, der Aufklärung von Straftaten oder dem technischen Betrieb der Anlage dienen. Nicht überwacht werden dürfte aber beispielsweise, welche Internetseiten der Arbeitnehmer ansteuert oder welchen Inhalt empfangene E-Mails haben.

## Fazit

Beim Umgang mit Arbeitnehmerdaten sind zahlreiche datenschutzrechtliche Besonderheiten zu beachten. Von der Einholung einer datenschutzrechtlichen Einwilligungserklärung der Arbeitnehmer ist nach Möglichkeit abzusehen. Gerade beim Einsatz moderner betrieblicher Kommunikationstechnik sollte externer Rat eingeholt werden, um in datenschutzrechtlich zulässiger Weise den betrieblichen Erfordernissen gerecht zu werden.

Autor:

**Dr. Sebastian Kraska**

Rechtsanwalt