Ähnlich wie auf diesem Motiv angedeutet, bleibt beim Beschäftigten-Datenschutz einiges unklar – trotz neuer Gesetze.

Fotos: picture alliance/ dpa, Lutz P. Kayser

DATENSCHUTZ | Ab Mai 2018 gelten neue Regeln für Beschäftigte – Was ändert sich konkret?

Rolle der Betriebs- und Personalräte in Sachen Datenschutz gestärkt

Ergänzend zur EU-Datenschutzgrundverordnung hat der Bundestag ein neues Bundesdatenschutzgesetz verabschiedet. Beide Gesetze regeln ab Mai 2018 im Zusammenspiel den Datenschutz am Arbeitsplatz.

Von Thomas Hau

Die EU-Datenschutzgrundverordnung wurde nach zähem Ringen verabschiedet. Sie gibt vor, wie in den EU-Mitgliedstaaten mit den persönlichen Daten umgegangen werden muss, damit niemand Schaden nimmt. Der Datenschutz wurde zwar von Grund auf neu geregelt, dabei wurden allerdings auch viele bewährte Prinzipien zum Schutz der Privatsphäre beibehalten, allen voran das Grundrecht, selbst über seine eigenen Daten bestimmen zu können (informationelle Selbstbestimmung). Allerdings blieb der Aspekt des Datenschutzes am Arbeitsplatz ungeregelt. Um diese Lücke zu schließen und wilden Interpretationen Einhalt zu bieten, was man alles mit Beschäftigtendaten machen darf, wurde in Deutschland das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) verabschiedet. Darin beschränkte man sich im Wesentlichen darauf, die bislang geltenden gesetzlichen Vorgaben zu übernehmen. Sowohl die Datenschutzgrundverordnung als auch das Datenschutzanpassungsgesetz treten zeitgleich am 25. Mai 2018 in Kraft.

Bewährtes bleibt

„Alles neu macht der Mai“ stimmt in diesem Fall nicht ganz. Sowohl in der EU-Datenschutzgrundverordnung als auch im Datenschutz-Anpassungsgesetz wurde viel Bewährtes übernommen. Allerdings gibt es auch einige neue Aspekte, auf die sich die Beschäftigten und ihre Interessenvertretungen einstellen müssen. Der neugeschaffene Paragraf 26 im Datenschutzanpassungsgesetz, ersetzt den „alten“ Paragrafen 32 im Bundesdatenschutzgesetz. Dort wird auf weniger als einer Seite der gesamte Beschäftigten-Datenschutz geregelt. Auf den ersten Blick sehen beide Paragrafen identisch aus – die Chance auf eine grundlegende Neuausrichtung des Beschäftigten-Datenschutzes wurde offensichtlich vertan – die Änderungen liegen in den Details.
Nach wie vor gilt der Grundsatz, dass nur die Daten von Beschäftigten erfasst und verarbeitet werden dürfen, wenn es zwingend erforderlich ist, um das Beschäftigungsverhältnis einzugehen, durchzuführen oder zu beenden. Dann muss auch der Beschäftigte nicht einverstanden sein. Sind die Daten hingegen nicht rechtlich erforderlich, sondern im Betriebsablauf einfach nur

nützlich, wie Handynummern und private E-Mailadressen, geht nichts, ohne dass der Beschäftigte sein Einverständnis gibt. Ist man abhängig beschäftigt, ist es ein heikles Thema, dem Arbeitgeber einen solchen „Wunsch“ abzuschlagen.
Deshalb wurde als Neuerung im Datenschutzanpassungsgesetz die Möglichkeit eines persönlichen Einverständnisses des Beschäftigten geregelt und mit Leitplanken versehen. Fortan können sich Mitarbeiter auf diese gesetzliche Regelung in Paragraf 26 Absatz 2 DSAnpUG-EU beziehen, wenn sie diese Daten nicht preisgeben wollen. Grundsätzlich darf eine solche Frage nach Beschäftigtendaten nur gestellt werden, wenn für den Beschäftigten ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird (wie betriebliche Altersvorsorge, Fahrtkostenzuschüsse, Teilnahme an Sportveranstaltungen oder ähnliches) oder Arbeitgeber und Mitarbeiter bei der Verwendung dieser Daten gleiche Interessen haben. Das viel praktizierte Prinzip, „Gib mir Deine Daten, ohne dass Du einen Vorteil davon hast“ ist damit definitiv vom Tisch. Die „neue“ Möglichkeit, Daten mit dem Einverständnis des Beschäftigten zu erhalten und zu verarbeiten, zielt maßgeblich auf Firmen ab, in denen es keine Betriebsräte und damit auch keine Möglichkeit zum Abschluss von Betriebsvereinbarungen gibt.

Positive Neuerung

Erstmalig für ein deutsches Datenschutzgesetz wird in dem Datenschutzanpassungsgesetz deutlich auf die Rolle von Betriebs- und Personalräten verwiesen, durch Abschluss von Betriebs- und Dienstvereinbarungen Mitarbeiter vor Missbrauch ihrer Daten zu schützen. Das ist positiv zu bewerten. Interessenvertretungen können aufgrund ihrer besonderen Rechtsstellung dem Wunsch eines Arbeitgebers, persönliche Daten von Beschäftigten zu erheben, eine Absage erteilen, wenn sich der einzelne Mitarbeiter in dem Zwang sieht, seine Daten preisgeben zu müssen. In diesem Zusammenhang wird darauf verwiesen, dass entweder persönliche Einverständnisse oder Betriebs-/Dienstvereinbarungen vorliegen müssen, wenn Beschäftigtendaten in Konzernen oder Unternehmensgruppen verarbeitet werden sollen.

HINTERGRUND |

Die EU-Datenschutzgrundverordnung zielte vorwiegend darauf ab, die Rechte der EU-Bürger als Verbraucher zu stärken, denn bislang war es Unternehmen ganz legal möglich, sich der Kontrolle durch die nationalen Aufsichtsbehörden zu entziehen. So war für Facebook Deutschland nicht die deutsche Aufsichtsbehörde zuständig, sondern die für ihre wirtschaftsfreundliche Arbeitsweise bekannte Aufsichtsbehörde in Irland. Das machte es deutschen Nutzern schwer, ihre Rechte auf Schutz der Privatsphäre geltend zu machen. Insgesamt gab es 173 Erwägungsgründe, den Schutz der Privatsphäre bei der Datennutzung EU-weit einheitlich zu regeln. Die EU-Datenschutzgrundverordnung löste gleichzeitig das bestehende Bundesdatenschutzgesetz ab. Allerdings waren darin auch wichtige Aspekte geregelt, die sich in der Grundverordnung nicht finden, zum Beispiel die Arbeit der Geheimdienste mit persönlichen Daten und der Beschäftigten-Datenschutz. Durch das DSAnpUG-EU wurden diese Lücken geschlossen. Ohne dieses Gesetz müsste man sich den Beschäftigten-Datenschutz aus der Grundverordnung ableiten. Das würde zu höchst unterschiedlichen Auffassungen führen, was man mit Beschäftigtendaten alles machen darf und was nicht. Das wurde durch das neue Gesetz korrigiert. Ab 25. Mai 2018 gelten in Deutschland beide Gesetze. TH

Bei näherer Betrachtung sind die wenigen Neuerungen jedoch wenig überraschend. Es handelt sich samt und sonders um Regelungen, die auch bislang schon existierten und sich aus Grundsatzurteilen der Arbeitsgerichte begründeten. Nun stehen sie verbindlich in einem Gesetz – immerhin. Ein großer Wurf ist mit dem Datenschutzanpassungsgesetz nicht gelungen: Der Datenschutz bleibt abstrakt und unverständlich. Aspekte wie sie täglich im Betriebsalltag auftreten – wie Standortbestimmung über Handys, Fingerabdruck zum Entsperren des Computers, Nutzung des betrieblichen Internets – all das muss man sich nach wie vor mühsam ableiten.
Grundsätzlich muss man abwarten, ob sich die neuen Regelungen im wirklichen Leben bewähren. Bei der Betrachtung der rasant voranschreitenden Digitalisierung in den Betrieben und Dienststellen gibt es jedoch berechtigte Zweifel, ob die jetzt getroffenen Regelungen die unzulässige Vorratsdatenspeicherung von Beschäftigtendaten wirksam verhindern.

Das will sicher kein Arbeitnehmer, dass seine privaten Daten auf dunklen Kanälen beim Arbeitgeber landen. Deshalb muss der Datenschutz klar geregelt sein.

Etwas Hoffnung

Wie Bundeskanzlerin Angela Merkel (CDU) und der damalige Wirtschaftsminister Sigmar Gabriel (SPD) am 17. November 2016 auf dem Saarbrücker IT-Gipfel bekundeten, soll der Datenschutz nicht den Fortschritt ausbremsen. „Das Prinzip der Datensparsamkeit, wie wir es vor vielen Jahren hatten, kann heute nicht die generelle Leitschnur für die Entwicklung neuer Produkte sein“, erklärte Merkel. Man müsse aufpassen, „dass ein Big-Data-Management dann nicht möglich sein wird“. Dass der Bundestag bei der Verabschiedung des neuen Datenschutzgesetzes diese Ansicht letztlich nicht geteilt, sondern die Rechte der Betroffenen in den Mittelpunkt gestellt hat, lässt zumindest hoffen.

| Thomas Hau ist Berater bei BEST.