

„Selbstverständlich beachten wir die Mitbestimmung!“

Karin Schuler // Datenschutz & IT-Sicherheit, Bonn

HIER LESEN SIE:

- dass gesetzliche Rahmenbedingungen nicht verhandelbar sind
- warum der Interessenvertretung trotz gesetzlicher Vorgaben noch Gestaltungsspielräume bleiben und diese auch ausgenutzt werden können
- drei Grundregeln um sich von vorgeblich zwingenden Gesetzesvorgaben nicht ins Bockshorn jagen zu lassen



Als ob es nicht schon Herausforderung genug wäre, die Mitbestimmung bei IKT-Systemen auf Grundlage des § 87 Abs. 1 Nr. 6 BetrVG bzw. § 75 Abs. 3 Nr. 17 BPersVG umzusetzen. Wie häufig müssen dem Arbeitgeber Grundlagen erläutert werden: dass auch ein „Pilotbetrieb“ schon mitbestimmungspflichtig ist, dass die Information der Interessenvertretung nicht erst erfolgen darf, wenn das System schon gekauft, die Berater bestellt und der Testbetrieb bereits in vollem Gange ist, dass der Betriebs- und Personalrat auch Datenschutzfragen mitbestimmen darf? Wie häufig muss man auch über Umfang und Aussagekraft vorgelegter Unterlagen diskutieren und Nachhilfe bei der Auslegung von Mitbestimmungsgesetzen erteilen? Jede Belegschaftsvertretung, jeder Sachverständige kennt die ritualisierten Schlagabtausche, die sich um die Umsetzung der genannten gesetzlichen Vorschriften ranken.

Und jetzt ein Trend, den man wirklich nicht auch noch brauchte: Immer häufiger stößt man nämlich auf Anwendungen, deren Betrieb in wesentlichen Grundzügen nicht verhandelbar scheint, weil ihr Einsatz gesetzlich normiert ist. Und zwar sowohl durch deutsches als auch durch europäisches oder gar internationales Recht.

Der Arbeitgeber argumentiert dabei häufig auf eine Art, die völlig ungewohnt ist: Er stellt sich als williger Verhandlungspartner dar („Selbstverständlich beachten wir die Mitbestimmung“), dem aber gesetzlich die Hände gebunden seien, weil eine bestimmte Vorschrift den Unternehmen ganz klar die beabsichtigte Verarbeitung

vorschreibe. Oder er setzt dem Betriebsrat – so oder ähnlich – die Pistole auf die Brust: „Wenn wir die Vorgaben des (amerikanischen) Sarbanes-Oxley-Acts nicht erfüllen, werden unsere Aktien nicht mehr an der New Yorker Börse gehandelt“ (siehe hierzu die Beiträge von Jochen Brandt und Dirk Fox in diesem Heft). Er nimmt sich selbst damit recht geschickt aus der Schusslinie und schiebt den Gesetzgeber als Pappkameraden vor. Schlimmer noch: man weiß sich zunächst gar nicht recht mit ihm zu streiten, weil man als Beschäftigtenvertretung ja ebenso an Recht und Gesetz gebunden ist wie das Unternehmen. Besonders heikel ist die Angelegenheit, wenn die gesetzliche

Vorschrift durch Anwendungen umgesetzt werden soll, die datenschutzrechtlich oder in Bezug auf Leistungs- und Verhaltenskontrolle großes Missbrauchspotenzial bergen.

In manchen Fällen scheinen Arbeitgeber gar mit der Belegschaftsvertretung einig, wenn es um die Ablehnung bestimmter gesetzlicher Vorgaben geht. Dennoch wollen sie natürlich keine Gesetze brechen oder sich strafbar machen.

Erfahrungsgemäß lohnt es sich daher immer nachzuforschen, wie weit die gesetzlichen Vorgaben tatsächlich zwingend sind, welche Konsequenzen bei Nichtbeachtung realistischerweise drohen und welche Gestaltungsspielräume man für eine

rechtskonforme Lösung hat. Da zeigt sich dann schnell, wie ernst die Beteuerungen des Arbeitgebers zu nehmen sind. Kann man sich möglicherweise tatsächlich auf eine gerade noch gesetzeskonforme Minimallösung einigen? Oder muss es doch die schöne bunte Software sein, die eigentlich viel mehr tut, als die eben noch beklagte gesetzliche Vorschrift verlangt?

Beispiel: Das leidige EU-Sanktionslistenscreening

Zur Erfüllung von EU-Vorgaben zur Terrorismusbekämpfung (EG 881/2002 und EG 2580/2001) sind im deutschen Außenwirtschaftsgesetz (§ 34 Abs. 4 und 7 AWG) Geschäfte mit sanktionierten Personen oder Institutionen unter Strafe gestellt. Welche Personen oder Institutionen jeweils als sanktioniert zu gelten haben, kann an diversen Sanktionslisten abgelesen werden, die durch die Europäische Union selbst oder auf nationaler Ebene durch Ministerien oder sonstige öffentliche Stellen erstellt werden.

Deutsche Unternehmen müssen daher im Ergebnis verhindern, dass sie durch wirtschaftliche Kontakte den auf den Sanktionslisten verzeichneten Personen die Möglichkeit geben, wirtschaftlich tätig zu werden. Abgesehen davon, dass der Pflegeprozess dieser Listen unter demokratischen Gesichtspunkten äußerst fragwürdig ist, lässt das AWG viele praktisch relevante Fragen ungeklärt: Bei welcher Art von Kontakten muss ein deutsches Unternehmen den Geschäftspartner prüfen? Muss es seine eigenen Mitarbeiter ständig neu überprüfen? Wie genau ist im Falle von Namensgleichheiten zu verfahren? Und viele weitere ...

Insofern kann dieses Gesetz als Paradebeispiel dafür dienen, wie man gerade keine Argumentationsgrundlage für eine umfassende und häufige Mitarbeiterkontrolle schafft. Beispielsweise lässt sich nirgends im Gesetz die Notwendigkeit bestimmter Kontrollzyklen für Mitarbeiter ableiten und nirgendwo wird verlangt, dass das Ergebnis eventuell durchgeführter Screenings dauerhaft aufbewahrt werden muss. Und dies sind nur zwei Gestaltungsfragen, bei denen eine Mitarbeitervertretung im Interesse der Beschäftigten auf eine möglichst daten-

sparsame und zurückhaltende Umsetzung der Bestimmungen des AWG dringen sollte.

Leider führen neue Kontrollvorschriften nicht selten dazu, dass eine Reihe von Softwareherstellern neue Absatzmärkte wittern und so schnell wie möglich Anwendungen zu deren Umsetzung auf den Markt bringen. Und Softwarehersteller lesen nicht immer die zugrunde liegenden Gesetze mit der gebotenen Sorgfalt. So landet manche unnötige, Daten sammelnde Funktion im neuen Produkt – die notwendigen Funktionen zur feingranularen Anpassung auf eigene, datenschutzförderliche Bedürfnisse fehlen hingegen zu oft. Insbesondere die Berechtigungsgestaltung ist oft nicht datenschutzgerecht gelöst. Ist so ein Produkt aber erst einmal verfügbar und beworben, greifen viele Unternehmen dankbar zu. Die unausgesprochene Annahme, was auf dem Markt verfügbar ist, könne nicht rechtswidrig sein, ist so unausrottbar wie falsch. So erlauben viele verbreitete Anwendungen keine geregelte und an den Erforderlichkeitszeitraum angepasste Löschung, was einen datenschutzkonformen Einsatz unmöglich macht. Bestraft wird bei einer Datenschutzprüfung durch die Aufsichtsbehörde jedoch nur der Anwender, nicht der Hersteller einer Software.

Und so kann man immer noch beobachten, dass mancher Software-Anbieter das Vehikel der gesetzlichen Vorgabe nutzt um in seinem Produkt noch ganz andere, weitreichende Funktionen unterzubringen – ohne sich über die datenschutzgerechte Gestaltung viele Gedanken zu machen. Die Interessenvertretung sollte daher auf jeden Fall prüfen, ob ein vorgestelltes Produkt die gesetzlichen Erfordernisse korrekt umsetzt oder möglicherweise übers Ziel hinauschießt. Ist erst einmal ein Produkt gefunden, bleibt anschließend immer noch die Aufgabe, die Konfiguration so datensparsam wie möglich vorzunehmen.

Am Beispiel des EU-Sanktionslistenscreenings würde das etwa heißen, dass man sich mit dem Arbeitgeber unter anderem über die Treffergenauigkeit einigen und diese so hoch wie möglich setzen sollte. Die Treffergenauigkeit bestimmt, wann ein überprüfter Beschäftigter, dessen Name einem auf der Sanktionsliste geführten Namen gleicht, als Treffer eingestuft wird.

Zum Schwerpunkt in dieser Ausgabe

Gemeinsam ist den im vorliegenden Schwerpunkt „Gesetzgebung als Betriebsgrundlage“ aufgegriffenen Fragestellungen und Anwendungen, dass der Gestaltungsspielraum durch gesetzliche Vorgaben stark eingeschränkt ist. Aber obwohl die Ablehnung solcher Anwendungen durch die Beschäftigtenvertretung nicht zur Debatte stehen kann, bestehen Mitbestimmungsrechte und Datenschutzerfordernisse natürlich weiterhin.

Die folgenden Artikel befassen sich daher in Bezug auf einzelne Gesetzesvorgaben mit der Frage, welche Rahmenbedingungen nicht verhandelbar sind, warum sie feststehen, was die gesetzlichen (oder sonstigen) Zwangsjacken genau vorschreiben – und natürlich: welche Gestaltungsspielräume (z. B. für Betriebs- oder Dienstvereinbarungen) trotzdem noch bleiben und ausgenutzt werden können.

Für Interessenvertretungen lassen sich bereits vorab drei Grundregeln mit auf den Weg geben, die man immer parat haben sollte um sich von vorgeblich zwingenden Gesetzesvorgaben nicht ins Bockshorn jagen zu lassen:

- Prüfe den genauen Inhalt und Umfang der harten, gesetzlichen Vorschriften („Der Blick ins Gesetz erleichtert die Rechtsfindung!“).
- Identifiziere die gestaltbaren Aspekte („Wozu macht das Gesetz keine Vorschriften?“).
- Prüfe die Software auf Umsetzungsgüte („Tut sie das, was sie muss und kann man alles Überflüssige abschalten?“).

Autorin

Karin Schuler ist freiberufliche Beraterin für Datenschutz und IKT-Sicherheit, stellvertretende Vorsitzende der Deutschen Vereinigung für Datenschutz e.V. und vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IKT-Produkte (rechtlich/technisch); sie berät Betriebs- und Personalräte, betriebliche Datenschutzbeauftragte und IKT-Sicherheitsbeauftragte; Kontakt: fon 0228 2420733, buero@schuler-ds.de, www.schuler-ds.de