

unterschreiben lassen. Diese Unterschrift wird durch die Signaturkarte ersetzt. Das erspart das Formular und gibt gleichzeitig den Zugriff frei.

Die Signatur erhält der Teilnehmer von einer berechtigten Stelle. Vorgesehen ist, dass sie auf eine Signaturkarte übertragen wird. Er könnte sie auch auf einer CD-ROM, einem USB-Stick oder einem anderen Datenträger erhalten. Der Vorteil der Signaturkarte liegt darin, dass der Teilnehmer mittels eines Passworts bzw. einer PIN nachweisen muss, dass er tatsächlich die Person ist, der ursprünglich die Karte ausgehändigt wurde. Und diese Prüfung kann der Chip auf der Karte machen (genauer: das Programm, das auf dem Chip vorhanden ist).

Durch das ELENA-Verfahren werden alle Beschäftigten, die Sozialleistungen beantragen, gezwungen, eine Signaturkarte zu beantragen. Kritiker behaupten deshalb, dass die Jobkarte auch ein Mittel ist, den Einsatz von Signaturen zu erzwingen. Die ist nämlich seit Jahren wenig erfolgreich.

Zukunft mit ELENA

Das einzig sichere bei ELENA ist, dass eine zentrale Datensammelstelle geschaffen wurde, bei der schützenswerte Daten von Millionen Beschäftigten gespeichert werden. Möglicherweise sind sie vor Hackern geschützt. Sicher können wir nicht sein, dass die gespeicherten Daten in Zukunft nicht für andere Zwecke genutzt werden. Sicher können wir aber sein, dass in Zukunft noch mehr Daten gespeichert und andere Ämter Zugriff auf sie erhalten werden.

Das alles werden wir im Unternehmen nicht verhindern können. Dafür ist der rechtliche Rahmen nicht gegeben. Zwar werden wir überprüfen können, ob tatsächlich nur die zulässigen Daten übermittelt werden. Aber die Missbrauchsgefahr liegt weniger beim Arbeitgeber als bei den politisch Verantwortlichen, die ELENA verabschiedet haben und die für die zukünftige Gestaltung verantwortlich sind.

Autor

Jochen Konrad-Klein ist Berater bei der Technologieberatungsstelle (TBS) Nordrhein-Westfalen, jochen.konrad-klein@tbs-nrw.de, www.tbs-nrw.de

Gläserne Belegschaften?

Eberhard Kiesche / Matthias Wilke

Sieben Jahre nach dem Erscheinen der 4. Auflage legt Däubler eine neue Auflage seines Standardwerks zum Arbeitnehmerdatenschutz vor. Der Autor berücksichtigt in der längst fälligen Neuauflage praxisbezogen die wichtigsten Datenschutzskandale seit dem Frühjahr 2008 und ordnet sie zu Recht als datenschutzwidrig in allen Einzelheiten ein (z. B. Randnummern 2 a–g). Detailliert werden alle gesetzlichen Neuerungen besprochen, die mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) in 2009 Auswirkungen auf den Arbeitnehmerdatenschutz haben.

Im Mittelpunkt des gut verständlichen Handbuchs steht dabei der neue § 32 BDSG,

von Arbeitnehmern genutzt, ist aber langfristig dafür geeignet, so Däublers Einschätzung.

Aus der Fülle seiner rechtlichen Einschätzungen und Hinweise können nur einige Themen hervorgehoben werden. Den Einsatz von Detektiven und Praktikanten als „verdeckte Ermittler“ hält Däubler für unzulässig (Randnummer 294). Die Pflicht zur Vorratsdatenspeicherung nach § 11a des Telekommunikationsgesetzes (Randnummer 378 c) trifft nicht die Arbeitgeber. Ein Screening bzw. Abgleich von Kontodaten oder eine Rasterfahndung nur aufgrund eines Generalverdachts und ohne konkrete Anhaltspunkte für eine Straftat ist nach § 32 Abs. 1 Nr. 2 BDSG nicht mehr zulässig (Randnummern 427 a–e). Daten von Beschäftigten ins Internet zu stellen, ist nur unter ganz engen Voraussetzungen möglich (Randnummern 507 l–m).

Zur Internationalisierung der Verarbeitung von Beschäftigtendaten entwickelt Däubler ganz praktische Hinweise, die insbesondere für Belegschaftsvertretungen und Datenschutzbeauftragte aus international tätigen Unternehmen von großem Nutzen sind. Überzeugend kritisiert dabei Däubler die Konstruktion des „Safe Harbour“ im Falle der USA und jüngste Datenübermittlungen aus der EU in die USA (Randnummer 504 a). Hier täte nach seiner Überzeugung ein inhaltliches Urteil des Europäischen Gerichtshofs Not.

Hilfreich aus Sicht der Praxis der Interessenvertretungen sind weiterhin auch Ausführungen zum Kündigungsschutz und Fortbildungsanspruch für betriebliche Datenschutzbeauftragte (Randnummern 607 a–f, 614 und 614 a), zu neuen Befugnissen der Aufsichtsbehörden, dem erweiterten Katalog von Ordnungswidrigkeiten, veränderten Bußgeldern und vor allem zu strafrechtlichen Sanktionen bei Datenschutzskandalen (Randnummern 623 a, 627 a–i).



die erste zentrale Vorschrift zu einem eigenständigen Beschäftigtendatenschutz (unter anderem: Randnummern 182 a ff., 209 a–b, 306 a).

Wie in den vorherigen Auflagen reagiert Däubler auf alle relevanten technischen Veränderungen und die damit verbundenen Kontrollmöglichkeiten wie z. B. E-Mail und Internet, Gentests, Videoaufnahmen, Bewegungsprofile mit GPS und Handy-Ortung sowie Einsatz der RFID-Technik (z. B. Seiten 143 f., 168 ff., 184, 318). Die RFID-Technik wird zwar im Augenblick nicht für die Kontrolle

Als Ausblick (Randnummer 948) definiert Däubler seine Anforderungen an ein Beschäftigtendatenschutzgesetz. Auch im Betrieb müsse die Zweckbindung von Daten endlich ernst genommen werden. Ein striktes Verbot der Zweckentfremdung sei zu fordern. Die Leitbegriffe im BDSG wie schutzwürdige Belange oder berechtigtes Interesse sollten durch nicht erschöpfende Beispielfälle konkretisiert werden. Dadurch könnte auch die Freiwilligkeit bzw. die Einwilligung im Arbeitsrecht besser handhabbar gemacht werden.

Das BDSG muss sich den neuen technischen Herausforderungen stellen, so z. B. der Videoüberwachung in nicht öffentlich zugänglichen Räumen, der Kontrolle von Telefon, E-Mail und Internet, der Einführung neuer biometrischer Methoden, der Identifizierung und der Ermittlung des Aufenthaltsorts mittels Handy-Ortung. Der Vorschlag des ehemaligen Arbeitsministers Scholz für einen Beschäftigtendatenschutz ist im Handbuch von Däubler abgedruckt.

Die Lektüre macht deutlich, dass das Fragezeichen hinter „Gläserne Belegschaften?“ nicht gestrichen werden kann. Durch seine Ausführungen zur Mitbestimmung verdeutlicht es den Weg, wie das informationelle Selbstbestimmungsrecht auch im Arbeitsleben verwirklicht werden kann. Es erleichtert Betriebs- und Personalräten die praktische Arbeit und ermutigt sie gleichzeitig, ihre Rolle als Garanten des Beschäftigtendatenschutzes wahrzunehmen.

Spiros Simitis, dem Vater des Datenschutzes in Deutschland, kann nur Recht gegeben werden: Das Däubler-Handbuch zum Arbeitnehmerdatenschutz bleibt eine der wichtigsten Publikationen für jeden, der sich mit der Verarbeitung von Arbeitnehmerdaten und ihren Konsequenzen auseinandersetzen will.

Wolfgang Däubler: Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz, 5. Auflage, 2009, Bund-Verlag, 625 Seiten, 49,90 €, ISBN: 978-3-7663-3919-5

Autoren:

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen, eberhard.kiesche@t-online.de
Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel, info@dtb-kassel.de

DATENSCHUTZTIPPS

aus der Praxis, für die Praxis

In dieser Rubrik stellt Hajo Köppen regelmäßig Informationen und Praxisfälle zum Thema Datenschutz vor, wie sie in den Berichten der Datenschutzbeauftragten und Aufsichtsbehörden der Länder und des Bundes zu finden sind ...

Dürfen personenbezogene Daten über Beschäftigte ins Internet? Eine Frage, die immer wieder zu Diskussionen führt - auch zwischen Dienststellenleitern und Personalräten. Einerseits will eine Behörde bürgerfreundlich sein, wogegen auch ein Personalrat nichts haben kann. Auf der anderen Seite haben aber Beschäftigte einen Anspruch auf Wahrung ihrer Persönlichkeitsrechte durch den Dienstherrn, worüber Personalräte wiederum zu wachen haben. Im 29. Tätigkeitsbericht (2008/2009) geht der Landesdatenschutzbeauftragte von Baden-Württemberg, Jörg Klingbeil, erneut auf diese Fragestellung ein (Seite 77) und revidiert seine bisherige Position.

Beschäftigtendaten ins Internet?

In der Vergangenheit wurde in den Tätigkeitsberichten aus Baden-Württemberg mehrfach diese Frage behandelt. Beispielsweise wurde im 23. Tätigkeitsbericht für das Jahr 2002 (Seite 69) darauf hingewiesen, dass die Veröffentlichung von Beschäftigten im Internet grundsätzlich nur mit Einwilligung zulässig ist; Ausnahmen seien nur hinsichtlich der Namen, dienstlichen Funktion und Erreichbarkeit von leitenden Beschäftigten sowie von Beschäftigten mit regelmäßigen Außenkontakten vertretbar, wobei auf die Umstände des jeweiligen Einzelfalls abzustellen sei. Im 26. Tätigkeitsbericht (2005, Seite 64) wurde zudem gefordert, dass stets sorgfältig geprüft werden müsse, ob auf die Angabe des Namens des Beschäftigten verzichtet werden kann, weil

die Angabe der dienstlichen Funktion und der dienstlichen Erreichbarkeit genügt. Dabei wurde darauf hingewiesen, dass etwa eine funktionsbezogene E-Mail-Adresse ohne den Namen des Beschäftigten auskommt.

Einfache „Spielregeln“, möchte man meinen, die allerdings nicht immer berücksichtigt werden, wie die Datenschützer in Baden-Württemberg feststellen mussten:

AUFSICHTSBEHÖRDE

Landesbeauftragter für den Datenschutz Baden-Württemberg
 Urbanstraße 32, 70182 Stuttgart
 fon 0711 61 55 41-0, fax 0711 61 55 41-15
 poststelle@fd.bwl.de

► www.baden-wuerttemberg.datenschutz.de

„Im Berichtszeitraum sind meine Mitarbeiter und ich dagegen immer wieder auf Internet-Seiten öffentlicher Stellen gestoßen, die nicht diesen Kriterien entsprachen. So fand meine Dienststelle auf der Internet-Seite einer Schule unter anderem weltweit uneingeschränkt abrufbare Elternbriefe. Darin waren nicht nur neue Lehrkräfte mit Namen und Unterrichtsfächern genannt, sondern es war auch zu lesen, dass zwei namentlich genannte Lehrerinnen ‚mit Beginn der Mutterschutzfrist beurlaubt‘ wurden.“ Diese und andere Erfahrungen haben den Datenschutzbeauftragten veranlasst, seine bisherige Position zu überdenken: „Aufgrund der Entwicklungen in letzter Zeit halte ich – über den Bereich der Schulen hinaus – das Veröf-