

Link: <https://www.computerwoche.de/a/paragraf-32-korrekturbeduerftig,2484317>

Datenschutzgesetz

Paragraf 32 korrekturbedürftig

Datum: 10.02.2011

Autor(en): Johannes Klostermeier

Vor kurzem hat das Bundeskabinett den Gesetzentwurf zum Arbeitnehmerdatenschutz beschlossen. Der Kölner Datenschutz-Rechtsexperte Professor Norbert Nolte aus der Kanzlei Freshfields Bruckhaus Deringer rät Unternehmen im Exklusiv-Interview mit CIO.de, private E-Mails zu verbieten.

Am 25. August 2010 hat die Bundesregierung einen Gesetzesentwurf zum Beschäftigtendatenschutz durch Ergänzung des Bundesdatenschutzgesetzes verabschiedet. Hintergrund ist der gesetzgeberische Schnellschuss des vergangenen Jahres zum Beschäftigtendatenschutz. Der Paragraf 32 im Bundesdatenschutzgesetz gilt laut allgemeiner Expertenmeinung als dringend korrekturbedürftig. **CIO.de**¹ berichtete darüber (**Probleme mit Compliance**²).

Von den geplanten Neuregelungen ist praktisch die gesamte Datenerhebung und Datennutzung durch Arbeitgeber im Verlauf eines Beschäftigungsverhältnisses betroffen. CIO.de sprach mit dem Kölner Datenschutz-Rechtsexperten Professor Norbert Nolte aus der **Kanzlei Freshfields Bruckhaus Deringer**³ über die Gesetzesnovelle.

CIO.de: Das Kabinett hat gerade den Gesetzentwurf zum Arbeitnehmerdatenschutz **beschlossen**⁴. Ist das eine gute Nachricht für die Unternehmen aus Expertensicht?



Der Kölner Datenschutz-Rechtsexperte Professor Norbert Nolte von der Kanzlei Freshfields Bruckhaus Deringer fordert eindeutige Regelungen.

Norbert Nolte: Im vergangenen Jahr hat der Gesetzgeber kurz vor den Wahlen einen gesetzgeberischen Schnellschuss losgelassen und versucht, in einem einzigen Paragraphen den gesamten Beschäftigtendatenschutz zu regeln. Man ist sich einig, dass das misslungen ist und dass es hier einer Änderung bedarf. Das steht so auch im Koalitionsvertrag. Die geplante Neuregelung erfüllt dieses Versprechen.

Aus rechtlicher Sicht, aus Arbeitnehmersicht und aus Arbeitgebersicht ist eine Neuregelung sinnvoll und hilfreich. Ich meine, es ist auch eindeutig, dass die neuen Regelungen Verbesserungen gegenüber dem Ist-Zustand bringen. Denn der jetzige Zustand ist viel zu unbestimmt. Jedes einzelne Thema bedurfte der rechtlichen Prüfung durch Juristen.

CIO.de: Das war doch gut für die Juristen, oder?

Nolte: Wir leben lieber von verlässlichen Antworten, als dass wir sagen müssen, "das kann eine Behörde auch wiederum anders sehen". Das hilft dem Mandanten nicht - und uns letztlich auch nicht. Wir freuen uns über eine klare Regelung.

CIO.de: Das Kabinett hat den Entwurf jetzt beschlossen. Das bedeutet aber nicht, dass es auf dem Weg zum Gesetz keine Änderungen mehr geben wird?

Nolte: Ja, das ist richtig. Die Regierung hat sich nun entschieden, ein solches Gesetz in den Bundestag einzubringen. Aber erst jetzt entscheidet der Gesetzgeber. Wir sind also noch im Vorfeld, im Gesetzgebungsverfahren. In diesem frühen Stadium kann sich noch einiges ändern. Es gibt an einigen Stellen Nachbesserungsbedarf.

CIO.de: Der DGB und die Arbeitgeberverbände haben sich beide kritisch zu dem Entwurf geäußert. Ist das ein gutes Zeichen?

Nolte: Der Teufel steckt im Detail, man muss sich jeden einzelnen Kritikpunkt genau anschauen. Mal fühlt sich die Arbeitnehmerseite benachteiligt oder sieht eine Verschlechterung gegenüber dem Ist-Zustand. Auf der anderen Seite sagen die Arbeitgeber, dass sie viele der von ihnen verlangten Maßnahmen, besonders im Bereich Compliance, in Zukunft nicht mehr durchführen können. Das ist ein Dilemma.

IT-Abteilungen besonders betroffen - Compliance wird verhindert

CIO.de: In den USA werden Unternehmen abgestraft, weil sie bestimmte Compliance-Regeln nicht eingehalten haben. Wird es für die deutschen Unternehmen jetzt einfacher oder schwieriger?

Nolte: Jedenfalls nicht leichter. Das betrifft besonders die IT-Abteilungen von Unternehmen. Das neue Gesetz bringt eine gute Klarstellung, in dem es feststellt, dass Firmen Beschäftigtendaten zur Wahrnehmung von Leistungs- und Verhaltenskontrollen erheben darf. Aber verschiedene Einzelregelungen machen das Leben der Compliance-Verantwortlichen und des IT-Chef nicht leichter. Ja, sie verhindern sogar die Einhaltung von Compliance-Maßnahmen.

CIO.de: Das sollten wir uns im Einzelnen näher angucken.

Nolte: Automatisierte Datenabgleiche von vorhandenen Beschäftigtendaten werden jetzt erlaubt zur Aufklärung von Straftaten und – das ist neu – von schwerwiegenden Pflichtverletzungen. Im Gesetz wird dieses Verfahren beschrieben. Erst anonym: Habe ich einen konkreten Verdacht, darf ich auf die Personenverknüpfung zurückgreifen, auf den einzelnen Beschäftigten, der unter Verdacht steht, und kann weiter ermitteln. Das ist verhältnismäßig, angemessen und meines Erachtens auch richtig.

Schwierig ist aber das Thema der Datenverarbeitung und der Erhebung von Daten ohne Kenntnis der Betroffenen. Man kann ja in vielen Fällen nicht unmittelbar zu demjenigen gehen, den man im Verdacht hat, und ihm mitteilen, dass man dagegen Maßnahmen plant. Denn dann werden diese erfolglos ins Leere gehen. Der Gesetzgeber sagt jetzt, man muss einen konkreten Verdacht wegen einer Straftat oder einer schwerwiegenden Pflichtverletzung gegen einen bestimmten Beschäftigten haben. Nur dann dürfe der Arbeitgeber neue Daten erheben. Oft hat man aber nur einen Verdacht gegen eine Gruppe von Beschäftigten. Deswegen sollte man diese Regelung auf einen Geschäftsbereich oder eine Abteilung ausdehnen.

Empfehlung: Private E-Mails verbieten

CIO.de: Ein weiterer Streitpunkt war immer die E-Mail-Kontrolle. Raten Sie auch dazu, die private Nutzung zu verbieten, um hier Klarheit zu schaffen?

Nolte: Das ist unsere Empfehlung, damit Kontrollmaßnahmen möglich bleiben. Ich befürchte, dass der Gesetzgeber die Unternehmen mit der Neuregelung in dieses Verbot hinein treibt. Ob das aber im Interesse der Arbeitnehmer ist, bezweifle ich. Wir alle nutzen doch E-Mail-Systeme am Arbeitsplatz in kleinerem Umfang gerne auch privat. Der Arbeitgeber würde ohne ein solches Verbot in Zukunft aber selbst auch in Verdachtsfällen regelmäßig daran gehindert, die E-Mails auf dem betrieblichen Server zu kontrollieren. Das leuchtet mir nicht ein, und das ist einer der Hauptkritikpunkte an dem Gesetzentwurf.

CIO.de: Es ist auch immer noch nicht geklärt, ob Unternehmen als TK-Anbieter anzusehen sind, ist das richtig?

Nolte: Eine Klärung wäre hier sehr hilfreich, schon deshalb, weil die Einräumung der Nutzungsmöglichkeit der E-Mail für private Zwecke ein Goodie ist, das ein Arbeitgeber einem Arbeitnehmer einräumen kann – oder auch nicht. Wenn er es denn gewährt, sollte er aber nicht wie die Telekom, 1&1 oder Alice als TK-Dienstleister angesehen werden, sondern weiter Arbeitgeber bleiben und in dieser Funktion auch weiterhin Zugriff auf die eigenen IT-Systeme haben.

Die private Nutzung infiziert sonst den gesamten E-Mail-Account, macht den Arbeitgeber zum TK-Anbieter und unterwirft ihn so dem Fernmeldegeheimnis mit allen Konsequenzen - bis hin zu dahinter stehenden strafrechtlichen Drohungen. Wir raten den Unternehmen, die private Nutzung zu verbieten und dieses auch zu kontrollieren. Nur so können sie die Anforderungen der Staatsanwälte oder etwa der Kartellbehörden, erfüllen, zum Beispiel bei einer Fusion betriebliche Daten umfassend bereit zu stellen. Sonst haben die Verantwortlichen ein Problem.

CIO.de: Bisher haben sich noch nicht viele Unternehmen an Ihren Ratschlag gehalten, oder?

Nolte: Da ist richtig. Wir haben dazu keine empirischen Daten, aber die allermeisten Unternehmen dulden den privaten E-Mail-Verkehr oder kontrollieren ein Verbot nicht konsequent.

Dazu kommt: Der Gesetzgeber will Kontrollmaßnahmen in Zukunft auch bei Einwilligung der Beschäftigten oder wenn Betriebsvereinbarungen darüber geschlossen wurden nicht mehr ermöglichen. Diese Einschränkung ist meines Erachtens eine Entmündigung der Betriebsräte und der zweite große Kritikpunkt am Gesetzentwurf.

CIO.de: Was gibt es noch für neue Punkte im Gesetzentwurf?

Bei Xing und LinkedIn will ich als Bewerber von einem potenziellen Arbeitgeber gefunden werden. Andere soziale Netzwerke haben dagegen einen privaten Charakter. Was das Bewerbungsverfahren angeht, ist vieles sehr vernünftig geregelt. Obwohl man natürlich darüber nachdenken kann, wie realistisch es ist, den HR-Abteilungen zu verbieten, bei Facebook oder Studi VZ nachzuschauen.

"Es sollte Nachbesserungen geben"

CIO.de: Haben Sie Bedenken zur Videoüberwachung?

Nolte: Hier ist der Kabinettsentwurf schärfer als der Vorschlag der Ministerien: Die heimliche Videoüberwachung ist jetzt komplett verboten. Wenn ich einen Verdacht habe, weil sich eine Ware im Lager ständig dezimiert, dann darf ich darauf keine heimliche Videoüberwachung mehr ausrichten. Das kann eine schwierige Einschränkung sein, denn eine ganze Lagerhalle kann man gar nicht komplett überwachen. Das macht nur Sinn, wenn es heimlich geschieht.

CIO.de: Wird Ihre Beratung in Zukunft einfacher?

Nolte: Ja und nein. Es sollte noch Nachbesserungen geben. Zwar wird man unbestimmte Rechtsbegriffe im Datenschutz nie ganz vermeiden können. Beim Entwurf wurde aber noch nicht vollständig sauber gearbeitet. Grundsätzlich können nicht zu allen Fragen Antworten im Gesetz stehen, weder zum Beschäftigtenschutz noch zur Wahrung der Interessen der Arbeitgeber. In vielen Einzelfällen kann immer noch Streit entstehen.

CIO.de: Müssen Unternehmen in Zukunft noch mehr auf die Einhaltung der Compliance-Regeln achten?

Nolte: Schon heute sind alle Unternehmen, die international agieren, ausländischen Rechtsordnungen unterworfen. Wenn Sie amerikanische Entscheidungen lesen, sehen Sie die Richter bildlich mit dem Kopf schütteln, wenn deutsche Unternehmen argumentieren, sie können bestimmte Daten nicht zur Verfügung stellen, weil es datenschutzrechtlich auch zum Zwecke der Compliance nicht erlaubt ist. In den USA versteht man das nicht. Sanktionen gibt es trotzdem. Das ist das große Problem der Compliance-Beauftragten. Das neue Gesetz verbessert das zwar in vielen Bereichen, in anderen, insbesondere was das E-Mail-Thema angeht, aber eben nicht. Ungeregelt bleibt auch der Datentransfer im Konzern, der zum Beispiel bei der konzernweiten Einführung einer SAP-Lösung notwendig werden kann. Das Gesetz behandelt derzeit jedes Konzernunternehmen wie einen fremden Dritten. Das ist wenig praxisgerecht.

Professor Norbert Nolte ist Rechtsanwalt und Partner im Kölner Büro von Freshfields Bruckhaus Deringer und Experte für Datenschutzrecht und Compliance.

Quelle: **CIO**⁵

Links im Artikel:

¹ <https://www.cio.de/>

² <https://www.cio.de/public-ict/datenschutz/2242961/index.html>

³ <http://www.freshfields.de/>

⁴ <https://www.computerwoche.de/management/compliance-recht/2352200/>

⁵ <https://www.cio.de/public-ict/datenschutz/2246127/index.html>

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.