



Stellungnahme

der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

*zum Referentenentwurf eines
Gesetzes zur Regelung des
Beschäftigtendatenschutzes
(Stand: 28.05.2010)*

I. Grundsätzliches

Die GDD begrüßt, dass das Bundesinnenministerium seiner Ankündigung gefolgt ist, in seinem Entwurf den Beschäftigtendatenschutz nicht in einem eigenständigen Gesetzeswerk, sondern als Abschnitt des Bundesdatenschutzgesetzes zu regeln. Positiv bewertet die GDD auch die Intention des Referentenentwurfs, eine gesetzliche Konkretisierung des richterrechtlich geprägten Arbeitnehmerdatenschutzes herbeizuführen. Zugleich ist es für die Fortentwicklung des Beschäftigtendatenschutzes sinnvoll, den Einsatz der Informations- und Kommunikationstechnologien im Beschäftigungsverhältnis unter dem Gesichtspunkt des Persönlichkeitsrechtsschutzes zu konkretisieren.

Bei einer Bestandsaufnahme der Regelungsinhalte vermisst die GDD allerdings eine Regelung der Datenschutzkontrolle beim Betriebsrat. Wie das Bundesarbeitsgericht in seiner Entscheidung vom 11.11.1997 angeregt hat, sollte in einem Arbeitnehmerdatenschutzgesetz die ungeklärte Rechtsfrage der Kontrolle des Betriebsrates durch den betrieblichen Datenschutzbeauftragten geregelt werden. Diese Rechtsfrage ist nach dem vorliegenden Entwurf weiterhin ungeklärt.

Der Referentenentwurf sieht ebenfalls keine Klarstellung hinsichtlich des zulässigen Inhalts bzw. der zulässigen Reichweite von Betriebsvereinbarungen vor. So ist bisher nicht eindeutig geklärt, inwiefern eine Betriebsvereinbarung vom Schutzniveau des BDSG abweichen kann. Hier bedarf es einer Klarstellung dahingehend, dass Betriebsvereinbarungen das Schutzniveau des BDSG nicht unterschreiten dürfen, sondern allenfalls anwendungsbezogen konkretisieren können und vor diesem datenschutzrechtlichen Hintergrund die Zugriffsrechte der Mitarbeitervertretung ebenfalls nach den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit einzuräumen sind.

Der Referentenentwurf trägt auch nicht Datenverarbeitungen von Beschäftigten im Konzern und Unternehmensverbänden Rechnung. Zunehmend werden unternehmerische

Ziele in nationalen und multinationalen Unternehmensverbänden verfolgt, wobei die Konzerne im wachsenden Maße darauf angewiesen sind, Mitarbeiterdaten im Rahmen ihrer Geschäftstätigkeit an konzernangehörige Unternehmen zu transferieren. Vielfach ist die Rechtsgrundlage für die notwendigen Datentransfers nicht ausreichend klar.

Einen Ansatz für arbeitsteiliges Zusammenwirken im Unternehmensverbund bietet die Regelung des § 32 Abs. 1 Satz 1 Halbsatz 2 BDSG-E, wonach die Vorschriften des Unterabschnitts auch auf Dritte anzuwenden sind, die für den Arbeitgeber tätig werden. Diese Regelung unterstellt, dass Arbeitgeberfunktionen auch auf Dritte ausgelagert werden können, so wie es bei Konzernen und Unternehmensverbänden häufig der Fall ist. Hier wäre eine gesetzliche Konkretisierung von standardisierten oder regelmäßig anzutreffenden Datenweitergaben wünschenswert.

Im Zusammenhang mit der Regelung des Beschäftigtendatenschutzes wäre auch eine Stärkung der Rechtsstellung des betrieblichen Datenschutzbeauftragten wünschenswert. Dabei kommt der ihm gesetzlich zugewiesenen Vorabkontrolle eine entscheidende Bedeutung zu. Der vorliegende Entwurf regelt diese Vorabkontrolle jedoch nur im Zusammenhang mit der verdeckten Videoüberwachung. Die isolierte Regelung der Vorabkontrolle in diesem Zusammenhang ist für die Gesamtbeurteilung der Notwendigkeit der Vorabkontrolle irreführend, da insoweit eine Rechtsunsicherheit dahingehend entsteht, ob bei anderen kritischen Datenverarbeitungen im Zusammenhang mit der Verarbeitung von Beschäftigtendaten keine Vorabkontrolle notwendig ist. Deshalb ist es ratsam, die Vorabkontrolle für den kritischen Umgang mit Beschäftigtendaten in einer generellen Bestimmung zu präzisieren.

Zu beanstanden ist überdies die Zersplitterung der Compliance-Regelungen innerhalb des Referentenentwurfs. Da wesentlicher Auslöser für die Vorlage des Gesetzentwurfs die rechtliche Unsicherheit über den zulässigen Umfang von Compliance-Maßnahmen ist, wäre es insofern sinnvoll, eine eigenständige abschließende Regelung für diesen Themenbereich vorzusehen. Darüber hinaus bedarf es einer eindeutigen Abgrenzung von präventiven und repressiven Zulässigkeitstatbeständen.

Generell ist im Hinblick auf die Gesetzestechnik anzumerken, dass entgegen der üblichen BDSG-Systematik getrennte Regelungen für die Datenerhebung bzw. die anschließende Datenverarbeitung und -nutzung geschaffen werden. Hier wäre es im Sinne der Verständlichkeit der gesetzlichen Regelungen ratsam, einheitliche Lebenssachverhalte jeweils in einer Vorschrift zusammenzuführen und z.B. eine Vorschrift über die Erhebung, Verarbeitung und Nutzung im Bewerbungsverfahren zu schaffen. Dadurch können auch gesetzliche Redundanzen und Verweisungen, die die Verständlichkeit und Lesbarkeit des Gesetzes erheblich erschweren, vermieden werden.

II. Zu den einzelnen Regelungen

Zu § 3 Abs. 13 BDSG-E

Diese Regelung nimmt eine Definition des Arbeitgebers vor und bezieht hierbei auch den Entleiher von Arbeitnehmern ein. Um Kollisionen mit dem arbeitsrechtlichen Arbeitgeber-Begriff zu vermeiden, sollte insoweit dahingehend formuliert werden, dass Entleiher von Beschäftigten Arbeitgebern gleichgestellt werden.

Zu § 32 Abs. 1 Satz 1 Halbsatz 2 BDSG-E

Die Formulierung „Dritte, die für den Arbeitgeber tätig werden“, ist mit Blick auf das gesetzgeberisch verfolgte Ziel zu unspezifisch. So werden Unternehmen, die mit der eigenverantwortlichen Personalsuche beauftragt werden („Headhunter“), zwar für den Arbeitgeber tätig, übernehmen aber keine Arbeitgeberfunktion, so dass für die Anwendung der §§ 32 ff. BDSG-E kein Raum ist. Besser wäre eine gesetzliche Formulierung wie folgt: „Sofern Dritte Arbeitgeberfunktionen wahrnehmen,“

Zu § 32a BDSG-E

§ 32a BDSG-E enthält Regelungen für die Datenerhebung vor Begründung des Beschäftigungsverhältnisses. Der Datenumgang im Zusammenhang mit internen Stellenausschreibungen stellt in der Praxis allerdings eine vergleichbare Problemstellung dar. Insofern ist eine Ergänzung der geplanten Regelung zu erwägen.

§ 32a Abs. 3 BDSG-E regelt die Zulässigkeit arbeitgeberseitig veranlasster gesundheitlicher Untersuchungen des Beschäftigten. Letztere sollen nach der geplanten Regelung von der Einwilligung des Arbeitnehmers abhängig sein.

Für ein gesetzliches Einwilligungserfordernis bei gesundheitlichen Untersuchungen bleibt jedoch wenig Raum. Auf Grund von Regelungen zur Arbeitssicherheit ist der Arbeitgeber zum Teil verpflichtet, vor Einstellung eine Untersuchung zu fordern. Die Teilnahme an der Untersuchung ist insofern notwendige Voraussetzung für die Einstellung. Daneben kann es weitere Fälle geben, in denen die gesundheitliche Tauglichkeit zwingende Voraussetzung für die Erfüllung der vorgesehenen arbeitsvertraglichen Verpflichtungen ist.

In beiden Fällen ist die Durchführung der Einstellungsuntersuchung Bestandteil des Bewerbungsverfahrens, mit der Folge, dass sie nicht von einer Einwilligung im Sinne von § 4a BDSG abhängig gemacht werden kann. Eine solche müsste nämlich freiwillig sein, was jedoch voraussetzen würde, dass das Bewerbungsverfahren auch ohne die notwendigen Untersuchungen weiter durchgeführt werden müsste.

Eine ähnliche Problematik stellt sich bei § 32a Abs. 4 BDSG-E, der die Durchführung von Eignungstests ebenfalls von der Einwilligung des Betroffenen abhängig macht. Auf welche Weise der Arbeitgeber die fachliche und persönliche Eignung eines Bewerbers ermittelt, ist zunächst seinem Ermessen überlassen. Insofern kann er die Entscheidung über die Einstellung auch von der Mitwirkung des Bewerbers an einem Assessment-Center abhängig machen. Auf eine förmliche Einwilligung kommt es insoweit nicht an, da es dem Bewerber freisteht, an dem Assessment-Center teilzunehmen oder nicht. Insofern bedarf es hinsichtlich der Eignungstests nur einer gesetzlichen Klarstellung, dass diese nach den Regeln der Fachkunde durchzuführen sind. Bestehen bleiben kann

auch die Regelung in § 32a Abs. 4 S. 5 BDSG-E, wonach bei Vorliegen beruflicher Schweigepflichten nur das Ergebnis des Eignungstests mitzuteilen ist.

Die Regelung des § 32a Abs. 5 BDSG-E gibt die bestehende Rechtslage wieder, wonach im Bewerbungsverfahren keine Auskunftspflicht im Hinblick auf das Vorliegen einer Schwerbehinderung besteht. Aus Gründen der Rechtsklarheit sollte jedoch ergänzend darauf hingewiesen werden, dass freiwillige Angaben des Bewerbers zur Inanspruchnahme seiner in SGB IX genannten Rechte verwendet werden dürfen.

§ 32a Abs. 8 BDSG-E regelt im Hinblick auf allgemein zugängliche Daten eine Ausnahme vom Grundsatz der Direkterhebung. Nach der Gesetzesbegründung sollen auch Datenerhebungen im Internet bei bestimmungsgemäßer Nutzung im Bewerbungsverfahren zulässig sein.

Diese Regelung ist nicht unproblematisch. Im Internet allgemein - insbesondere aber auch in sozialen Netzwerken - finden sich vielfach Informationen, die dem privaten Bereich zuzuordnen sind und grundsätzlich unter dem Gesichtspunkt der Erforderlichkeit für die Entscheidung über die Einstellung nicht verwertet werden dürften. Auf Grund der Signalwirkung im Hinblick auf einen zukunftsorientierten Beschäftigtendatenschutz scheint eine konkretere Regelung zur Datenerhebung im Internet geboten. Sinnvoll wären etwa Regelbeispiele für zulässige Nutzungen (z.B. Datenerhebungen in beruflichen Netzwerken).

§ 32a Abs. 9 BDSG-E regelt den Grundsatz der Verhältnismäßigkeit bei der Datenerhebung vor Begründung eines Beschäftigungsverhältnisses. Mit Blick auf die Bedeutung des Verhältnismäßigkeitsprinzips empfiehlt sich, diesen Grundsatz im Zusammenhang mit der Regelung zur Erforderlichkeit in § 32a Abs. 1 BDSG-E zu verankern.

Zu § 32b BDSG-E

§ 32b Abs. 2 BDSG-E regelt die Datenverarbeitung und -nutzung ohne vorherige Datenerhebung nach § 32a BDSG-E. Systematisch ist aber schwer abzugrenzen, wann eine solche Datenverarbeitung bzw. -nutzung ohne vorausgehende Erhebung vorliegt. Deshalb sollte der Gesetzgeber zum besseren Verständnis die Formulierung aus der Gesetzesbegründung aufgreifen, wo daran angeknüpft wird, dass der Arbeitgeber Beschäftigtendaten ohne Nachfrage vom Beschäftigten erhält bzw. ihm die Daten auf andere Weise zugetragen werden.

§ 32b Abs. 3 BDSG-E regelt, dass Bewerberdaten nicht gelöscht werden müssen, wenn der Beschäftigte in ihre weitere Speicherung eingewilligt hat. In der Praxis hat sich als interessengerecht herausgestellt, dass bei einem weiteren Interesse an einem Bewerber dieser über die weitere Speicherung seiner Daten informiert und ihm ggf. ein Widerspruchsrecht eingeräumt wird.

Die beabsichtigte Neuregelung fordert hingegen eine förmliche Einwilligung nach § 4a BDSG. Dies ist für die Unternehmen mit erheblichem Aufwand verbunden und wird auch vom Bewerber als bürokratischer Formalismus empfunden.

Überdies könnte die beabsichtigte Regelung dahingehend interpretiert werden, dass ohne Einwilligung Bewerberdaten nach Abschluss des Bewerbungsverfahrens unmittelbar zu löschen sind. Eine weitere Speicherung kann jedoch auch auf Grund unternehmenseigener Interessen gerechtfertigt sein (z.B. Speicherung von Bewerberdaten, so lange ggf. noch Ansprüche wegen AGG-Verstößen geltend gemacht werden können). Insoweit empfiehlt sich, die vorgesehene Regelung ersatzlos zu streichen.

Zu § 32c BDSG-E

§ 32c Abs. 1 Satz 3 BDSG-E nimmt Bezug auf § 32a Abs. 8 BDSG-E. Auf die diesbezüglichen Ausführungen wird verwiesen.

Zu § 32d BDSG-E

§ 32d Abs. 3 BDSG-E regelt die Verarbeitung und Nutzung von Beschäftigtendaten im Zusammenhang mit der Durchsetzung von Compliance-Anforderungen. In § 32e BDSG-E werden Compliance-Anforderungen im Zusammenhang mit Maßnahmen „ohne Kenntnis des Beschäftigten“ geregelt. Nach ihrem Wortlaut erfassen beide Regelungen sowohl präventive als auch repressive Maßnahmen („verhindern oder aufzudecken“). Wie § 32d Abs. 3 BDSG-E und § 32e BDSG-E genau von einander abzugrenzen sind, bleibt unklar.

Sinnvoll wäre es, eine einheitliche Regelung zu schaffen, die sich mit Datenerhebungen, -verarbeitungen und -nutzungen im Zusammenhang mit Compliance-Maßnahmen befasst. Dabei sollte zum einen klar zwischen präventiven und repressiven Maßnahmen differenziert werden. Deshalb sollte statt des Begriffes „Aufdeckung“ auch der Begriff „Aufklärung“ verwendet werden. Zum anderen müsste deutlicher werden, welche exakten Regelungen für die Informationsbeschaffung und welche für die anschließende Nutzung der erhobenen Daten gelten sollen.

§ 32d BDSG-E regelt die Datenverarbeitung und -nutzung im Beschäftigungsverhältnis. Es sollte eine gesetzliche Klarstellung dahingehend erfolgen, dass für die Datenverarbeitung und -nutzung außerhalb des Beschäftigungsverhältnisses § 28 BDSG weiter Anwendung findet. Entscheidend ist, dass die Interessenabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG mit Blick auf die Verwendung von Beschäftigtendaten außerhalb des Beschäftigtenverhältnisses durch die in den §§ 32 ff. BDSG enthaltenen Regelungen nicht abgeschnitten wird.

Zu § 32e BDSG-E

§ 32e Nr. 1 BDSG-E stellt darauf ab, dass ein Verdacht gegen einen Beschäftigten vorliegt, im Beschäftigungsverhältnis eine schwerwiegende Vertragsverletzung begangen zu haben. In der Praxis wird es aber vielfach so sein, dass sich der Verdacht der schwerwiegenden Vertragsverletzung nicht gegen einen einzelnen Beschäftigten, sondern gegen eine Gruppe von Beschäftigten richtet, von denen einzelne oder mehrere die Tat begangen haben können. Insoweit bedarf es einer entsprechenden Anpassung des Gesetzestextes, wonach der Verdachtsmoment auf Beschäftigte (Plural) abstellt. Eine entsprechende Vorbildregelung für den Verdacht hinsichtlich einer Beschäftigtengruppe enthält § 32f Abs. 2 BDSG-E.

Abzustellen ist nach § 32e Nr. 1 BDSG-E auf eine schwerwiegende Vertragsverletzung zu Lasten des Arbeitgebers, die diesen zu einer fristlosen Kündigung aus wichtigem Grund berechtigen würde. Als Voraussetzung für konkrete Maßnahmen zur Durchsetzung der Compliance birgt dies erhebliche Risiken. Die Hürden für eine fristlose Kündigung gem. § 626 BGB sind sehr hoch und in der Regel auch unwägbar. Im Vorfeld ist kaum sicher prognostizierbar, ob sich bestehende Verdachtsmomente bestätigen werden und die aufzudeckende Vertragsverletzung eine außerordentliche Kündigung rechtfertigen wird. Daher sollte allein auf den konkreten Verdacht einer schwerwiegenden Vertragsverletzung abgestellt werden.

Zu § 32f BDSG-E

§ 32f BDSG-E regelt die Beobachtung nicht öffentlich zugänglicher Betriebsstätten durch Videoüberwachung. Sinnvoll wäre, den Beschäftigtendatenschutz im Zusammenhang mit der Videoüberwachung in § 32f BDSG-E abschließend zu regeln, also auch öffentlich zugängliche Bereiche einzubeziehen.

Zu § 32g BDSG-E

Problematisch ist die Beschränkung der Datenerhebung nach § 32g Abs. 1 Satz 1 BDSG-E auf die „Arbeitszeit“. Eine Aussage für Pausen- und Ruhezeiten wird nicht getroffen. Die Übernachtung in Fahrerkabinen eines Nutzfahrzeugs würde beispielsweise problematisch, weil der Arbeitgeber die Ortung ggf. deaktivieren müsste. Der Arbeitgeber könnte in dieser Zeit das Fahrzeug nicht sichern.

Weiterhin erscheint die geforderte unverzügliche Löschung als zu eng, da die Ortungsdaten ggf. auch für Dokumentationen und Rechtsstreitigkeiten relevant sein können. Ein Verweis auf die entsprechende Erforderlichkeit wäre besser.

Zu § 32h BDSG-E

Lichtbilder sind nicht regelmäßig biometrische Verfahren im Sinne der Vorschrift. Insofern macht es Sinn, die Verwendung von Lichtbildern von Beschäftigten aus der Vorschrift des § 32h BDSG-E herauszulösen und allgemein zu regeln.

Zu § 32i BDSG-E

Die Regelungen über die Nutzung von Telekommunikationsdiensten differenzieren zwischen der Erhebung von Inhalten und Verkehrsdaten während der Kommunikation und der in Absatz 5 geregelten nachgelagerten Kontrolle.

Hinsichtlich der Kontrolle der Privatnutzung der Telekommunikation stellt § 32i Abs. 5 Satz 2 BDSG-E auf die strengen Voraussetzungen des § 32e BDSG-E ab. Hier sollte differenziert werden. Zur Ermittlung, ob eine übermäßige Privatnutzung der Telekommunikation vorliegt, sollte eine stichprobenartige Kontrolle der Verkehrsdaten auch bei erlaubter Privatnutzung zulässig sein und die Kontrolle nicht von den hohen Hürden des § 32e BDSG-E abhängig gemacht werden.

Zu den Bedenken gegen § 32e BDSG-E vgl. bereits oben.

Zu § 32j BDSG-E

§ 32j BDSG-E fordert bei Datenverlusten immer die Unterrichtung des Beschäftigten und zwar unabhängig davon, ob der Datenverlust zu einer Beeinträchtigung der Rechte oder schutzwürdigen Interessen führt. Ein Bedürfnis für eine solche Regelung ist nicht ersichtlich. Dem Schutzbedürfnis der Betroffenen wird durch § 42a BDSG hinreichend Rechnung getragen. § 32j BDSG-E sollte daher ersatzlos gestrichen werden.

Zu § 32I BDSG-E

§ 32I BDSG-E verbietet die Einwilligung als Erlaubnistatbestand für den Umgang mit Beschäftigtendaten, sofern dies nicht ausdrücklich vorgesehen ist. Die Regelung erkennt, dass auch im Arbeitsverhältnis Einwilligungen vielfach notwendige Rechtsgrundlage sind. Die im Gesetz in Bezug genommenen Erlaubnistatbestände fehlen für solche Beschäftigungsverhältnisse, die nur mit einer Einwilligung des Bewerbers bzw. Arbeitnehmers durchführbar sind (z.B. Einwilligung in ein Prüfrecht vor Ort bei Telearbeit; Einwilligung in die Sicherheitsüberprüfung).

Zudem kommt es insbesondere in Konzernen unternehmensübergreifend zur Arbeit in Matrixstrukturen. Weiterhin ist Bestandteil der Personalarbeit der Aufbau von konzernweit zugänglichen Datenbanken mit Kenntnissen und Fähigkeiten (Skills) von Mitarbeitern. In Ermangelung einer anderen Rechtsgrundlage erfolgt die hierfür notwendige Datenverarbeitung auf Grundlage einer Einwilligung, deren Freiwilligkeit unproblematisch ist. Deshalb sollte von einem generellen Verzicht auf die Einwilligung als Erlaubnistatbestand für die Arbeit mit Beschäftigtendaten abgesehen werden. Die Einholung einer Einwilligung könnte jedoch klarstellend an die Voraussetzung geknüpft werden, dass der Arbeitgeber an ihrer Abgabe ein berechtigtes Interesse hat.

Bonn, den 17.06.2010