BRUNO SCHIERBAUM

Datenschutz – technisch und organisatorisch

Die technisch-organisatorische Seite des Datenschutzes hat vor allem mit Datensicherheit zu tun und ist insoweit eher eine Aufgabe für die IKT-Spezialisten und vielleicht noch den betrieblichen Datenschutzbeauftragten, könnte man meinen – das aber wäre ein Irrtum!

Mit der Novellierung des Bundesdatenschutzgesetzes (BDSG) im Jahre 2001 sind die ehemals zehn Zielvorgaben (›10 Gebote‹) in der Anlage zu § 9 BDSG auf nunmehr acht reduziert worden (siehe info-Kasten auf Seite 16). Diese vom Unternehmen zu treffenden Maßnahmen dienen dem Schutz der Persönlichkeitsrechte und damit der technisch-organisatorischen Umsetzung des BDSG. Betriebs- und Personalräte haben bei der Umsetzung der Zielvorgaben ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG oder nach den entsprechenden Vorgaben in den Landespersonalvertretungsgesetzen. Denn – wie so oft in der Informations- und Kommunikationstechnik (IKT) – lassen sich Maßnahmen der Datensicherheit gleichzeitig auch für eine Leistungs- oder Verhaltenskontrolle der Beschäftigten nutzen.

Die rechtlichen Vorgaben

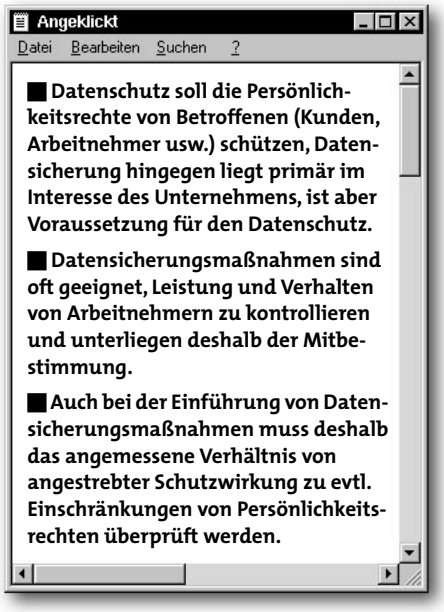
Nach § 9 BDSG haben nicht-öffentliche Stellen (also vor allem privatwirtschaftliche Unternehmen), soweit sie personenbezogene Daten erheben, verarbeiten oder nutzen, alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um allgemein die Anforderungen des BDSG zu erfüllen, vor allem aber die in der Anlage zu § 9 BDSG genannten ›Gebote‹. Einschränkend gilt, dass nur die technisch-organisatorischen Maßnahmen erforderlich sind, bei denen der dafür nötige Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht.

Datenschutz und Datensicherung

Im Zusammenhang mit dem § 9 BDSG tauchen die Begriffe ›Datenschutz‹ und ›Datensicherung‹ auf. Auch wird diese Vorschrift häufig als ›Datensicherungsvorschrift‹ bezeichnet. Diese Vermischung der doch recht unterschiedlichen Begriffe ist darauf zurückzuführen, dass natürlich bereits vor dem Inkrafttreten des ersten BDSG im Jahre 1977 die Unternehmen Datensicherungsmaßnahmen ergriffen haben, wie zum Beispiel den Schutz von Dateien, Datenträgern, Programmen und Datenverarbeitungsanlagen. Und in der Tat eignen sich viele Maßnahmen, die zur Datensicherung ergriffen werden auch, um den Datenschutzvorschriften genüge zu tun.

Aber dennoch gibt es bei den beiden Begriffen in Bezug auf die mit ihnen verbundenen Ziele grundsätzliche Unterschiede, die nicht verwischt werden sollten:

- Unter Datensicherung versteht man die Summe an Maßnahmen zur Sicherung des ordnungsgemäßen Ablaufs der Datenverarbeitung durch Sicherung der Hard- und Software vor Verlust, Beschädigung oder Missbrauch oder auch vor unbefugtem Zugriff auf Daten.
- Beim Datenschutz hingegen geht es in erster Linie um die Verhinderung unzulässiger Erhebung, Verarbeitung oder Nutzung personenbezogener Daten. Oder anderes ausgedrückt: Es geht beim Datenschutz um den Schutz der Persönlichkeitsrechte allgemein, insbesondere aber bei der automatisierten (also computergestützten) Datenverarbeitung.



Der Unterschied zwischen Datenschutz und Datensicherung ist am Besten an dem jeweiligen Schutzzweck zu erkennen: Datensicherung dient dem Interesse der datenverarbeitenden Stelle (des Unternehmens), Datenschutz hingegen dient unmittelbar dem Schutz des Betroffenen (des Beschäftigten oder auch des Kunden). Da das BDSG gemäß § 1 den Zweck hat, den einzelnen Betroffenen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, handelt es sich bei § 9 BDSG also nicht um eine Datensicherungsvorschrift, sondern um eine Vorschrift zum Datenschutz.

Das ändert sich auch nicht dadurch, dass Datensicherungsmaßnahmen im Einzelfall auch der Umsetzung des Datenschutzes dienen. Es erklärt aber, warum das BDSG nur Maßnahmen vorschreibt, die dem Schutz der Betroffenen (Arbeitnehmer, Kunden usw.) dienen.

Verhältnismäßigkeitsprinzip

Die in der Anlage zu § 9 BDSG vorgeschriebenen technischen und organisatorischen Maßnahmen, unterliegen – wie schon kurz erwähnt – ausdrücklich dem Verhältnismäßigkeitsprinzip. Das heißt: Sie sind nur dann und nur in dem Umfang ›erforderlich‹ (also von Gesetzes wegen vorgeschrieben), »wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.« Hierdurch wird klargestellt, dass nicht mit ›Kanonen auf Spatzen‹ geschossen werden soll.

Ein Missverständnis gilt es jedoch auszuschließen: Der Grundsatz der Verhältnismäßigkeit richtet sich *nicht* nach der Frage, ob die vom BDSG ausgesprochenen Zielvorgaben zu beachten sind – damit wäre ja die Verbindlichkeit des BDSG aufgehoben –, sondern es geht einzig und allein um Art und Umfang der Maßnahmen, die die Einhaltung der gesetzlichen Vorgaben sicher bewirken sollen. Und zwar so sicher, dass es zu Verletzungen der Datenschutzziele nicht kommen kann (auch nicht gegen den Willen der Verantwortlichen).

Die Begriffe ›technisch‹ und ›organisatorisch‹ sind dabei weit auszulegen:

So gehören zu den technischen Maßnahmen nicht nur die, die sich direkt auf Hard- und Software beziehen, sondern es gehört auch das gesamte bauliche Umfeld des Unternehmens mit dazu (z.B. die Schaffung speziell gesicherter Räume).

Und organisatorische Maßnahmen gehen in der Regel auch mit personellen Regelungen, Maßnahmen und Vorkehrungen einher (z.B. Zuordnung von Aufgaben, Befugnissen und Verantwortlichkeiten, Gestaltung der Arbeitsabläufe, Zugangs- und Zugriffsregelungen oder die Einrichtung stichprobenartiger Erfolgskontrollen).

Datenschutzkonzept

Wegen der unterschiedlichen Verhältnisse in den einzelnen Unternehmen ist es nicht möglich, ein allgemein gültiges und für alle Unternehmen zu übernehmendes Datenschutzkonzept zu entwickeln. Vielmehr liegt es in der Verantwortung jeder einzelnen verantwortlichen Stelle (Unternehmen, Institution) ein entsprechendes Datenschutzkonzept mit technischen und organisatorischen Datenschutzmaßnahmen zu erstellen (siehe: ›Datenschutzkonzept: Was hilft und was hilft nicht?‹ in CF 9/03 ab Seite 26).

Hier ist es die Aufgabe des betrieblichen Datenschutzbeauftragten, auf die Umsetzung der Zielvorgaben hinzuwirken. Zudem sind die technischen und organisatorischen Maßnahmen Bestandteil der nach § 4e BDSG notwendigen Übersichten (die z.B. Angaben zu den mit Datenerhebung und -nutzung verbundenen Zwecken oder zu Löschfristen und Datenübermittlungen enthalten müssen). Diese Übersichten hat das Unternehmen gemäß § 4g Abs. 2 BDSG dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen.

Mitbestimmung

Häufig sind technische und organisatorische Maßnahmen auch Bestandteil von Betriebsvereinbarungen. So wird zum Beispiel in Vereinbarungen auf den § 9 BDSG verwiesen oder es werden detaillierte Maßnahmen, wie Zugriffsberechtigungskonzepte oder der Umgang mit Protokollierungen, festgelegt.

Wie bereits erwähnt unterliegt die Umsetzung der technischen und organisatorischen Maßnahmen der Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG, da bereits Maßnahmen wie die Vergabe von Passwörtern oder auch die Protokollierung von Zugriffen Grundlage für Leistungs- und Verhaltenskontrollen sein können.

Dabei ist gemäß § 31 BDSG zu beachten, dass personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, auch wirklich nur für diese Zwecke verwendet werden dürfen.

Technisch-organisatorische Maßnahmen

Im BDSG werden acht Zielvorgaben genannt (siehe info-Kasten Seite 16), deren Umsetzung dem Unternehmen obliegt. Die Vorschrift selbst nennt keine konkreten Maßnahmen, da dies zum einen den Rahmen der Rechtsvorschrift sprengen würde und zum anderen die Vorgaben nach wenigen Jahren bereits veraltet wären.

(1) Zutrittskontrolle

Mit der Zutrittskontrolle soll Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten

info

Übersicht

Die ›acht Gebote‹ zum Datenschutz – Anlage zu § 9 BDSG

(1) Zutrittskontrolle	**Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.**
(2) Zugangskontrolle	**Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.**
(3) Zugriffskontrolle	**Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.**
(4) Weitergabekontrolle	**Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.**
(5) Eingabekontrolle	**Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.**
(6) Auftragskontrolle	**Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.**
(7) Verfügbarkeitskontrolle	**Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.**
(8) Getrennte Verarbeitung	**Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.**

verarbeitet und genutzt werden, verwehrt werden.

Zweck dieser Zutrittskontrolle ist es, zu verhindern, dass sich unbefugte Personen Datenverarbeitungsanlagen nähern, weil sonst das Risiko einer unbefugten Kenntnisnahme personenbezogener Daten oder gar der unbefugten Bedienung der Anlage bestünde. Mit Datenverarbeitungsanlagen ist jedes Gerät gemeint, mit dem Daten automatisiert verarbeitet werden können, insbesondere Großrechner, Server, Personal-Computer, Laptops ⮕, Chipkarten ⮕ aber auch die gesamte ›Peripherie‹ (wie Drucker, Datenspeicher usw.).

Ein solcher Schutz gestaltet sich im Fall eines Rechenzentrums als nicht besonders schwierig. Bei einzelnen Arbeitsplätzen irgendwo im Betrieb sieht das allerdings ganz anders aus. Das Risiko, dass Kunden, nicht zuständige Kollegen, Reinigungspersonal oder Hausmeister Zutritt zu einem Arbeitsplatzrechner bekommen, ist kaum auszuschalten. Hier kommt es deshalb vor allem darauf an, dass diese Unbefugten den Arbeitsplatzrechner nicht etwa in Betrieb nehmen und/oder nutzen können.

Beispiele für Maßnahmen:

- ›Closed-Shop‹-Betrieb (in sich abgeschlossener Betrieb),
- Einrichtung von Sicherheitszonen,
- Kontrolle durch Pförtner u.ä.,
- Schlüsselregelung,
- automatische Zugangskontrolle,
- Berechtigungsausweise,
- spezielle Regelung für Reinigung, Wartung und Reparatur.

Zugangskontrolle

Mit der Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Im Gegensatz zur Zutrittskontrolle ist hier nicht von Datenverarbeitungsanlagen die Rede, sondern von ›Datenverarbeitungssystemen‹. Im Blickpunkt stehen in diesem Fall nämlich nicht nur die Geräte (Hardware), sondern außerdem die Datenverarbeitungsprogramme (Software) und die Daten selber.

Mit ›Zugang‹ ist das Eindringen in solche Datenverarbeitungssysteme gemeint – über Tastatur und Maus, aus einem Netzwerk heraus oder auf irgendeinem anderen Weg. Es sollen alle Eingriffe, die die Funktionsfähigkeit des Datenverarbeitungssystems beeinträchtigen können(wie z.B. verändernde Eingriffe in Daten, Software oder Hardware), verhindert werden.

Beispiele für Maßnahmen:

- Festlegung und Kontrolle der Befugnisse,
- Zuordnen von Benutzern zu bestimmten Endgeräten,
- Vergabe von Passwörtern,
- Protokollierungen aller Zugänge/Zugriffe,
- automatisches Abschalten des Personal-Computers (›log-off‹).

Zugriffskontrolle

Mit der Zugriffskontrolle soll gewährleistet werden, dass die zur Benutzung des Systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

›Zugriffsberechtigung‹ ist die Befugnis eines Beschäftigten oder einer Gruppe von Beschäftigten, mit einer festgelegten Menge an Daten umzugehen. Diese Zugriffsberechtigungen der einzelnen Beschäftigten müssen dabei datenschutzgerecht festgelegt werden. Das heißt: Der einzelne Beschäftigte darf nur Zugriff auf die personenbezogenen Daten eingeräumt bekommen, die er für die Erfüllung seiner Arbeitsaufgabe benötigt. So werden beispielsweise für die Lohnbuchhaltung andere Daten benötigt als für die Personalplanung. Die jeweilige Zugriffsberechtigung wird sich also immer auf bestimmte Daten beziehen, wobei jeder Zugriff noch differenziert werden kann nach ›Lesen‹, ›Schreiben‹, ›Ändern‹ und so weiter.

Beispiele für Maßnahmen:

- Festlegung und Kontrolle der Zugriffsbefugnisse, differenziert nach Programmen, Daten und Zugriffsart,
- Identifikation der Zugreifenden (Passwort),
- Protokollierung aller Zugriffe,
- Verschlüsselung,
- Einschränkung der Abfragemöglichkeit,
- Begrenzung der Nutzung einzelner Programmfunktionen (funktionell/zeitlich),
- Archivierung für Sicherungskopien,
- Sperrung des Zugriffs nach Dienstschluss.

Weitergabekontrolle

In Ergänzung zur Zugriffskontrolle soll mit der Weitergabekontrolle durch technische und organisatorische Maßnahmen gewährleistet werden, dass sämtliche Aspekte der Weitergabe personenbezogener Daten durch Datenübertragung überprüfbar und nachvollziehbar sind und dass der Zugriff Unbefugter auf dem Transportweg verhindert wird.

Diese Forderung kann in geschlossenen Systemen mit geschlossenen Benutzergruppen auch relativ leicht erfüllt werden. Sobald Netze aber offen sind, sobald also über öffentliche Netze Zugang zu externen Rechnern möglich ist und damit auch eine Datenübertragung, stößt diese Forderung an Grenzen. Denn es zeichnet offene Systeme ja gerade aus, dass die Übermittlung an einen unbestimmten Kreis erfolgt oder bestimmt ist.

Beispiele für Maßnahmen:

- Festlegung, welche Daten zu welchen Zwecken an wen weitergeleitet werden sollen,
- Dokumentation der Abruf- und Übertragungsprogramme, der Übermittlungswege und der entsprechenden Übermittlungsgeräte,
- Führen einer Übersicht mit den Stellen, an die Daten weitergeleitet werden,
- Protokollierung der Abruf- und Übermittlungsaktivitäten.

Eingabekontrolle

Mit der ›Eingabekontrolle‹ soll gewährleistet werden, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert und entfernt worden sind.

Bei dieser Zielvorgabe geht es um die Nachprüfbarkeit des Verarbeitungsvorgangs. Zeitpunkt, Inhalt und Urheber von Datenspeicherung und -verarbeitung sollen zumindest im Nachhinein ermittelt und überprüft werden können.

Beispiele für Maßnahmen:

- Erstellung von Nutzerprofilen,
- automatisierte Protokollierungen der Dateneingabe, -änderung oder -löschung,
- automatisierte Protokollierung der System-/Netzverwalter-Aktivitäten,
- Sicherung der Protokolldaten gegen Verlust oder Veränderung,
- Freigabe und Dokumentation aktueller Programmversionen.

Auftragskontrolle

Die ›Auftragskontrolle‹ soll gewährleisten, dass personenbezogene Daten, die im Auftrag für andere verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Diese Zielvorgabe ist eine Ergänzung zu den detaillierten Vorgaben zur Auftragsdatenverarbeitung, die in § 11 BDSG geregelt ist (siehe: ›Datenschutz bei Auftragsdatenverarbeitung ...‹ in CF 6/05 ab Seite 4).

Beispiele für Maßnahmen:

- sorgfältige Auswahl des Auftragnehmers,
- differenzierte Aufgaben-/Auftragsbeschreibung,
- Verpflichtung des Auftragnehmerpersonals auf das Datengeheimnis,
- exakte Beschreibung und Prüfung der technischen und organisatorischen Maßnahmen des Auftragnehmers,
- gemeinsame Kontrolle von Auftragnehmer und Auftraggeber in Bezug auf den Datenschutz,
- vertragliche Regelung zur Auftragsdatenverarbeitung.

Verfügbarkeitskontrolle

Durch die neu ins BDSG aufgenommene ›Verfügbarkeitskontrolle‹ soll erreicht werden, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Dabei stellt die Verfügbarkeit von Daten ein Grundziel der informationstechnischen Sicherheit dar und meint die Gefahr, dass auf personenbezogene Daten nicht, nicht vollständig oder nicht rechtzeitig zugegriffen werden kann.

Beispiele für Maßnahmen:

- Erarbeitung eines Datensicherungskonzepts,
- Maßnahmen gegen Feuer-, Wasser- und Blitzschäden – dazu gehören Maßnahmen wie ...
  - in Hochwassergebieten Server-Räume [→] möglichst weit über der Wassergrenze,
  - feuerfeste Tresore für Sicherungskopien,
- Einrichtung einer unterbrechungsfreien Stromversorgung,
- Auslagerung von Servern zur Datensicherung,
- keine Verwendung von Originaldaten für Testzwecke.

Trennungsgebot

Durch das ›Trennungsgebot‹ soll gewährleistet werden, dass zu unterschiedlichen Zwecken erhobene Daten

nicht ohne Weiteres vermischt werden können. Erreicht werden soll, dass die verantwortliche Stelle (das Unternehmen) schon bei der Inbetriebnahme der Datenverarbeitung darauf achtet, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden. Im Arbeitsleben wird das Trennungsgebot insbesondere dann zur Anwendung kommen müssen, wenn die Beschäftigten gleichzeitig Kunden in ihrem Unternehmen sind, wie dies beispielsweise bei Banken und Versicherungen der Fall ist.

Beispiele für Maßnahmen:

- Trennung der Datensätze durch Speicherung in physikalisch getrennten Datenbanken,
- Verschlüsselung,
- Vergabe von Zugriffsberechtigungen,
- Festlegung von ›Rollen‹ (Beschäftigter, Kunde) in einem Informationssystem.

Bruno Schierbaum, BTQ Beratungsstelle für Technologiefolgen und Qualifizierung im Bildungswerk ver.di in Niedersachsen, Donnerschweer Straße 84, 26123 Oldenburg, fon 0441-82068, **schierbaum@btq.de**

Weiterführende Literatur:

Gola/Schomerus: Bundesdatenschutzgesetz, Kommentar, 8. Auflage, 2005

Rossnagel (Hrsg.): Handbuch Datenschutzrecht, 2003

Simitis (Hrsg.): Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, 2003

Koch (Hrsg.): Der betriebliche Datenschutzbeauftragte, 2003

Chipkarte = Plastikkarte mit integriertem Computerchip, der sowohl einen Datenspeicher wie auch Programmfunktionen enthalten und z.B. als Betriebsausweis dienen kann (auch → Seite 13)

Laptop (*lap* = Schoß) = Sammelbegriff für mobile (auf dem Schoß platzierte) Personal-Computer; der Begriff ist heute weitgehend abgelöst durch die Bezeichnung ›Notebook‹

Server (Zusteller) = spezieller Computer zur Verwaltung von Netzwerken mit verschiedenen Aufgaben (Netzsteuerung, zentrale Datenspeicherung, Softwarebereitstellung)

aus der praxis

datenschutztipps

für die praxis

In dieser Serie werden regelmäßig Informationen und Praxisfälle zum Datenschutz veröffentlicht, wie sie in den Berichten der Datenschutzbeauftragten und Aufsichtsbehörden der Länder und des Bundes zu finden sind ...

HAJO KÖPPEN

Personalgespräche und Mitarbeiterbefragungen

Zunehmend werden in Landesbehörden im Rahmen von Organisationsuntersuchungen und Umstrukturierungsmaßnahmen Mitarbeiterbefragungen und Personalgespräche durchgeführt, um über die in Personalakten vorhandene Informationen hinaus weitere Beschäftigtendaten als Grundlage etwa für anstehende Personalmaßnahmen zu beschaffen. Über einen solchen Fall berichtet der Sächsische Datenschutzbeauftragte in seinem 12. Tätigkeitsbericht:

1.

So führten auf Anordnung des zuständigen Staatsministeriums Mitarbeiter der Regionalschulämter mit angestellten Lehrkräften der Mittelschulen und Gymnasien Personalgespräche (Seite 47). Hintergrund der Gespräche war, dass die Regionalschulämter wegen der Haushaltslage und der zukünftig niedrigeren Schülerzahlen Änderungskündigungen aussprechen sollen. Bei den Gesprächen wurden keine Fragebögen verwendet, so dass den Mitarbeitern nichts Schriftliches vorlag. Neben Daten, die sich bereits in der Lehrerpersonaldatenbank oder in der Personalakte befanden, wurden auch weitergehende Informationen mit zum Teil sehr sensiblem Charakter abgefragt. Etwa zu bestehenden Unterhaltspflichten, zu einer Arbeitslosigkeit des Ehegatten, zu gesundheitlichen Beeinträchtigungen, zu Schulden und dem Vorliegen eines sozialen Härtefalles. Diese weitgehende Verarbeitung zusätzlicher Daten wurde damit begründet, den Betroffenen die Gelegenheit zu geben, für sie arbeitsrechtlich günstige Angaben zu machen.

Der Datenschutzbeauftragte findet an diesem Verfahren überhaupt kein Gefallen: »Das Resultat dieser für die Lehrer nicht transparenten Verfahrensweise war, dass im Übermaß und uneinheitlich Daten über persönliche Verhältnisse der Mitarbeiter verarbeitet worden waren.« Zwar ist eine Verarbeitung personenbezogener Daten zur Personalplanung und -verwaltung nach § 37 Sächsisches Datenschutzgesetz (SächsDSG) durchaus zulässig. So kann es für die sachgerechte Entscheidung über Teilkündigungen durchaus notwendig sein, bereits im Vorfeld zusätzliche Daten der Beschäftigten zu erheben.

Dem datenschutzrechtlichen Grundsatz der Erforderlichkeit entsprechend hält der Datenschutzbeauftragte aber ein abgestuftes Verfahren für zwingend notwendig. So ist der Kreis der zu befragenden Beschäftigten anhand eines zu erstellenden Kriterienkatalogs möglichst frühzeitig einzugrenzen: »Nachdem für Teilkündigungen (objektive) Bedarfskriterien wie Unterrichtsfächer und Ausbildung verarbeitet und ausgewertet worden sind, können bei Bedarf in