

Datenschutz

Beschäftigten-Datenschutz durch Vorabkontrolle

Dass es sich bei dem novellierten BDSG nicht um „den großen Wurf“ handelt, ist von Datenschützern oft beklagt worden.¹⁾ Es gibt jedoch einige Änderungen, die für die verantwortliche Stelle (dieses ist im öffentlichen Bereich die Behörde), den betrieblichen/behördlichen Datenschutzbeauftragten (nachfolgend bDSB) und auch für die Interessenvertretung von praktischer Bedeutung sind. Eine dieser Änderungen ist die in § 4 d BDSG verankerte Vorabkontrolle, die es in ähnlicher Form vor der Novellierung des Datenschutzrechts in einigen Landesdatenschutzgesetzen, wie z.B. dem Niedersächsischen Datenschutzgesetz, bereits gab. Die Vorabkontrolle kann dem Personalrat wichtige Anhaltspunkte bei der Umsetzung seiner Mitbestimmungsrechte geben, die er nach den Personalvertretungsgesetzen beim Datenschutzrecht hat.

Die Vorgabe des Art. 20 EG-Datenschutzrichtlinie²⁾ zur Vorabkontrolle machte die Verankerung im BDSG und auch in allen Landesdatenschutzgesetzen erforderlich. Die Vorabkontrolle stellt eine zusätzliche Maßnahme zur Prüfung der rechtmäßigen Datenverarbeitung dar und ist als Ergänzung zur Zulässigkeitsprüfung der Datenverarbeitung (§ 4 i.V.m. § 28 BDSG) und zu den umzusetzenden technischen und organisatorischen Maßnahmen (§ 9 BDSG) zu sehen. Die Vorabkontrolle ist vom bDSB vor Inbetriebnahme bestimmter Datenverarbeitungen durchzuführen. Die Ergebnisse einer Vorabkontrolle enthalten in jedem Fall **wichtige Informationen für die Interessenvertretung**, die bei der Umsetzung der weiteren Beteiligungsrechte nach dem Personalvertretungsrecht nützlich sein können. Gerade deswegen sollte die Interessenvertretung die Vorgaben zur Vorabkontrolle kennen.

Rechtliche Vorgabe

Die Vorabkontrolle ist vom Gesetzgeber in § 4 d Abs. 5 und 6 BDSG in dem Paragraphen, der mit „Meldepflicht“ über-

schrieben ist, verankert worden. Eine Vorabkontrolle ist vor Beginn der Datenverarbeitung durchzuführen, **soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen**.

Eine Vorabkontrolle ist insbesondere – das heißt in jedem Fall – dann durchzuführen, wenn

- besondere Arten von personenbezogenen Daten verarbeitet werden oder
- die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeit, seiner Leistung oder seines Verhaltens.

Das BDSG sieht Ausnahmen von der Vorabkontrolle vor. Sie muss nicht durchgeführt werden, wenn

- eine gesetzliche Verpflichtung oder
- eine Einwilligung des Betroffenen vorliegt oder
- der Zweckbestimmung eines Vertragsverhältnisses oder
- vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Zuständigkeit und Zeitpunkt

Zuständig für die Vorabkontrolle ist der bDSB (§ 4 d Abs. 6 BDSG).³⁾ Ein bDSB⁴⁾ ist schriftlich zu bestellen, wenn die verantwortliche Stelle (Behörde) personenbezogene Daten automatisiert erhebt, verarbeitet oder nutzt. Eine Bestellung muss auch erfolgen, wenn personenbezogene Daten auf andere Weise – dieses bedeutet manuelle Datenverarbeitung – erhoben, verarbeitet oder genutzt werden und damit in der Regel zwanzig Personen beschäftigt sind. Durch diese gesetzliche Regelung wird der bDSB als obligatorische Institution für den öffentlichen Bereich eingeführt.

Bevor der bDSB die Vorabkontrolle durchführen bzw. überhaupt prüfen kann, ob eine Vorabkontrolle durchgeführt werden muss, ist er von der verantwortlichen Stelle zu unterrichten. Ihm müssen gemäß § 4 d Abs. 6 BDSG folgende Übersichten zur Verfügung gestellt werden:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- Anschrift der verantwortlichen Stelle,
- Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung,
- eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Datenkategorien,
- Empfänger und Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
- Regelfristen für die Löschung von Daten,
- eine geplante Datenübermittlung in Drittstaaten,
- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die vorgesehenen technischen und/oder organisatorischen Maßnahmen zum Datenschutz (§ 9 BDSG) zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind,
- die zugriffsberechtigten Personen.

Da es zur Durchführung der Vorabkontrolle diese Informationen (Übersichten) bereits **vor der Einführung bzw. Anwendung einer Datenverarbeitung** – also in der Planungsphase – geben muss, müssen diese Informationen nicht nur dem

1) Dieses gilt in gleicher Weise für die Datenschutzgesetze der Länder. Denn letztlich sind bei der Novellierung der Datenschutzgesetze nur die durch die EG-Datenschutz-Richtlinie zwingend erforderlichen Veränderungen vorgenommen worden.

2) Vgl. zur EG-Datenschutzrichtlinie: Dammann/Simitis, EG-Datenschutzrichtlinie, Kommentar, 1997; Schierbaum, Nichtumsetzung der EG-Datenschutzrichtlinie, PersR 1998, S. 502 ff.

3) Die Aufgaben des bDSB sind in § 4 g BDSG aufgelistet. Sinnvollerweise hätte der Gesetzgeber der besseren Übersicht wegen an dieser Stelle die Vorabkontrolle als Aufgabe des bDSB mit aufnehmen sollen.

4) Vgl. zum behördlichen Datenschutzbeauftragten ausführlich: Schierbaum, Behördlicher Datenschutzbeauftragter – doppelter Kontrollauftrag bei der Verarbeitung von Beschäftigtendaten, PersR 2001, S. 454 ff.

bDSB, sondern auch der Interessenvertretung zur Verfügung gestellt werden.

In Bezug auf den Zeitpunkt der Informationen ist die im BDSG festgelegte „Rechtzeitigkeit“ zu beachten. Dieses ergibt sich aus § 4 g Abs. 1 Nr. 1 BDSG, wo festgelegt ist, dass der bDSB bei der Aufgabe der Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme rechtzeitig zu unterrichten ist. Die Unterrichtung ist dann als rechtzeitig anzusehen, wenn sie vor dem Einsatz der automatisierten Datenverarbeitung erfolgt und das zu einem Zeitpunkt, zu dem der bDSB die Vorabkontrolle noch durchführen kann und eine entsprechende Stellungnahme für die Leitung der verantwortlichen Stelle (Dienststelle/Behörde) abgeben kann.⁵⁾

Erst die Informationen versetzen den bDSB in die Lage, sich einen Überblick über den geplanten Soll-Zustand zu verschaffen. Im Rahmen seiner Weisungsfreiheit⁶⁾ ist der bDSB befugt, selbst zu entscheiden, ob im Einzelfall eine Vorabkontrolle durchzuführen ist. In Zweifelsfällen hat er sich an den Bundesbeauftragten für den Datenschutz (BfD) zu wenden. Dabei ist es interessant, dass er sich von der gesetzlichen Vorgabe her nicht erst an den Arbeitgeber, sondern gleich an den BfD wenden soll. Der BfD übernimmt hier eine Beratungsfunktion. Das Ergebnis einer Vorabkontrolle ist zu Dokumentationszwecken immer schriftlich festzuhalten, da nur so eine Kontrollierbarkeit und Überprüfung durch die Aufsichtsbehörde bzw. den BfD möglich ist.⁷⁾

Auch wenn es zu den Aufgaben des bDSB gehört, die Vorabkontrolle durchzuführen, obliegt die Verantwortung für die Umsetzung des Datenschutzes und damit auch für die Umsetzung der Vorabkontrolle der Leitung der verantwortlichen Stelle. Diese Verantwortung ist im neuen BDSG dahingehend untermauert worden, indem festgelegt wurde, dass der bDSB auf die Einhaltung des BDSG „hinwirkt“. Wird eine Vorabkontrolle durchgeführt und der bDSB kommt zu dem Ergebnis, dass bestimmte technische und organisatorische Maßnahmen zu treffen sind oder auch dass bestimmte Datenverarbeitung und Speicherung bestimmter Daten zu unterbleiben hat, sind die entsprechenden Vorgaben von der verantwortlichen Stelle umzusetzen. Ein Verstoß gegen die Vorschläge des bDSB muss immer auch als Verstoß gegen das Datenschutzrecht gewertet werden.

Wie die Vorabkontrolle durchzuführen ist, bleibt dem bDSB im Rahmen seiner Weisungsfreiheit selbst überlassen. Anhaltspunkte geben hier z.B. die Vorschläge der Landesbeauftragten für den Datenschutz in Niedersachsen, Hessen und Nordrhein-Westfalen,⁸⁾ auf die weiter unten eingegangen wird.

Vorabkontrolle bei besonderen Risiken

Die Festlegung, bei welchen Datenverarbeitungen eine Vorabkontrolle durchzuführen ist, hat die EG-Datenschutzrichtlinie den nationalen Gesetzgebern überlassen. Einen gewissen Anhaltspunkt kann der Erwägungsgrund 53 der Datenschutzrichtlinie geben. Danach sollen der Vorabkontrolle bestimmte Formen der Datenverarbeitung unterliegen. Es soll sich dabei um die Verarbeitungen handeln, die aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung – wie zum Beispiel der Zweckbestimmung, die betroffenen Personen von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrages auszuschließen – oder die aufgrund der Verwendung einer neuen Technik besondere Risiken im Hinblick auf die Rechte und Freiheiten der betroffenen Personen aufweisen.

Der deutsche Gesetzgeber sieht eine Vorabkontrolle dann vor, wenn die automatisierte Verarbeitung „**besondere Risiken für die Rechte und Freiheiten der Betroffenen**“ aufweisen. Das heißt, dass grundsätzlich bei jeder automatisierten Verarbeitung die Prüfung angezeigt ist, ob damit besondere Risiken einhergehen. Da die Bandbreite der Interpretation der Begriffe „besondere Risiken für die Rechte und Freiheiten der Betroffenen“ kaum einzugrenzen ist, steht dem bDSB hier zwangsläufig ein Beurteilungsspielraum zu.

Um Anhaltspunkte für die Praxis zu geben, sind risikobehaftete Verarbeitungen – wie oben dargestellt – diejenigen, die die betroffene Person von der Inanspruchnahme eines Rechts, einer Leistung oder eines Vertrages ausschließen. Hier sind zum Beispiel die Nutzung von Warndateien der Versicherungswirtschaft sowie von Handels- und Kreditauskunfteien zu nennen. Die Verfahren, nicht-kreditwürdige Personen durch so genannte Scoring-Verfahren „herauszufiltern“, sind als typische Anwendungsfälle für Vorabkontrollen anzusehen. Der Bundesbe-

auftragte für den Datenschutz sieht in der Vorabkontrolle einen ersten Schritt gegen einen unverhältnismäßigen Einsatz von Videoüberwachung durch öffentliche Stellen und private Stellen.⁹⁾ Videoüberwachung, die mit gespeicherten Bilddaten Profilabgleiche durchführt, birgt als neue Technologie zusätzliche Risiken für das Persönlichkeitsrecht in sich.¹⁰⁾ Für den Bereich des Arbeitnehmer-Datenschutzes werden u.a. die Speicherung und Nutzung von Qualifikations-Datenbanken oder von Persönlichkeitsprofilen und den damit einhergehenden Profilabgleichen oder der weiteren Auswertungsmöglichkeiten der Vorabkontrolle unterliegen müssen.

Vorabkontrolle bei besonderen Datenarten

Bei den in § 4 d Abs. 5 Nr. 1 und 2 BDSG genannten Fällen, in denen eine Vorabkontrolle durchzuführen ist, handelt es sich **nicht um eine abschließende Aufzählung**, sondern um Fälle/Beispiele, in denen **in jedem Fall** eine Vorabkontrolle durchzuführen ist. Als erstes der Beispiele dafür, wann eine Vorabkontrolle durchzuführen ist, wird die Verarbeitung besonderer Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) angeführt. Besondere Arten personenbezogener Daten sind Angaben über

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit oder Sexualleben.

Vorabkontrolle bei Bewertung der Persönlichkeit

Als zweites Beispiel dafür, wann ebenfalls eine Vorabkontrolle durchzuführen ist,

5) Vgl. Klug, Die Vorabkontrolle – Eine neue Aufgabe für betriebliche und behördliche Datenschutzbeauftragte, Recht der Datenverarbeitung 2001, S. 14.

6) Die Weisungsfreiheit des bDSB ist in § 4 f Abs. 3 BDSG geregelt: Der bDSB „ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei“.

7) Vgl. Schild, Meldepflichten und Vorabkontrolle, Datenschutz und Datensicherheit 2001, S. 286.

8) Diese Vorschläge sind über das Internet abzurufen: www.lfd.niedersachsen.de, www.datenschutz.hessen.de bzw. www.nordrhein-westfalen.datenschutz.de

9) Vgl. Jabobs, Perspektiven des neuen Datenschutzrechts, Datenschutz und Datensicherheit 2000, S. 7.

10) Vgl. hierzu: Schierbaum, Videoüberwachung und Datenschutz, PersR 2003, S. 439 ff.

wird die Verarbeitung personenbezogener Daten genannt, die dazu bestimmt sind, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens. Das heißt u.a., immer wenn die Datenverarbeitung eine Leistungs- und Verhaltenskontrolle ermöglicht, greift die Vorabkontrolle. Bei den Begriffen Leistungs- und Verhaltenskontrolle kann für die Konkretisierung auf den § 75 Abs. 3 Nr. 17 BPersVG¹¹⁾ und die einschlägigen Kommentierungen zurückgegriffen werden. Die Möglichkeit einer Leistungs- oder Verhaltenskontrolle ist immer beim Einsatz technischer Systeme wie z.B. Personalinformationssysteme, Personaldatenbanken, Telekommunikationsanlagen, bei Videoüberwachung, Zeiterfassungs- und Zugangskontrollsystemen oder bei der Nutzung von E-Mail und Internet gegeben.

Ausnahmen von der Vorabkontrolle

Eine Vorabkontrolle kann nach § 4 d Abs. 5 BDSG entfallen, wenn

- eine gesetzliche Verpflichtung oder
- eine Einwilligung des Betroffenen vorliegt oder
- die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen unterliegt.

Durch diese Ausnahmen soll laut Gesetzesbegründung eine sachgerechte Eingrenzung der Fälle einer Vorabkontrolle erreicht werden. Liegt eine klare und eindeutige **gesetzliche Regelung vor**, die die Verarbeitung personenbezogener Daten **anordnet**, ist eine Verletzung des allgemeinen Persönlichkeitsrechts auszuschließen. Diese Ausnahme ist akzeptabel. Es genügt jedoch nicht, dass ein Gesetz die Datenverarbeitung erlaubt oder voraussetzt.¹²⁾

Dass bei einer **Einwilligung** durch den Betroffenen eine Vorabkontrolle nicht durchgeführt werden muss, muss aus unterschiedlichen Gründen hingegen als problematisch angesehen werden. Zum einen bleibt der einwilligenden Person im Verhältnis zu Behörden, Unternehmen oder Arbeitgebern häufig gar keine andere Wahl als eine gewünschte Einwilligung zu geben und zum anderen kann durchaus eine Einwilligung für unrechtmäßige Datenverarbei-

tung abgefordert werden, was vom Einwilligenden in der Regel nicht erkannt werden kann. Schild¹³⁾ liefert hierfür ein Beispiel vom Klinikum „Rechts der Isar“: „Was nützt z.B. eine Einwilligung, wenn das dafür angewandte automatisierte Verfahren so gestaltet ist, dass die verarbeitenden Blutwerte nicht nur vom behandelnden Arzt, sondern aller Welt über das Internet zur Verfügung stehen.“

Zudem ist eine Vorabkontrolle vor Einführung der Datenverarbeitungsanlage erforderlich, wohingegen eine Einwilligung des Betroffenen, von dem Daten in der Datenverarbeitungsanlage gespeichert werden sollen, zeitlich später erfolgen wird. So kann man vor der Einführung des technischen Systems nur vom **Wunsch** einer Einwilligung ausgehen. Liegt in einem Fall nach Einführung eines entsprechenden technischen Systems dann keine Einwilligung vor, wäre das datenverarbeitende Verfahren möglicherweise unrechtmäßig, da keine Vorabkontrolle stattgefunden hat. So ist die Aufnahme der Ausnahmeregelung „Einwilligung“ in Bezug auf die Vorabkontrolle insgesamt als wenig durchdacht und damit als praxisfern anzusehen.

Zudem soll es sich um eine nicht risikobehaftete Datenverarbeitung handeln, wenn diese „der **Zweckbestimmung eines Vertragsverhältnisses** oder eines vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient“. Vertragsverhältnisse sind alle Arten von Verträgen, wie z.B. Arbeits- und Dienstverträge, Kauf-, Leih-, Werkverträge oder Dienstleistungs- und Mietverträge. Vertragsähnliche Vertrauensverhältnisse können während der konkreten Anbahnung eines Vertrages im Rahmen von Vorverhandlungen bestehen. So besteht während der Bewerbung um einen Arbeitsplatz und auch nach Beendigung eines Arbeitsverhältnisses ein vertragsähnliches Vertrauensverhältnis. Da die betriebliche Praxis zeigt, dass in der Regel sowohl in der Bewerbungsphase um einen Arbeitsplatz als auch bei der konkreten Datenverarbeitung nach Abschluss eines Arbeitsvertrages Datenerhebung, -verarbeitung und -nutzung geplant ist bzw. auch durchgeführt wird, die **über die Zweckbestimmung des Arbeitsvertragsverhältnisses hinausgeht**, dürfte die verankerte Ausnahme für den Arbeitsbereich nicht greifen. So wird bei jeder technischen Kontrolleinrichtung im Arbeitsleben eine Vorabkontrolle durchgeführt werden müssen.

Regelungen in den Landesdatenschutzgesetzen

Eine Vorabkontrolle ist in den novellierten Landesdatenschutzgesetzen aufgenommen worden.¹⁴⁾ Die Regelungen weichen jedoch in einigen Punkten von denen im BDSG ab. So ist nicht in jedem Fall der behördliche Datenschutzbeauftragte für die Vorabkontrolle zuständig. Die Verankerung des behördlichen Datenschutzbeauftragten in den Landesdatenschutzgesetzen ist, soweit die Gesetze novelliert worden sind, erfolgt und wird bei den noch zu novellierenden Datenschutzgesetzen erfolgen müssen. Wie die Datenschutzgesetze von Hessen (HDSG), Brandenburg (BbgDSG) Schleswig-Holstein (LDSG-SH) und Baden-Württemberg (LDSG-BaWü) weist auch das Niedersächsische Datenschutzgesetz (NDSG) dem bDSB eine Prüftätigkeit bei der Vorabkontrolle zu. Soweit allerdings im Geltungsbereich des LDSG-BaWü ein bDSB nicht zu bestellen ist, ist der Landesbeauftragte für den Datenschutz für die Vorabkontrolle zuständig. In Schleswig-Holstein ist bei einer Nichtbestellung eines bDSB dem Unabhängigen Landeszentrum für den Datenschutz Gelegenheit zur Vorabkontrolle zu geben. Gemäß den Datenschutzgesetzen in Hessen, Brandenburg, Nordrhein-Westfalen und Baden-Württemberg obliegt die Vorabkontrolle zunächst der verantwortlichen Stelle und innerhalb dieser demjenigen, der für den Einsatz eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist. Das Ergebnis der Vorabkontrolle ist aufzuzeichnen und nachfolgend dem bDSB zuzuleiten. Nach dem Bayerischen Datenschutzgesetz hat der bDSB die Aufgabe, die Freigabe von Datenverarbeitungen zu erteilen. Nur wenn den Einwendungen des bDSB nicht Rechnung getragen wird, legen sie die Entscheidung über

11) Nach § 75 Abs. 3 Nr. 17 BPersVG unterliegen die Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, der Mitbestimmung des Personalrats.

12) Vgl. Simitis (Hg.), Kommentar zum Bundesdatenschutzgesetz, 5. Aufl., § 4 d Rn. 26.

13) Vgl. Schild, (Fn. 7) S. 285 f.

14) Die nachfolgenden Ausführungen stützen sich auf die Abhandlung von Klug, Die Vorabkontrolle – Eine Aufgabe für betriebliche und behördliche Datenschutzbeauftragte, RDV 2001, S. 18 f.

die datenschutzrechtliche Freigabe der Leitung der öffentlichen Stelle vor.

Nach dem hessischen, nordrhein-westfälischen und niedersächsischen Datenschutzgesetzen ist die Vorabkontrolle nicht nur bei bestimmten vorher festgelegten, sondern bei allen Verfahren zur automatisierten Datenverarbeitungen durchzuführen. Dabei dürfen Datenverarbeitungen nur zum Einsatz kommen, wenn über technische und organisatorische Maßnahmen der Schutz der Persönlichkeitsrechte gewährleistet ist.

Umsetzung der Vorabkontrolle

Als Beispiel für die Umsetzung der Vorabkontrolle soll die Checkliste des Hessischen Datenschutzbeauftragten in ganz leicht veränderter Form dargestellt werden. Sind verschiedene Verfahren geplant, sollte die Vorabkontrolle für alle Alternativen durchgeführt werden. Danach ist folgender Ablauf zu durchlaufen:

1. Grundangaben

- zur verantwortlichen Stelle
- zur Zweckbestimmung
- zur Rechtsgrundlage
- zur Art der gespeicherten Daten
- zur Schutzbedürftigkeit der Daten, insbesondere bei sensiblen Daten
- zum Kreis der Betroffenen
- zur Übermittlung
- zu den zugriffsberechtigten Personengruppen
- zu den Fristen für die Löschung

2. Prüfung, ob

- die Art der gespeicherten Daten
- die Übermittlungen
- die Eingrenzung der Zugriffsberechtigten
- die Lösungsfristen

von der angegebenen Zweckbestimmung und Rechtsgrundlage gedeckt sind, insbesondere auch unter Berücksichtigung des Grundsatzes der Datenvermeidung und Datensparsamkeit. Ist dies nicht der Fall, muss geprüft werden, ob Änderungen im Verfahren möglich sind, die zu einem positiven Ausgang der Prüfung führen. Ist dies nicht möglich, ist das Verfahren auszuschließen.

3. Prüfungen, ob die Rechte der Betroffenen gewährt sind.

- Können die erforderlichen Auskünfte, Berichtigungen, Sperrungen und Löschungen durchgeführt werden?

- Ist sichergestellt, dass der Betroffene seine Rechte ohne unverhältnismäßigen Aufwand geltend gemacht werden kann?

Auch hier ist im Negativfall die Nachbesserungsmöglichkeit zu prüfen und wenn auch diese mit negativem Ergebnis endet, ist die Alternative auszuschließen.

4. Risikofaktoren für einen Missbrauch der Daten sind zu ermitteln.

- die Vertraulichkeit
- die Integrität
- die Verfügbarkeit

der Daten. Dazu gehören z.B. die Gefahr, dass Datenträger oder „Computerlisten“ während des Transports gestohlen werden, Virenbefall, Gefahr von unbefugten Zugriffen. Ggf. sind Personengruppen, die für missbräuchliche Verwendung in Frage kommen, zu benennen.

5. Beurteilung der möglichen Folgen bei missbräuchlicher Verwendung der Daten, z.B.

- Gefahren oder Nachteile für die Betroffenen
- Schadensersatzansprüche
- finanzielle Schäden
- „Vertrauensschaden“

6. Angaben zur Technik

- Einzelplatz
- bei vernetzten Rechnern auch Angaben zur Netzstruktur und Datenhaltung
- eingesetzte Software
- sowie zu den technischen und organisatorischen Maßnahmen

7. Abgleich der Risikofaktoren

unter besonderer Berücksichtigung der Schutzbedürftigkeit der personenbezogenen Daten mit den getroffenen Sicherheitsmaßnahmen und Entscheidung, ob das Restrisiko unter Anwendung des Verhältnismäßigkeitsgrundsatzes tragbar ist. Ist das Restrisiko zu hoch, ist zu überprüfen, ob eine Nachbesserung der Technik des Verfahrens oder der technischen und organisatorischen Maßnahmen eine positive Bewertung ergibt. Ist dies nicht der Fall, ist die Alternative auszuschließen. Bei vertretbarem Restrisiko endet die Vorabkontrolle dieser Alternative mit positivem Ergebnis.

Schriftlich ist festzuhalten, welche Alternativen geprüft wurden, die Risikoabwägung und die Gründe für die Auswahl der Alternative. Das Ergebnis der Vorabkontrolle und die Begründung sind dem behördlichen Datenschutzbeauftragten zur

Prüfung vorzulegen (dieses trifft nach dem BDSG so nicht zu, denn der BDSB hat die Vorabkontrolle durchzuführen).

Datenschutz durch Mitbestimmung

Bei allen wichtigen Vorgaben des BDSG sollte die Interessenvertretung im Auge behalten, dass sie in Bezug auf den Beschäftigten-Datenschutz über die Beteiligungsrechte nach dem BPersVG nachhaltig Einfluss nehmen kann auf den Umfang der Erhebung, Verarbeitung und Nutzung von Daten, auf Auswertungen und deren Verteiler sowie auf zugriffsberechtigte Personen und Lösungsfristen. Hierzu stehen dem Personalrat Informations-, Überwachungs- und Mitbestimmungsrechte zur Verfügung.

Das **Informationsrecht** ist die Basis für die weitere Beteiligung des Personalrats. So ist der Personalrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten (§ 68 Abs. 2 BPersVG). Rechtzeitig ist die Unterrichtung dann, wenn den einzelnen Personalratsmitgliedern ausreichend Zeit zur Verfügung steht, sich mit den Einzelheiten der beabsichtigten Maßnahme noch vor der Beratung und Beschlussfassung des Personalrats vertraut zu machen. Zudem muss die Maßnahme – z.B. die Einführung von Datenverarbeitungssystemen – noch gestaltungsfähig sein.

Das Bundesverwaltungsgericht hat in seinem Beschluss vom 8. 11. 1989¹⁵⁾ die Informationen deutlich dargestellt, die dem Personalrat bei der Einführung von EDV-Systemen zur Verfügung gestellt werden müssen. Folgende Informationen sind vom Arbeitgeber zur Verfügung zu stellen:

- Hardwarebeschreibungen (das technische System)
- Softwarebeschreibungen
- Verknüpfungsmöglichkeiten mit anderen Systemen (Schnittstellen)
- gespeicherte personenbezogene Daten der Beschäftigten
- Auswertungsmöglichkeiten
- angemessenes Datenschutzkonzept

Mit der Novellierung des BDSG gehören zu den Informationen auch die **Ergebnisse einer Vorabkontrolle**. Fristen zur Stellungnahme des Personalrats bzw. in

¹⁵⁾ Vgl. BVerwG, Beschluss v. 8. 11. 1989 – 6 P 7.87 –, PersR 1990, 102.

Bezug auf die Mitbestimmungsrechte laufen erst dann, wenn der Personalrat abschließend informiert worden ist. Darauf sollte der Personalrat den Arbeitgeber schriftlich hinweisen.

Nach § 68 Abs. 1 Nr. 2 BPersVG hat der Personalrat **darüber zu wachen**, dass die zu Gunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsvorschriften durchgeführt werden. Ein Gesetz in diesem Sinne ist auch das BDSG. So kann sich die Überwachung des Personalrats auch auf die Aufgabenerfüllung des bDSB und damit auch auf das Durchführen einer **Vorabkontrolle** beziehen.

Das **Mitbestimmungsrecht** nach § 75 Abs. 3 Nr. 17 BPersVG kommt zum Tragen bei Einführung und Anwendung von tech-

nischen Einrichtungen, die dazu bestimmt sind, Leistung oder Verhalten der Beschäftigten zu überwachen. Das Mitbestimmungsrecht kommt immer dann zur Anwendung, wenn die technische Einrichtung objektiv geeignet ist zur Leistungs- oder Verhaltenskontrolle. Im Rahmen der Umsetzung des Mitbestimmungsrechts können auch hier die Ergebnisse einer Vorabkontrolle dem Personalrat die Arbeit – z.B. bei der Entwicklung einer Dienstvereinbarung – erheblich erleichtern.

Fazit

Mit der vom Datenschutzrecht vorgegebenen Vorabkontrolle betreten die meisten verantwortlichen Stellen Neuland. So zwingt die Vorgabe zur rechtzeitigen Information

des bDSB. Die Vorabkontrolle kann einen erheblichen Arbeitsaufwand bedeuten, wobei dem bDSB ein Beurteilungsspielraum zusteht, wann automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Für die Interessenvertretung enthält die Vorabkontrolle wichtige Einschätzungen zur Umsetzung des Datenschutzrechtes, die bei der Umsetzung der Beteiligungs- und Mitbestimmungsrechte sehr hilfreich sein können. Zusätzlich kann die Interessenvertretung sich von der sachkundigen Person des bDSB u.a. über die Vorabkontrolle informieren lassen.

Bruno Schierbaum
BTQ Niedersachsen
Donnerschweer Str. 84
26123 Oldenburg
E-Mail: schierbaum@btq.de