Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung

Handlungsempfehlungen

Die Handlungsempfehlungen „Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung“ sind im Rahmen des Projektes eGovernment von einer Arbeitsgruppe des Arbeitskreises Personalwesen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet worden.

Die Federführung der Arbeitsgruppe lag beim Landesbeauftragten für den Datenschutz Niedersachsen; weitere Mitglieder der Arbeitsgruppe waren Mitarbeiterinnen und Mitarbeiter des Sächsischen Datenschutzbeauftragten, des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein sowie des Bundesbeauftragten für den Datenschutz.

Der Text der Orientierungshilfe ist von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Sitzung am 16./17. März 2006 in Magdeburg zustimmend zur Kenntnis genommen worden.

I. Allgemeines

Im Zuge der Modernisierung und Steigerung der Effizienz der öffentlichen Verwaltungen wird beim Bund und in den Ländern derzeit eine Vielzahl automatisierter Personalinformationssysteme/Personalmanagementverfahren und automatisierter Verfahren zur betriebswirtschaftlichen Steuerung der Haushaltswirtschaft eingesetzt. Die Verfahren werden vielfach über Schnittstellen mit anderen Systemen der Personaldatenverarbeitung, so etwa mit Bezügeverfahren, Reisekostenverfahren und Systemen zur automatisierten Arbeitszeiterfassung verknüpft.

Automatisierte Personalinformationssysteme und Personalmanagementverfahren haben zum Ziel, die in einer Organisation an vielen Stellen vorhandenen personenbezogenen Informationen über die einzelnen Mitarbeiterinnen und Mitarbeiter in einer zentralen Datenbank zu erfassen, zu pflegen und für die einzelnen Verfahren der Personalbearbeitung per Abruf zur Verfügung zu stellen. Durch die zentrale Erfassung, Pflege und Bereitstellung der Daten werden Datenredundanzen, Datenabweichungen und inaktuelle Dateninhalte bei der immer noch in großem Umfang arbeitsteilig organisierten Personalbewirtschaftung vermieden. Im Hinblick auf den hohen Schutzbedarf einzelner Personaldaten bzw. von Personalaktendaten müssen für diese Verfahren neben einer Beschreibung der Verarbeitungszwecke genaue Festlegungen über Schnittstellen zu den Fachverfahren, Zugriffsberechtigungen, Nutzungs- und Auswertungsmöglichkeiten sowie über die zur Gewährleistung von Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit erforderlichen Maßnahmen getroffen werden.

Bei **Verfahren zur betriebswirtschaftlichen Steuerung der Haushaltswirtschaft einschließlich der Kosten-/Leistungsrechnung** geht es vor allem darum, den Ressourcenverbrauch unter Kosten-Nutzen-Gesichtspunkten zu erfassen und über ein damit verbundenes Berichtswesen Möglichkeiten des Controllings und des Nachsteuerns während des Haushaltsjahres zu erschließen. Der Ressourcenverbrauch wird in der Regel dadurch ermittelt, dass die für die festgelegten Produkte und Tätigkeiten auf den einzelnen Arbeitsplätzen aufgewendeten Arbeitsanteile arbeitstäglich von den Bediensteten durch Zeitaufschreibung erfasst werden. Durch diese Art der Erfassung entstehen in großem Umfang personenbezogene Daten, die auch einen Rückschluss auf das Arbeitsverhalten der jeweiligen Arbeitsplatzinhaberinnen und -inhaber ermöglichen; daher müssen die Zugriffsmöglichkeiten sowie die Nutzungszwecke für die weitere Verwendung dieser Informationen genau definiert und über ein Berechtigungskonzept und weitere datenschutzrechtliche Leitplanken abgesichert werden.

Bei der Einführung betriebswirtschaftlicher Steuerungsinstrumente in der öffentlichen Verwaltung und effizienter Personalmanagementverfahren wird es auch künftig vor dem Hintergrund der sich stetig verknappenden finanziellen Ressourcen mehr denn je erforderlich sein, Transparenz auf der Kostenseite herzustellen und Leistungsbemessungen zu ermöglichen sowie den Personalstellen Instrumente zur Verfügung zu stellen, die für eine effektive Personalplanung und -bewirtschaftung sowie für zielgerichtete Personalentwicklungsmaßnahmen unverzichtbar sind.

Mitarbeiterinnen und Mitarbeiter sowie Personalvertretungen begegnen der Einführung derartiger Verfahren aus Sorge um die Entstehung des „gläsernen“ Bediensteten häufig skeptisch bis zurückhaltend. Befürchtungen gehen dahin, dass Informationen aus den unterschiedlichsten Datenquellen ohne Kenntnis der betroffenen Bediensteten durch vielfältige Datenverknüpfungen, auch über Schnittstellen mit anderen automatisierten Verfahren, ge-

zielt zusammengeführt und ausgewertet werden können. Vor allem besteht die Sorge, dass die Ergebnisse aus dem zur Steuerung der Verfahren eingesetzten „Berichtswesen“ und dem „Controlling“ letztlich auch zu einer unzulässigen individuellen Verhaltens- und Leistungskontrolle genutzt werden könnten.

Die Handreichung stellt konkrete umsetzungsorientierte Handlungsempfehlungen vor, die aus datenschutzrechtlicher Sicht und unter dem Aspekt der Datensicherheit bei der Einführung und Anwendung derartiger Verfahren zu erfüllen sind.

II. Allgemeine datenschutzrechtliche Leitplanken

Personenbezogene Daten fallen bei der Nutzung dieser technisch unterstützten Verfahren als Inhaltsdaten (Personaldaten bzw. Personalaktendaten) und als Protokolldaten (mit besonderer Zweckbindung) an.

Für den Umgang mit diesen Daten gelten die folgenden allgemeinen Grundsätze:

1. Personenbezogene Daten der Beschäftigten dürfen in technikgestützten Verfahren nur in dem Umfang gespeichert, übermittelt und genutzt werden, in dem dies rechtlich zulässig und im Rahmen der festgelegten Zwecke zur Durchführung der der jeweiligen Stelle obliegenden personalwirtschaftlichen, organisatorischen und sozialen Aufgaben erforderlich ist **(Grundsatz der Zulässigkeit, Zweckbindung und Erforderlichkeit)**.

2. In einem **Berechtigungskonzept** ist festzulegen, welche Stellen und/oder Funktionsträgerinnen oder Funktionsträger im Rahmen der ihnen übertragenen Aufgaben für welche Zwecke und in welcher Form (lesend/ verändernd) befugt sind, auf Daten zuzugreifen oder Auswertungen vorzunehmen. Das Berechtigungskonzept ist fortzuschreiben und mindestens so lange zu speichern wie die zugehörigen Protokolldaten.
3. Es ist schon im Vorfeld bei der Auswahl und Gestaltung der automatisierten Verfahren darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden **(Grundsatz der Datenvermeidung und Datensparsamkeit)**.

4. Die Betroffenen sind über ihren persönlichen Datenbestand, die Zwecke der Verarbeitung und Zugriffsberechtigungen zu unterrichten. Ihre Rechte auf Auskunft, Sperrung und Löschung sind zu wahren. **(Transparenzgebot und Betroffenenrechte)**.

5. Arbeits- und dienstrechtliche Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient **(Verbot der automatisierten Einzelentscheidung).**

6. Zulässige dienststellenübergreifende Auswertungen der in den Verfahren verarbeiteten Personaldaten sollten **soweit möglich anonym oder pseudonym** erfolgen; dies gilt nicht für Auswertungen, Abgleiche oder Zusammenführungen, die sich auf die in der Anlage aufgeführten Merkmale (Informationen zur dienstlichen Funktion und Erreichbarkeit = so genannte Funktionsträgerdaten) beschränken.

7. Die Sicherungsziele **Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit** sind - ausgerichtet am Schutzbedarf der Daten - durch geeignete technisch-organisa-

torische Maßnahmen zu gewährleisten; das Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik BSI gibt dazu zahlreiche Hilfestellungen.

Für die Ausgestaltung der Datenschutz- und Datensicherungsmaßnahmen ist - ggf. aus einer Vorabkontrolle (vgl. Ziffer 9) - ein **Sicherheitskonzept** zu entwickeln und entsprechend dem Stand der Technikfortzuschreiben. Die für das jeweilige Verfahren fachlich Verantwortlichen sind verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen spätestens mit dem Einsatz des Verfahrens umzusetzen und zu dokumentieren, falls dies noch nicht im Sicherheitskonzept enthalten ist. Insbesondere mit Protokollierungsverfahren ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, wer welche Beschäftigtendaten zu welcher Zeit eingegeben, verändert, übermittelt und/oder abgerufen hat; entsprechendes gilt auch für die Systemadministration.

8. **Protokolldaten** von Anwenderinnen und Anwendern sowie Administratorinnen und Administratoren, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert werden, dürfen grundsätzlich nicht für andere Zwecke, insbesondere nicht für eine Verhaltens- und Leistungskontrolle, verarbeitet werden. Die Zweckbindung muss daher technisch und organisatorisch (z. B. durch Dienstanweisung) sichergestellt werden. Für Art, Umfang und Aufbewahrung der Protokollierung gilt der Grundsatz der Erforderlichkeit. Soweit technisch möglich und ausreichend sollte auf personenbezogene Daten verzichtet werden. Die Beteiligungsrechte des Personalrates sind zu beachten.

9. Vor der Einführung und Anwendung neuer Verfahren oder im Falle einer wesentlichen Veränderung der Verfahren ist eine **Vorabkontrolle** (auch **„Technikfolgenabschätzung“** genannt) durchzuführen, wenn dies durch eine Rechtsvorschrift vorgesehen ist.

10. Die Verfahren sind in inhaltlicher und technischer Hinsicht ausreichend und nachvollziehbar zu **dokumentieren**.

11. Die **behördlichen Beauftragten für den Datenschutz** sind bei der Entwicklung und Implementierung der Verfahren frühzeitig zu beteiligen.

12. Um die Akzeptanz zu fördern, wird empfohlen, über Einführung und Anwendung der Verfahren eine **Dienstvereinbarung** mit dem Personalrat abzuschließen, in der insbesondere die Fragen der Zugriffsberechtigungen, der Zulässigkeit und Zweckbestimmung von Auswertungen und die Durchführung von Kontrollen für alle Beteiligten eindeutig und klar geregelt werden. Soweit die Verfahren geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sind die Mitbestimmungs- bzw. Mitwirkungsrechte der Personalvertretung zu berücksichtigen.

III. Personalinformationssysteme/Personalmanagementverfahren

1. Sofern ein **Freitextfeld** zwingend erforderlich ist, muss hinreichend konkret geregelt werden, welche Sachverhalte oder Eintragungen hier nur zulässig sein können.

2. Die besonderen Vorschriften über den Schutz von **Personalaktendaten** sind zu beachten; um dies zu erleichtern, wird empfohlen, Personalaktendaten besonders zu kennzeichnen.

3. Auswertungen unterliegen einer engen **Zweckbindung**. Es wird empfohlen, den Katalog der zulässigen Auswertungen in zentralen oder ressortspezifischen Dienstvereinbarungen festzulegen. Bei allen Auswertungen ist auf eine frühestmögliche **Anonymisierung oder Pseudonymisierung** zu achten.

4. Von den Unterlagen über **medizinische oder psychologische Untersuchungen** und Tests dürfen im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet oder genutzt werden, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz der Beschäftigten dient.

IV. Verfahren der Haushaltsbewirtschaftung

1. Im Rahmen der technisch-organisatorischen Maßnahmen könnte es sich empfehlen, den Zugang zum System (**Benutzerkennung**) z. B. durch Vergabe einer **Identifikationsnummer** zu **pseudonymisieren.**

   Die Identifikationsnummer sollte durch eine **Vertrauensperson** vergeben werden. Die im Einvernehmen mit der Personalvertretung zu bestellende Vertrauensperson ist bei der Erfüllung ihrer Aufgaben weisungsunabhängig. Die Vertrauensperson sollte im Hauptamt nicht mit Personalangelegenheiten, Aufgaben des Controllings oder systemadministrativen Aufgaben befasst sein. Für die Vertrauensperson sollte nach demselben Verfahren eine Vertreterin/ ein Vertreter bestellt werden. In kleinen Dienststellen kann von dieser Verfahrensweise abgewichen werden.

2. Ist-Personalkosten, Beihilfe- oder sonstige Krankheitskosten sollen in den Haushaltsbewirtschaftungssystemen nur verarbeitet werden, soweit hierbei Rückschlüsse auf bestimmte Beschäftigte ausgeschlossen sind. Dies ist z. B. mittels aggregierter Ist-Daten oder pauschalierter Durchschnittssätze zu gewährleisten.

3. Eine personenbezogene Auswertung der durch die Verfahren erfassten Werte muss unterbleiben, soweit der beabsichtigte Zweck auch durch Zusammenfassung von ähnlichen Produkten oder Leistungen oder durch Aggregation im Berichtswesen erreicht werden kann.

4. Auch die im Rahmen einer Kosten- und Leistungsrechnung (**KLR**) und sonstiger Controlling-Verfahren erhobenen Daten über Mitarbeiterinnen und Mitarbeiter (etwa personenbezogene Zeitdaten) dürfen nicht zum Zwecke einer unzulässigen Verhaltens- und Leistungskontrolle einzelner Beschäftigter verwendet werden. Daher müssen diese Daten auch hier so früh wie möglich anonymisiert bzw. Personenbezüge durch Aggregierung aufgelöst werden. Die Beschäftigten sollten im übrigen aus Gründen der Transparenz rechtzeitig und umfassend über derartige Verfahren informiert werden.

Anlage (Funktionsträgerdaten):

Name
Vorname
Anrede
Funktionsbezeichnung/ Dienststellung
Organisationseinheit (z. B. Referat, Dezernat)
Dienststelle (Behördenbezeichnung)
Adresse der Dienststelle (Straße, Hausnummer, Ort, Postleitzahl)
dienstliche Tele fonnummer
dienstliche Telefaxnummer
dienstliche E -Mail-Adresse (Internet)
dienstliche E -Mail-Adresse (X.400)
Bundesland
Ort
Öffentliche Schlüssel für Verschlüsselung und elektronische Signatur
Zimmernummer