LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/10323**

25.11.2015

Antwort

der Landesregierung

auf die Kleine Anfrage 4006 vom 26. Oktober 2015
des Abgeordneten Dirk Schatz PIRATEN
Drucksache 16/10051

EPOS.NRW - Erhöhte Anforderungen an den Datenschutz und die Datensicherheit bei der Personaldatenverarbeitung

Der Finanzminister hat die Kleine Anfrage 4006 mit Schreiben vom 24. November 2015 namens der Landesregierung beantwortet.

Vorbemerkung der Kleinen Anfrage

Die Landesregierung verfolgt im Rahmen des Programms EPOS.NRW (Einführung von Produkthaushalten zur outputorientierten Steuerung - Neues Rechnungswesen) das Ziel, die Effizienz und Effektivität des Verwaltungshandelns durch eine Modernisierung des Rechnungswesen zu steigern.

Diese Modernisierung bringt jedoch auch weitreichende Änderungen in der Personaldatenverarbeitung der einzelnen Ministerien und Landesbetriebe mit sich. So ist die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorgesehen. Die gemeinsame Nutzung einer solchen Infrastruktur bringt erhöhte Anforderungen an den Datenschutz und die Datensicherheit mit sich. Zum einen werden die Begriffe „Mandant“ und „Mandantenfähigkeit“ relevant. Mandantenfähigkeit ist gegeben, wenn Unternehmen, Behörden oder Organisationen in der Lage sind, Daten in einer Datenbank logisch zu trennen und zu verwalten. Im Rahmen der ständigen Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurde am 11.10.2012 vom Arbeitskreis Technische und Organisatorische Datenschutzfragen eine Orientierungshilfe zur Mandantenfähigkeit von IT-Systemen verabschiedet. In dieser Empfehlung werden die Schritte dargestellt, die aus Datenschutzsicht notwendig sind, um eine ausreichende Trennung der Daten zu gewährleisten. Danach setzt eine ausreichende Mandantentrennung voraus, dass die Zugriffsberechtigungen, Verarbeitungsfunktionen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden. Zudem müssen mandantenspezifische Benutzerken-

Datum des Originals: 24.11.2015/Ausgegeben: 30.11.2015

nungen angelegt werden, um sicherzustellen, dass mit diesen Kennungen nur auf Daten des jeweiligen Mandanten zugegriffen werden kann. Notwendig sind also eine getrennte Berechtigungsvergabe und unterschiedliche Konfigurationsmöglichkeiten.

Zum anderen verlangt die Umstellung auf eine gemeinsame Datenhaltung ein zentrales Sicherheitskonzept, wie es in § 10 Abs. 3 DSG NRW vorgeschrieben ist. Dazu gehört insbesondere die vorab zu stellende Schutzbedarfsanalyse, die die Schutzbedürftigkeit, Vertraulichkeit und Integrität der personenbezogenen Daten feststellen muss. Zudem ist zu prüfen, ob für den Bereich besonders sensibler Daten, eine separate EPOS-Serverumgebung einzurichten wäre. So empfiehlt es zumindest der Datenschutzbeauftragte des Landes Mecklenburg-Vorpommern, der von Beginn an die Einführung des Programms EPOS begleitete und seine datenschutzrechtlichen Bedenken vorbringen konnte (Landtag Mecklenburg-Vorpommern, Unterrichtung durch den Datenschutzbeauftragten für Datenschutz und Informationsfreiheit, Drs. 5/3844, Drs. 6/712, Drs. 6/2810).

Um den hohen Schutzbedarf von Personaldaten in den EPOS-nutzenden Behörden zu gewährleisten, fehlt bislang auch ein spezieller datenschutzrechtlicher Maßnahmenkatalog für Nordrhein-Westfalen.

Vorbemerkung der Landesregierung

Die in der Kleinen Anfrage zitierten Drucksachen des Datenschutzbeauftragten des Landes Mecklenburg-Vorpommern beziehen sich offensichtlich auf ein Datenverarbeitungsverfahren EPOS, das u. a. im Land Mecklenburg-Vorpommern zur Personalakten-verwaltung eingesetzt wird. Zwischen diesem EPOS-Verfahren und EPOS.NRW besteht Namensgleichheit. Beide Datenverarbeitungs-verfahren haben nichts miteinander gemeinsam.

Es wurden jedoch auch in der Datenschutzkonzeption zu EPOS.NRW die Hinweise aus den in der Anfrage aufgeführten Drucksachen des Landes Mecklenburg-Vorpommern aufgegriffen.

1. Auf welche möglichen Gefahren durch den Einsatz von EPOS.NRW wurde die Landesregierung durch die Vorabkontrolle i.S.d. § 10 Abs. 3 S. 1 DSG NRW aufmerksam gemacht?

Das Sicherheitskonzept in Verbindung mit der Vorabkontrolle zu EPOS.NRW setzt sich i. S. d. § 10 Abs. 3 DSG NRW mit folgenden Gefahren dezidiert auseinander und skizziert die entsprechenden Gegenmaßnahmen:

- Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten
- Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten
- Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten
- Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten
- Fehlende oder nicht ausreichende Vorabkontrolle
- Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten
- Fehlende Transparenz für Betroffene und die Datenschutz-Kontrollinstanzen

- Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten
- Unzulässige automatisierte Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten
- Fehlende oder unzureichende Datenschutzkontrolle.

2. Inwieweit wurden vor Inbetriebnahme von EPOS.NRW behörden-spezifische Sicherheitskonzepte erarbeitet i.S.d. § 10 Abs. 3 DSG NRW?

Für das Datenverarbeitungsverfahren EPOS.NRW wurde ein zentrales Sicherheitskonzept erstellt. Behördenspezifische Sicherheitskonzepte sind in den Dienststellen zu erstellen und zu führen.

3. Ist EPOS.NRW (von Beginn an) der kontinuierlichen Evaluation (Datenschutzberichte) durch den nordrheinwestfälischen Landesdatenschutzbeauftragten unterstellt?

Ja.

4. Wie beurteilt die Landesregierung die „Mandantenfähigkeit“ bzw. die ausreichende Trennung personenbezogener Beschäftigungsdaten im Rahmen des Programms EPOS.NRW?

Als mandantenfähig wird Informationstechnik bezeichnet, die auf demselben Server (Hardware) mehrere Mandanten, also Kunden (hier Budgeteinheiten des Landes, z.B. Verwaltungen, Behörden), bedienen kann, ohne dass diese gegenseitig Einblick in ihre Daten haben. Jeder Kunde kann nur seine Daten sehen und ändern. Eine Trennung der personenbezogenen Beschäftigtendaten auf Mandantenebene erfolgt nicht, das Datenverarbeitungsverfahren EPOS.NRW wird in einem einzigen Mandanten betrieben, d.h. es erfolgt keine technische Trennung von Daten auf dem Server (Hardware). Die notwendige Trennung der personenbezogenen Beschäftigtendaten wird durch technisch gleichwertige Maßnahmen der Berechtigungsvergabe realisiert. Eine gewollte Ausnahme stellen die Zahlungspartner des Landes Nordrhein-Westfalen dar: Diese sind, über Dienststellengrenzen hinweg, für alle am Datenverarbeitungsverfahren EPOS.NRW beteiligten Behörden nutzbar. Ziel von EPOS.NRW ist es, Zahlungspartner des Landes unter Beachtung der Grundsätze der Wirtschaftlichkeit und Sparsamkeit landesweit einmalig im Datenverarbeitungsverfahren EPOS.NRW zur Verfügung zu stellen.

5. Wie beurteilt die Landesregierung die Notwendigkeit eines speziellen datenschutzrechtlichen Maßnahmenkatalogs für die EPOS-nutzenden Behörden in NRW?

Die Notwendigkeit wird erkannt.

Das Sicherheitskonzept zum Datenverarbeitungsverfahren EPOS.NRW beschreibt einen Maßnahmenkatalog gegen die in der Antwort zur Frage 1 aufgezeigten Gefahren.
Dieser kann im Hinblick auf behördenspezifische Gefahren durch die Dienststellen ergänzt werden.