Stellungnahme des SBB Beamtenbund und Tarifunion Sachsen e.V. zum Entwurf der Verordnung der Sächsischen Staatsregierung über die Verarbeitung personenbezogener Daten nach dem Sächsischen Personalanalysegesetz - Sächsische Personalanalysegesetz-Durchführungsverordnung (SächsPersAnGDVO)

Der SBB Beamtenbund und Tarifunion Sachsen e.V. hatte nach Vornahme von Änderungen insbesondere hinsichtlich des Datenschutzes grundsätzlich keine Bedenken gegen das Sächsische Personalanalysegesetz vorgetragen. Die Sächsische Personalanalyse-Durchführungsverordnung soll nun die in § 4 des Sächsischen Personalanalysegesetzes vorgesehene Verordnungsermächtigung konkretisieren.

Inhalt und Umfang der zu verarbeitenden personenbezogenen Daten, das Verfahren der Datenbereitstellung und der Datenverarbeitung, die Zeitpunkte der Datenübermittlung an die Staatskanzlei sowie die notwendigen personellen, technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes sollen darin geregelt werden.

Bereits der Umfang der Verordnung mit gerade mal fünf Paragrafen lässt vermuten, dass der gesetzgeberische Auftrag, eine Konkretisierung und Verfahrensbeschreibung vorzunehmen, nicht sehr umfassend umgesetzt wurde. So wird an einigen Stellen lediglich der Auftrag aus dem Personalanalysegesetz wiederholt.

Aber auch die getroffenen Regelungen verbleiben an der Oberfläche.

Die in § 2 Inhalt der Einzeldatensätze aufgeführten Merkmale sind soweit differenziert, dass nun, gerade bei kleineren Dienststellen oder Gemeinden, trotz vorgesehener Pseudonymisierung Rückschlüsse auf die Person getroffen werden können. Auch ist nicht ersichtlich, warum das Merkmal Geschlecht abgefragt wird. Fraglich ist, ob dies diskriminierungfrei ist. Unklar ist, nach welchen Kriterien die Staatskanzlei für einzelne Merkmale einheitliche Kataloge vorgeben solle. Diese, im letzten Satz des Paragrafen vorgesehene Möglichkeit, bleibt unbestimmt und genügt damit nicht den Anforderungen an eine konkrete Zweckbestimmung.

Die in § 3 Abs. 3 vorgesehene Pseudonymisierung ist grundsätzlich notwendig und damit begrüßenswert. Wie oben bereits angemerkt, wird jedoch eine Rückverfolgbarkeit befürchtet. Auch hier wird die Staatskanzlei wiederum ermächtigt, das zu verwendenden Verfahren vorzugeben. Damit genügt unserer Auffassung nach nicht die Verordnung dem gesetzgeberischen Zweck, nämlich eine Konkretisierung vorzunehmen. Vielmehr wird diese der Staatskanzlei überlassen.

Nicht klar wird, warum Geburtsdatum und Personalnummer als Grundlage für die Erstellung des Datensatzkennzeichens verwendet werden. Es ist allgemein bekannt, dass gerade das Geburtsdatum und auch die vielen Mitarbeitern zugängliche Personalnummer nur eine schwache Pseudonymisierung ermöglichen auch wenn ein Hash-Verfahren genutzt werden soll, um diese beiden Eingaben zu kombinieren und damit eine Rückverfolgung deutlich zu erschweren.

Die Vorgabe „Das dafür zu verwendende Verfahren wird einheitlich von der Staatskanzlei vorgegeben.“ ist aus Sicht des SBB bedenklich. Die Einheitlichkeit ist natürlich sinnvoll. Allerdings sollte hier ein Hash-Verfahren nach dem aktuellen Stand der Technik verwendet werden und die Vorgabe nicht durch die Staatskanzlei, sondern durch den Datenschutzbeauftragten des Freistaats Sachsen erfolgen. Sonst besteht klar ein potentieller Interessenkonflikt. Die Verfahren und auch die Hardware entwickeln sich ständig weiter. Was vor zehn Jahren noch als sicher galt, ist es heute häufig nicht mehr.

Um die Schwäche des Datenpaares Geburtsdatum und Personalnummer zu verdeutlichen, wird hier beispielhaft die Größe des Datenraums sowie die sich daraus ergebende Zeit für eine vollständige Suche abgeschätzt. Als Alter eines aktiv Beschäftigten kommen 18 bis 67 Jahre in Frage, das sind 50 mögliche Geburtsjahre. Ein Jahr hat 365 oder 366 Tage. In einer Abschätzung nach oben liefert das also 50 x 400 = 20.000 mögliche Geburtsdaten. Eine Personalnummer ist 7-stellig, das gibt 10.000.000 Möglichkeiten. Multipliziert mit der Zahl der in Frage kommenden Geburtsdaten liefert dies 200.000.000.000 = 2 x 10^{11} Möglichkeiten. Dies entspricht in etwa nur der Sicherheit eines 6-stelligen Passworts, wenn Groß- und Kleinbuchstaben sowie Dezimalziffern und noch zwei Sonderzeichen – insgesamt 64 Zeichen – verwendet werden, da der Logarithmus von 200 Milliarden zur Basis 64 in etwa 6,3 beträgt. Es ist mit einer *Brute-Force*-Attacke (vollständiges Durchprobieren) bereits auf aktueller Rechentechnik in weniger als einer Minute zu knacken.

Deshalb ist es sinnvoll, den Suchraum durch das Anfügen einer dritten Eingabe, bekannt unter dem Begriff *Salt*, signifikant zu vergrößern. Dieses *Salt* wird bei jeder Pseudonymisierung zufällig erzeugt und dient dann als dritte Eingabe für das Hash-Verfahren. Wählt man z. B. sechs zufällige Großbuchstaben als *Salt*, so wird der Suchraum 26^6 mal so groß und man erhält somit in etwa 300 Mio. als Multiplikator der Anzahl der Möglichkeiten. Damit steigt die Sicherheit gegen De-Pseudonymisierung auf in etwa eine Passwortlänge von elf Stellen, was als derzeit ausreichend angesehen wird. Das Knacken würde mit aktueller Rechentechnik mehrere Jahre dauern.

Zusammenfassend empfiehlt der SBB zur Pseudonimisierung:

1) Nicht die Staatskanzlei, sondern der Landesdatenschutzbeauftragte sollte das zu verwendende Hash-Verfahren festlegen.
2) Das Verfahren ist regelmäßig dem algorithmischen und technischen Fortschritt anzupassen.
3) Als dritte Eingabe für das Hash-Verfahren neben Geburtsdatum und Personalnummer ist ein mindestens 6-stelliges, zufällig generiertes *Salt* zu verwenden.

Nur so kann aus Sicht des SBB eine angemessene Pseudonymisierung sichergestellt werden.

Die im Datenschutzrecht notwendige Zweckbindung von Datenerhebung und Datenverarbeitung wird sowohl in dem zugrunde liegenden Personalanalysegesetz, als auch in der konkretisierenden Verordnung unserer Ansicht nach nicht hinreichend deutlich. So spricht § 1 des Personalanalysegesetzes lediglich von ressortübergreifenden strategischen Personalmanagement, durch die Verordnung wird dies nicht deutlicher. § 4 Abs. 3 der Verordnung spricht von einem Personalstrukturbericht, oder Anlass bezogenen Sonderauswertungen nach automatisierter Auswertung. Welchen Inhalts, welcher Zielrichtung und mit welchem Zweck dieser Auswertung erfolgen soll, wird an keiner Stelle konkretisiert. Dies wäre vor allem hinsichtlich der in § 3 Abs. 1 S. 1 des Personalanalysegesetzes aufgeführten Schranke, dass die personalverwaltenden Stellen der Staatskanzlei nur die personenbezogenen Daten übermitteln, die für deren Aufgabenerfüllung zwingend erforderlich sind, notwendig gewesen. Vor dem Hintergrund, dass das Personalanalysegesetz bewusst einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung ist es

zwingend erforderlich, die Zweckbestimmung der Datenanalysen und Berichterstattung konkret, transparent und nachprüfbar zu machen. Dies ist nicht gegeben.

Auch dem Grundsatz der Datensparsamkeit und Datenminimierung wird nicht hinreichend Genüge getan. So ist in § 4 Abs. 7 eine Löschfrist der Daten nach einem Zeitraum von elf Jahren ab dem Stichtag, zu dem sie gebildet wurden, vorgesehen. Dieser Zeitraum wird als entschieden zu lang angesehen. Wenn der Zweck der Datenverarbeitung der ist, halbjährliche Berichte zur ganzheitlichen Personalplanung zu erstellen, ist nicht einsehbar, warum die dem Bericht zugrunde liegenden Einzeldatensätze über ein Jahrzehnt aufbewahrt werden müssen.

gez.
Nannette Seidler
Landesvorsitzende