Telefon: 233 – 6 77 77

Referat für Informations- und Telekommunikationstechnik RIT-R

Tischvorlage

Bericht zum Datenschutz-Verstoß 2016 im Kreisverwaltungsreferat

Antrag Nr. 14-20 / A 04071 der FDP-HUT Stadtratsfraktion
vom 11.05.2018, eingegangen am 11.05.2018

Sitzungsvorlage Nr. 14-20 / V 11732

2 Anlagen

Beschluss des IT-Ausschusses vom 16.05.2018 (SB)
Öffentliche Sitzung

I. Vortrag des Referenten

Am 11.05.2018 hat die Stadtratsfraktion FDP-HUT einen Antrag (14-20 / A 04071) zum Thema „Datenschutz-Verstoß 2016 im Kreisverwaltungsreferat“ gestellt und um dringliche Behandlung in der Sitzung des IT-Ausschuss am 16.05.2018 gebeten.

Die im Antrag (Anlage 1) gestellten Fragen beantwortet das Referat für Informations- und Telekommunikationstechnik mit dieser Tischvorlage.

1. Sachlage

Nach § 50 Abs. 1 BMG haben Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene die Möglichkeit, Auskunft aus dem Melderegister über Daten von Gruppen von Wahlberechtigten, für deren Zusammensetzung das Lebensalter entscheidend ist, zu erhalten.

Im Rahmen der Bundestagswahl 2017 wurden von verschiedenen Parteien Gruppenauskünfte aus dem Melderegister beantragt. Die Datenanforderungen wurden zunächst vom Bürgerbüro, KVR II/212 (Auskünfte und Sperren) auf ihre rechtliche Zulässigkeit geprüft und im Anschluss freigegeben. it@M als städtischer IT-Dienstleister wurde – wie auch in der Vergangenheit – mit der Durchführung der Datenübermittlung beauftragt. Dabei wurde auf die Anwendung der unterschiedlichen Sperrschlüssel von Auskunftssperren (Sperrschlüssel 1, 3, 6, 11 und 12), des bedingten Sperrvermerkes und des Ausschlusses von Personen mit unbestimmten Geschlecht ausdrücklich hingewiesen.

Nicht gesondert hingewiesen wurde darauf, dass die Übermittlungssperren nach § 50 Abs. 5 BMG (Sperre 7 - Widerspruch gegen eine Datenübermittlung an Parteien und Wählergruppen) zu beachten sind, da dies bisher in allen Datenfreigaben von it@M automatisch berücksichtigt wurde.

Bei der Bundestagswahl 2017 wurden erstmals Daten für Parteien zur Wahlwerbung aus dem neuen Einwohnerfachverfahren „OK.EWO“gezogen. Ein Bestandteil des Einwohnermeldeverfahrens OK.EWO ist der so genannte „Auswertassistent“ (AWA).

Als Grundlage für die Filtereinstellungen an der Auswert-Applikation dienen die jeweiligen datenschutzrechtlichen Freigaben des Kreisverwaltungsreferates. Dort werden die Auswahl- und Ausschlusskriterien der Auswertung nach den gesetzlichen Bestimmungen aufgeführt. Dies gilt auch für die auszuschließenden Auskunfts- und Übermittlungssperren.

Für die erste Datenübermittlung wurden durch it@M nicht alle vom Kreisverwaltungsreferat im Freigabeschreiben beauftragten Auskunfts- und Übermittlungssperren in den Filtereinstellungen berücksichtigt.

Auf Grund der Filterkriterien wurden vom AWA insgesamt 68.322 Adress-Sätze ausgegeben und an den Empfänger übermittelt.

Durch das Fehlen der Sperre 7 wurden dabei auch die Anschriften von 2.247 Personen übermittelt, die der Weitergabe ihrer Anschrift an politische Parteien durch Eintragung bei der Meldebehörde widersprochen hatten.

Außerdem wurden die Adressen von fünf Personen ausgegeben, die eine Sperre 12 eingetragen hatten. Dieser Schlüssel wurde bei der Filtereinstellung vergessen.

Die Filtereinstellungen enthielten auch keinen Ausschluss für Personen, die wegen fehlender deutscher Staatsangehörigkeit gar nicht wahlberechtigt waren. So wurden auch 12.324 solcher Personen beauskunftet (und in der zweiten Auswertung weitere 2.147).

Des weiteren wurde ein Fehler im Datenmodell entdeckt, der sich bei der Auswertung bei der Zuordnung zu den Bezirken auswirkt. Es wurden also auch Personen genannt, die gar nicht in den angefragten Bezirken wohnten.

In keiner der fünf Adressübermittlungen waren jedoch, wie der Artikel in der Süddeutschen Zeitung vom 09.05.2018 darstellt, Personen enthalten, die eine Auskunftssperren mit Schlüssel 3 für Gefahr für Leib und Leben aufweisen.

2. Beantwortung des Stadtratsantrags

Welche Maßnahmen erfolgten, um technisch-organisatorische Mängel abzustellen?

Nach Bekanntwerden der fehlenden Filterung nach Sperre 7 durch eine Beschwerde, wurde der Filter entsprechend für alle künftigen Adressübermittlungen an politische Parteien angepasst. In den folgenden vier weiteren Auswertungen für politische Parteien waren demnach keine unzulässigen Ausgaben im Hinblick auf Sperre 7 mehr enthalten.

Aufgrund dieses Vorfalls wurden die folgenden Qualitätssicherungsmaßnahmen zwischen Kreisverwaltungsreferat und it@M vereinbart:

- Das Kreisverwaltungsreferat achtet zukünftig vordringlich auf eine vollständige und verständliche Anforderung im Rahmen der datenschutzrechtlichen Freigabe.
- it@M definiert die dafür notwendige Auswerteparameter für das Auswertewerkzeug AWA. Als zusätzliche Qualitätssicherungsmaßnahme wird diese Parametereinstellung in einem 4-Augen-Prinzip durch eine 2. Mitarbeiterin bzw. einen 2. Mitarbeiter geprüft, um sicher zu stellen, dass die vom Kreisverwaltungsreferat als Fachdienststelle vorgegebenen Kriterien korrekt umgesetzt werden.
- Ebenso wurde die nachfolgend beschriebene Kontrolle der Daten eingeführt.

Welche Kontrolle erfolgt vor der Ausgabe von Daten an Dritte?

Es wird eine um zusätzliche Datenfelder (im wesentlichen Sperrkennzeichen) erweiterte Rohdatenmenge erzeugt und diese stichprobenartig ausgewertet, um sicher zu stellen, dass genau die beauftragten Daten ausgegeben werden.

Nach Prüfung der erweiterten Daten ebenfalls im 4-Augen-Prinzip wird die Rohdatenmenge wieder auf die an den Empfänger weiterzugebenden – freigegebenen – Datenfelder reduziert.

Durch diese Maßnahmen und den für alle Beteiligten darüber hinaus geltenden Sorgfaltsmaßstab werden nach Ansicht der beteiligten Dienststellen vergleichbare Fehler und entsprechende Datenschutzverletzungen zukünftig ausgeschlossen.

Bei weiteren individuellen Auswertungen im Jahr 2018, die mit dem vereinbarten, geänderten Prozess durchgeführt wurden, sind keine Datenschutzprobleme aufgetreten.

Auch in Zukunft wird der engmaschige Kontakt und die zielorientierte Zusammenarbeit zwischen Kreisverwaltungsreferat und dem RIT fortgesetzt, um Datenschutzverletzungen auszuschließen.

Mit welchen Schadensersatzansprüchen ist seitens der betroffenen Bürger zu rechnen und welche Regressansprüche können gegenüber dem IT-Dienstleister in diesem Fall geltend gemacht werden?

Bisher wurden seitens der betroffenen Bürgerinnen und Bürger keine Schadensersatzansprüche geltend gemacht.

Nach der Stellungnahme der Rechtsabteilung des Direktoriums (Anlage 2) erscheint ein Vermögensschaden unwahrscheinlich, kann jedoch ohne Kenntnisse des konkreten Einzelfalls nicht abschließend beurteilt werden. Auch beim Ersatz immaterieller Schäden kommt es in besonderem Maße auf die Umstände des Einzelfalls an.

Der Schadensersatzanspruch ist nach Art. 14 Abs. 2, S. 3 und 4 BayDSG auf insgesamt 125.000 Euro begrenzt, und zwar auch dann, wenn von der Datenschutzverletzung mehrere Personen betroffen sind.

Mit der Auswertung wurde der städtische IT-Dienstleister it@M beauftragt. Gegen den stadtinternen IT-Dienstleister können keine Regressforderungen geltend gemacht werden.

Inwieweit der mit der Erstellung des Auswerteassistenten beauftragte IT-Dienstleister für eventuell entstehende Schadensersatzpflichten in Regress genommen werden kann, wird von it@M geprüft.

Welche zusätzlichen Sicherheitskriterien wurden eingerichtet und welche Maßnahmen wurden getroffen, damit der Datenschutz (u. a. bei Neukonfiguration einer Datenbanksoftware) gewährleistet ist?

Bei der Landeshauptstadt München ist das Vorgehen in Bezug auf die Einführung von IT-Lösungen im Allgemeinen und IT-Sicherheit und Datenschutz im Speziellen standardisiert. Im Hinblick auf diese grundlegenden Vorgehensweisen zu IT-Sicherheit und Datenschutz kommen die Vorgaben zur Informationssicherheit sowie die Vorgehensweise bei der Einführung von IT-Lösungen („Prozessmodell IT-Service“) zum Tragen. Die Aktivitäten in Bezug auf IT-Sicherheit sind auf der Basis der international anerkannten Norm ISO/IEC 27001 („IT-Sicherheitsverfahren, Informationssicherheits-Managementsysteme - Anforderungen") ausgestaltet. Auf diese Weise wird sichergestellt, dass bei der Einführung einer neuen IT-Lösung die entsprechenden Regularien der IT-Sicherheit und des Datenschutzes eingehalten und entsprechende Sicherheitsmaßnahmen etabliert werden.

Konkret werden hierzu die Phasen des „Prozessmodells IT-Service" durchlaufen, in deren Rahmen entsprechende Konformitätsprüfungen und speziell das Risikomanagement IT-Sicherheit verbindlich vorgegeben sind. In diesem Zusammenhang werden Risiken bei dem Betrieb einer IT-Lösung in der städtischen IT-Infrastruktur identifiziert und bewertet sowie im Anschluss über geeignete technische und organisatorische Sicherheitsmaßnahmen behandelt. Grundsätzlich gilt, dass in diese Überprüfungen auch immer jeweils aktuelle Entwicklungen bzw. neue Erkenntnisse im Themenbereich einfließen. Insbesondere sind dies natürlich verlässliche Aussagen oder Empfehlungen von für die öffentliche Hand relevanten Stellen, wie z. B. dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

3. Abstimmung

Die Tischvorlage wurde mit dem Kreisverwaltungsreferat abgestimmt. Die Anmerkungen der Fachdienststelle wurden aufgenommen.

II. Antrag des Referenten

1. Der Stadtrat nimmt den Vortrag des Referenten zur Kenntnis.
2. Der Antrag Nr. 14-20 7 A 04071 der Stadtratsfraktion FDP-HUT vom 11.05.2018 ist damit geschäftsordnungsmäßig erledigt.
3. Der Antrag unterliegt nicht der Beschlussvollzugskontrolle.

III. Beschluss

nach Antrag.

Der Stadtrat der Landeshauptstadt München

Die / Der Vorsitzende — Der Referent

Ober-/Bürgermeister/-in
ea. Stadtrat/-rätin

Thomas Bönig
Berufsm. Stadtrat

IV. Abdruck von I. mit III.
über die Stadtratsprotokolle

an das Direktorium - Dokumentationsstelle
an die Stadtkämmerei
an das Revisionsamt
z. K.

V. Wv.: it@M-Beschuss- und Berichtswesen