UNABHÄNGIGES DATENSCHUTZ ZENTRUM SAARLAND

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Fritz-Dobisch-Straße 12 . 66111 Saarbrücken
Postfach 102631 . 66026 Saarbrücken
Telefon 0681/94781-0
Telefax 0681/94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
Fritz-Dobisch-Straße 12 . 66111 Saarbrücken

Saarbrücken, im Juni 2015

Az: O1011/11
Bearbeiter/in: Thorsten Sokoll
Durchwahl: -41
E-Mail: sokoll@datenschutz.saarland.de

Nutzung von Tablet-Computern zum Zugriff auf ein Ratsinformationssystem

Handreichung zum technisch-organisatorischen Datenschutz, Stand: Juni 2015

Vorwort

Statt in Papierform werden Ratsunterlagen den Ratsmitgliedern häufig bereits elektronisch zur Verfügung gestellt.
Als verantwortliche Stelle für das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten nach § 3 Abs. 3 Saarländisches Datenschutzgesetz (SDSG) hat die Kommunalverwaltung hierbei den Schutz der Daten zu gewährleisten und die für die automatisierte Datenverarbeitung technisch-organisatorischen Maßnahmen eigenverantwortlich festzulegen.

Diese Handreichung soll die Kommunalverwaltung bei der Auswahl eines geeigneten Betriebsszenarios unterstützen.

Über den technisch-organisatorischen Datenschutz hinausgehende rechtliche Anforderungen sind nicht Teil dieser Handreichung und sollten ebenfalls im Vorfeld abgeklärt und schriftlich fixiert werden (beispielsweise sind im Falle einer Privatnutzung eines von der Kommunalverwaltung bereitgestellten Endgeräts auch steuerliche Aspekte -wie eventuell ein geldwerter Vorteil für die Privatnutzung- zu berücksichtigen,..).

Rechtliche Rahmenbedingungen

§ 11 SDSG führt hierzu aus:

„(1) Vor dem erstmaligen Einsatz automatisierter Verfahren zur Verarbeitung personenbezogener Daten ist zu prüfen, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht erwachsen können (Vorabkontrolle). Automatisierte Verfahren dürfen nur dann eingesetzt werden, wenn sichergestellt ist, dass keine Gefahren für das informationelle Selbstbestimmungsrecht bestehen oder diese durch Maßnahmen nach Absatz 2 verhindert werden können.
Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Gefahren und der Art der zu schützenden personenbezogenen Daten angemessen ist."

Die angesprochene Vorabkontrolle muss vor dem erstmaligen Einsatz durch die Kommunalverwaltung erfolgen. Auf der Seite des Unabhängigen Datenschutzzentrums stehen unter www.datenschutz.saarland.de hierfür im Bereich „Themen" entsprechende Formulare zum Download bereit. Zur Minimierung der Gefährdungen für das Recht auf informationelle Selbstbestimmung hat die Kommunalverwaltung als verantwortliche Stelle geeignete Maßnahmen zu ergreifen. Diese sind in §11 Abs. 2 SDSG beschrieben:

„(2) Werden personenbezogene Daten automatisiert verarbeitet, ist die innerbehördliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass diese Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können."

Allgemeine Überlegungen

Die essentiellen Fragen hinsichtlich der Nutzung von mobilen Endgeräten zur Ratsarbeit lauten:

- Darf ein von der Kommunalverwaltung zur Ratsarbeit bereitgestelltes Endgerät auch privat genutzt werden?
- Darf ein privates Endgerät auch zur Ratsarbeit genutzt werden?

Wie in der Einleitung angemerkt: Die Kommunalverwaltung ist die verantwortliche Stelle für das Ratsinformationssystem und die darin enthaltenen personenbezogenen Daten und legt somit in Eigenverantwortung die technisch-organisatorischen Maßnahmen fest.

Für die Bereitstellung von Ratsinformationen zum Zugriff durch Tablet-Computer sind mindestens die gleichen Sicherheitsanforderungen einzuhalten, wie diese beispielsweise für die Verwaltungscomputer der mit der Ratsarbeit betrauten Verwaltungsmitarbeiter gelten. Auf Grund zusätzlicher Gefährdungen bei mobilen Endgeräten (z. B. durch Verlust) sind darüber hinaus zusätzliche Maßnahmen zu ergreifen.

Bei der weiteren Betrachtung sollte man sich daher folgende Fragen stellen:

Darf der Verwaltungsmitarbeiter..

- .. den Verwaltungscomputer privat nutzen?
- .. seinen Privatcomputer für seine Verwaltungstätigkeit benutzen?
- .. den Verwaltungscomputer Freunden, Bekannten oder seinen Kindern zur Nutzung überlassen?
- .. selbst beliebige Software installieren?
- .. seinen Computer oder das Betriebssystem selbst aussuchen?
- .. sich selbst um die Absicherung des Verwaltungscomputer kümmern (Virenschutz, Passwortschutz,..)?
- .. bei einem Defekt den Verwaltungscomputer bei einem beliebigen Dienstleister abgeben?
- .. bei seinem Ausscheiden den Verwaltungscomputer mit all seinen Daten mit nach Hause nehmen?

Vermutlich werden Sie alle obigen Fragen mit „nein“ beantwortet und für den internen Dienstbetrieb entsprechende technisch-organisatorische Maßnahmen getroffen, sowie Dienstanweisungen oder konkrete Handlungsvorgaben erteilt haben.

Demnach sind schon zu Beginn einer elektronischen Gremienarbeit, wie auch im laufenden Betrieb und schließlich auch bei der Beendigung dieser Tätigkeit die entsprechenden technisch-organisatorischen Maßnahmen zu ergreifen. Hierzu zählen auch konkrete Anweisungen, wie beispielsweise bei einem Defekt, bei einem Sicherheitsvorfall oder auch einem Verlust vorzugehen ist. Deshalb sollte dies im Rahmen einer Nutzungsvereinbarung schriftlich fixiert werden.

Die Löschung von Daten – und damit die Vernichtung von Unterlagen – ist vorzunehmen, wenn diese für die Aufgabenerfüllung des Mandatsträgers nicht mehr benötigt werden. Dies kann auch bei noch laufendem Mandat ohne Bedenken baldmöglichst vorgenommen werden, weil die Gremienmitglieder bei Bedarf jederzeit im Rahmen ihrer Zuständigkeiten auf die archivierten Dokumente bei der Verwaltung oder ihrer Fraktion zurückgreifen können.
Um ein solches unwiederbringliches Löschen elektronischer Dokumente zu erreichen, bedarf es i.d.R. einer speziellen Software, die durch mehrmaliges Überschreiben die Daten endgültig löschen kann.

Konkrete Betriebsszenarien

Im Folgenden wird davon ausgegangen, dass die Nutzung des Ratsinformationssystems mittels einer App geschieht.
Dies ist der Nutzung des Ratsinformationssystems über den Internetbrowser vorzuziehen, da bei dieser beispielsweise nicht festgelegt werden kann, dass die Dateien im Offline-Betrieb ausschließlich in einem verschlüsselten Bereich abgelegt werden können. Weiterhin besteht bei einer Nutzung per Internetbrowser beispielsweise die Gefahr, dass der Zugriff ebenfalls über einen ungesicherten Computer (z.B. Internetcafé) erfolgen kann.

Die „Ratsinformationssystem-App" sollte folgende Funktionalitäten aufweisen:

- Benutzer-Authentifizierung beim Öffnen der App durch Eingabe eines Passworts oder besser: einer Kombination aus Benutzername und Passwort
- Verschlüsselte Kommunikation mit dem Ratsinformationssystem
- Verschlüsselte Ablage eventueller Offline-Ratsinformationen
- Ratsinformationen dürfen aus der App nicht in andere Anwendungen (Cloud, E-Mail,..) übertragen werden können

Die Umsetzung und Kontrolle der technisch-organisatorischen Maßnahmen durch die Gemeinde wird in den folgenden Fällen von Fall zu Fall hin immer schwieriger.

→Von der Kommunalverwaltung bereitgestelltes Endgerät mit verbotener Privatnutzung (Ziffer 1a)
→ Von der Kommunalverwaltung bereitgestelltes Endgerät mit erlaubter Privatnutzung (Ziffer 1b)
→Privates Endgerät mit zugelassener Nutzung für die Gremienarbeit (Ziffer 2)

Grundsätzlich gilt:
Zur technischen Durchsetzung von Sicherheitsmaßnahmen sollte das Endgerät in eine von der Kommunalverwaltung betriebene und verwaltete Managementlösung eingebunden werden.
Dies könnte beispielsweise durch die Einbindung in Microsoft Active Directory/Exchange Server und die entsprechenden Gruppenrichtlinien bzw. besser in eine eigenständige Mobile Device Management Lösung (MDM) geschehen.
So kann die Kommunalverwaltung zentral beispielsweise einen genügend komplexen Endgeräte-Zugangsschutz einrichten. Weiterhin kann die Gemeinde im Falle eines Endgerät-Verlustes bei Tablet-Computern eine Löschung aus der Ferne (remote wipe) initiieren.
Ausgeschiedene Ratsmitglieder dürfen keinen Zugang zu bisherigen und künftigen Ratsinformationen haben

Vor Einsatz des Ratsinformationssystems sollten zumindest die folgenden Punkte im Rahmen einer Nutzungsvereinbarung schriftlich fixiert werden. Hierbei ist zu klären wer für den jeweiligen Punkt verantwortlich ist und welche Regelungen bei den einzelnen Punkten gelten sollen.

- Endgeräte-Auswahl
- Endgeräte-Beschaffung
- Einrichtung eines Zugangsschutzes (PIN, Passwort, Fingerabdruck,..) für das Endgerät
- Einrichtung einer Verschlüsselung für das Endgerät
- Einbindung in eine zentrale Verwaltungsplattform (MDM)
- Installation von Betriebssystem-Updates
- Installation eines Schadprogramm-Schutzprogramms (dies ist abhängig von der Endgeräte-Auswahl möglich)
- Installation von Apps
- Nutzung der Druckfunktion
- E-Mail-Nutzung einer von der Verwaltung bereitgestellten E-Mail-Adresse
- E-Mail-Nutzung einer privaten E-Mail-Adresse
- Internet-Nutzung im Rahmen der Ratstätigkeit
- Internet-Nutzung im Rahmen der Privatnutzung
- Verbot von administrativem Zugang zum Endgerät durch Jailbreaking bzw. Rooting
- Verbot der Speicherung von Ratsinformationen außerhalb der „Ratsinformationssystem-App“
- Gewährleitung von Benutzersupport für die Nutzung des Ratsinformationssystems
- Gewährleitung von Benutzersupport für die Nutzung des Endgeräts
- Meldung und Maßnahmen von/bei Sicherheitsvorfällen
- Maßnahmen bei Beendigung der Mandatsträgertätigkeit
- Maßnahmen bei Zuwiderhandlung gegen die Nutzungsvereinbarung
- Maßnahmen bei Wartung/Reparatur des Endgeräts
- Maßnahmen zur Löschung des Endgeräts bei Verlust
- Maßnahmen zur Entsorgung des Endgeräts

1) Von der Kommunalverwaltung bereitgestelltes Endgerät

a) Verbotene Privatnutzung: Company Owned, Business only (COBO)

Bei diesem Betriebsszenario ist die stringente Trennung zwischen dienstlicher/privater Nutzung und dienstlichen/privaten Daten am einfachsten und effektivsten geregelt.

Beispielhafte Regelungen hierbei sind:

	Verantwortlich	**Regelung**
Endgeräte-Auswahl	Verwaltung	Beschränkung auf eine mobile Plattform
Endgeräte-Beschaffung	Verwaltung	Beschaffung durch die Verwaltung
Einrichtung eines Zugangsschutzes (PIN, Passwort, Fingerabdruck,..) für das Endgerät	Verwaltung	Zentrale Vorgabe durch die Verwaltung
Einrichtung einer Verschlüsselung für das Endgerät	Verwaltung	Zentrale Vorgabe durch die Verwaltung
Einbindung in eine zentrale Verwaltungsplattform (MDM)	Verwaltung	Einbindung in das MDM der Verwaltung
Installation von Betriebssystem-Updates	Verwaltung	Zentral durch die Verwaltung, Nutzung des MDM-Systems
Installation eines Schadprogramm-Schutzprogramms	Verwaltung	Zentral durch die Verwaltung
Installation von Apps	Verwaltung	Zentral durch die Verwaltung
Nutzung der Druckfunktion innerhalb der "Ratsinformations-App"	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
E-Mail-Nutzung einer von der Verwaltung bereitgestellten E-Mail-Adresse	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
E-Mail-Nutzung einer privaten E-Mail-Adresse	Verwaltung	Verboten
Internet-Nutzung im Rahmen der Ratstätigkeit	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
Internet-Nutzung im Rahmen der Privatnutzung	Verwaltung	Verboten
Verbot von administrativem Zugang zum Endgerät durch Jailbreaking bzw. Rooting	Verwaltung	Verboten, Nutzung des MDM-Systems
Verbot der Speicherung von Ratsinformationen außerhalb der „Ratsinformationssystem-App“	Verwaltung	Verboten, Sicherheitsfunktion der "Ratsinformationssystems-App"
Gewährleitung von Benutzersupport für die Nutzung des Ratsinformationssystems	Verwaltung	Zentral durch die Verwaltung
Gewährleitung von Benutzersupport für die Nutzung des Endgeräts	Verwaltung	Zentral durch die Verwaltung
Meldung und Maßnahmen von/bei Sicherheitsvorfällen	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Beendigung der Mandatsträgertätigkeit	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Zuwiderhandlung gegen die Nutzungsvereinbarung	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Wartung/Reparatur des Endgeräts	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen zur Löschung des Endgeräts bei Verlust	Verwaltung	Vorgegebene Regelung der Verwaltung, Nutzung des MDM-Systems
Maßnahmen zur Entsorgung des Endgeräts	Verwaltung	Vorgegebene Regelung der Verwaltung

b) *Erlaubte Privatnutzung: Corporate Owned Personally Enabled (COPE) bzw. Private Use of Company Equipment (PUOCE)*

Hieraus können sich folgende Problematiken ergeben:

- Unzureichende Trennung von Ratsdaten und Privatdaten
- Zwang zum Löschen privater Daten: falls beispielsweise das Endgerät verloren geht, sollte die Kommunalverwaltung das Löschen aus der Ferne (remote wipe) einsetzen, um die Ratsdaten schützen zu können. Auch die privaten Daten werden dabei auf dem Endgerät gelöscht.
- Die Kommunalverwaltung darf nicht den Mail- und Internetverkehr des Endgeräts überwachen (und beispielsweise auf Schadsoftware untersuchen), da dies den Vorschriften des Telemediengesetzes zuwider laufen würde.

Beispielhafte Regelungen hierbei sind:

Endgerät der Verwaltung, erlaubte Privatnutzung	**Verantwortlich**	**Regelung**
Endgeräte-Auswahl	Verwaltung	Beschränkung auf eine mobile Plattform
Endgeräte-Beschaffung	Verwaltung	Beschaffung durch die Verwaltung
Einrichtung eines Zugangsschutzes (PIN, Passwort, Fingerabdruck,..) für das Endgerät	Verwaltung	Zentrale Vorgabe durch die Verwaltung
Einrichtung einer Verschlüsselung für das Endgerät	Verwaltung	Zentrale Vorgabe durch die Verwaltung
Einbindung in eine zentrale Verwaltungsplattform (MDM)	Verwaltung	Einbindung in das MDM der Verwaltung
Installation von Betriebssystem-Updates	Verwaltung/ Mandatsträger	Zentral durch die Verwaltung, Nutzung des MDM-Systems, selbst durch den Mandatsträger
Installation eines Schadprogramm-Schutzprogramms	Verwaltung	Zentral durch die Verwaltung
Installation von Apps	Verwaltung/ Mandatsträger	Zentral durch die Verwaltung/selbst durch den Mandatsträger
Nutzung der Druckfunktion innerhalb der "Ratsinformations-App"	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
E-Mail-Nutzung einer von der Verwaltung bereitgestellten E-Mail-Adresse	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
E-Mail-Nutzung einer privaten E-Mail-Adresse	Mandatsträger	Erlaubt, Einrichtung durch den Mandatsträger
Internet-Nutzung im Rahmen der Ratstätigkeit	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
Internet-Nutzung im Rahmen der Privatnutzung	Mandatsträger	Erlaubt, Einrichtung durch den Mandatsträger
Verbot von administrativem Zugang zum Endgerät durch Jailbreaking bzw. Rooting	Verwaltung	Verboten, Nutzung des MDM-Systems
Verbot der Speicherung von Ratsinformationen außerhalb der „Ratsinformationssystem-App“	Verwaltung	Verboten, Sicherheitsfunktion der "Ratsinformationssystems-App"
Gewährleitung von Benutzersupport für die Nutzung des Ratsinformationssystems	Verwaltung	Zentral durch die Verwaltung
Gewährleitung von Benutzersupport für die Nutzung des Endgeräts	Verwaltung	Zentral durch die Verwaltung, kein Support für Probleme im Bereich der Privatnutzung
Meldung und Maßnahmen von/bei Sicherheitsvorfällen	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Beendigung der Mandatsträgertätigkeit	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Zuwiderhandlung gegen die Nutzungsvereinbarung	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Wartung/Reparatur des Endgeräts	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen zur Löschung des Endgeräts bei Verlust	Verwaltung	Vorgegebene Regelung der Verwaltung, Nutzung des MDM-Systems
Maßnahmen zur Entsorgung des Endgeräts	Verwaltung	Vorgegebene Regelung der Verwaltung

2) Privates Endgerät mit zugelassener Nutzung für die Gremienarbeit

Privates Endgerät: Bring Your Own Device (BYOD) bzw. Corporate Liable Employee Owned (CLEO)

Ein privates Endgerät sollte nur dann zur Gremienarbeit zugelassen werden, wenn es in das Device-Management der Kommunalverwaltung eingebunden wird. Nur so lassen sich die erforderlichen technisch-organisatorischen Maßnahmen verbindlich umsetzen. Andernfalls müsste man das Ratsmitglied zur entsprechenden Einhaltung dieser Maßnahmen organisatorisch verpflichten.

Weiterhin können sich folgende Problematiken ergeben:

- Unzureichende Trennung von Ratsdaten und Privatdaten
- Zwang zum Löschen privater Daten: falls beispielsweise das Endgerät verloren geht, sollte die Verwaltung das Löschen aus der Ferne (remote wipe) einsetzen, um die Ratsdaten schützen zu können. Hierbei werden auch die privaten Daten auf dem Endgerät gelöscht.
- Falls der Benutzer den administrativen Zugang auf sein Endgerät freischaltet (Jailbreaking/Rooting), lassen sich unter Umständen die technischen Maßnahmen der Kommunalverwaltung umgehen.
- Falls der Benutzer sein Endgerät mit Schadsoftware infiziert hat, kann dies unter Umständen Auswirkungen auf die Infrastruktur des gesamten Ratsinformationssystems haben.
- Falls die Kommunalverwaltung die zugelassenen Endgeräte nicht hinsichtlich Gerätevielfalt und Betriebssystem beschränkt, ist mit nicht unerheblichem Supportaufwand auf Seiten der Kommunalverwaltung zu rechnen.

Beispielhafte Regelungen hierbei sind:

	Verantwortlich	**Regelung**
Endgeräte-Auswahl	Verwaltung/ Mandatsträger	Eventuelle Beschränkung auf eine mobile Plattform
Endgeräte-Beschaffung	Mandatsträger	Beschaffung durch den Mandatsträger
Einrichtung eines Zugangsschutzes (PIN, Passwort, Fingerabdruck,..) für das Endgerät	Verwaltung	Zentrale Vorgabe durch die Verwaltung
Einrichtung einer Verschlüsselung für das Endgerät	Verwaltung	Zentrale Vorgabe durch die Verwaltung
Einbindung in eine zentrale Verwaltungsplattform (MDM)	Verwaltung	Einbindung in das MDM der Verwaltung
Installation von Betriebssystem-Updates	Mandatsträger	Durch den Mandatsträger
Eventuelle Installation eines Schadprogramm-Schutzprogramms	Mandatsträger	Durch den Mandatsträger
Installation von Apps	Mandatsträger	Durch den Mandatsträger
Nutzung der Druckfunktion innerhalb der "Ratsinformations-App"	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
E-Mail-Nutzung einer von der Verwaltung bereitgestellten E-Mail-Adresse	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
E-Mail-Nutzung einer privaten E-Mail-Adresse	Mandatsträger	Erlaubt, Einrichtung durch den Mandatsträger
Internet-Nutzung im Rahmen der Ratstätigkeit	Verwaltung	Erlaubt, Einrichtung durch die Verwaltung
Internet-Nutzung im Rahmen der Privatnutzung	Mandatsträger	Erlaubt, Einrichtung durch den Mandatsträger
Verbot von administrativem Zugang zum Endgerät durch Jailbreaking bzw. Rooting	Verwaltung	Verboten, Nutzung des MDM-Systems
Verbot der Speicherung von Ratsinformationen außerhalb der „Ratsinformationssystem-App"	Verwaltung	Verboten, Sicherheitsfunktion der "Ratsinformationssystems-App"
Gewährleitung von Benutzersupport für die Nutzung des Ratsinformationssystems	Verwaltung	Zentral durch die Verwaltung
Gewährleitung von Benutzersupport für die Nutzung des Endgeräts	Verwaltung	Zentral durch die Verwaltung, kein Support für Probleme im Bereich der Privatnutzung
Meldung und Maßnahmen von/bei Sicherheitsvorfällen	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Beendigung der Mandatsträgertätigkeit	Verwaltung	Vorgegebene Regelung der Verwaltung

Maßnahmen bei Zuwiderhandlung gegen die Nutzungsvereinbarung	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen bei Wartung/Reparatur des Endgeräts	Verwaltung	Vorgegebene Regelung der Verwaltung
Maßnahmen zur Löschung des Endgeräts bei Verlust	Verwaltung	Vorgegebene Regelung der Verwaltung, Nutzung des MDM-Systems
Maßnahmen zur Entsorgung des Endgeräts	Verwaltung	Vorgegebene Regelung der Verwaltung

Fazit/Empfehlungen

Unabhängig von der angestrebten Lösung gilt:

- Die Kommunalverwaltung ist die verantwortliche Stelle für die im Ratsinformationssystem (und somit auch für die in der Ratsinformationssystem-App) enthaltenen Daten und legt in dieser Rolle die technisch-organisatorischen Maßnahmen fest.

- Vor Beginn des Einsatzes sollte schriftlich fixiert werden, welche Rechte und Pflichten die Beteiligten (Kommunalverwaltung, Ratsmitglied) zu beachten haben.

- Das Ratsmitglied sollte zusätzlich durch die Kommunalverwaltung zumindest schriftlich, besser noch ergänzend im Rahmen einer angebotenen Schulung, über die Risiken und Sicherheitsmaßnahmen informiert werden.

- Mittels technischer Lösungen lassen sich gemeinsame Sicherheitsstandards einheitlich umsetzen und gewährleisten. Wenn eine technische Lösung verfügbar ist, so ist diese organisatorischen Regelungen vorzuziehen.

- Zur zentralen Verwaltung sollten die Endgeräte in eine Verwaltungslösung (MDM) eingebunden werden.

Das Unabhängige Datenschutzzentrum Saarland empfiehlt für die Gremienarbeit ein von der Kommunalverwaltung bereitgestelltes Endgerät mit verbotener Privatnutzung.

Als verantwortliche Stelle kann die Kommunalverwaltung im Rahmen der Abwägung der Verhältnismäßigkeit in eigener Verantwortung eine geregelte Privatnutzung gestatten. Dieser Tablet-Computer darf jedoch nicht für weitere Tätigkeiten bei einer anderen verantwortlichen Stelle (Banken, Sparkassen, Unternehmen, selbstständige Tätigkeiten,..) genutzt werden. Andernfalls besteht die Gefahr, dass u.U. beide verantwortlichen Stellen anderslautende technisch-organisatorische Maßnahmen für die Nutzung ein und desselben Tablet-Computers vorschreiben.

Von der Einbindung privater Endgeräte in die Gremienarbeit wird abgeraten und dies sollte nur in Betracht kommen, falls die Kommunalverwaltung ihren Ratsmitgliedern kein mobiles Endgerät zur Verfügung stellt.