# Landeshauptstadt Magdeburg

## Stellungnahme der Verwaltung

öffentlich

| Stadtamt | Stellungnahme-Nr. | Datum |
|---|---|---|
| BOB | S0450/19 | 16.10.2019 |

zum/zur

F0233/19 – SR Zander, Fraktion Gartenpartei/Tierschutzallianz

Bezeichnung

Datenspeicherung

| Verteiler | Tag |
|---|---|
| Der Oberbürgermeister | 29.10.2019 |

**Anfrage des SR Zander:**

Sehr geehrter Herr Oberbürgermeister,

für die Arbeit während der VII. Wahlperiode wurden die Stadträte mit iPads ausgestattet, nicht öffentliche Vorlagen werden mit Wasserzeichen versehen.

So werden z.B. Einladungen zu Sitzungen oder Drucksachen, die durch die Fraktionsgeschäftsstelle für die Stadträte ausgedruckt werden, mit dem Namen des Mitarbeiters versehen.

Ich möchte gerne wissen:

1. Welche Daten werden wo gespeichert und wer hat Zugriff auf die gespeicherten Daten?

2. Wie wird sichergestellt, dass ein externer Zugriff durch Admins oder durch Dritte auf die iPads verhindert wird?

3. Auf welche gesetzliche Grundlage bezieht sich die Landeshauptstadt Magdeburg bei der Kennzeichnung der nicht öffentlichen Vorlagen?

4. Im Rathaus wurde eine Sicherheitstür eingebaut die per Transponder zu öffnen ist, in diesem Zuge werden die Türen zu den Büroräumen ebenfalls mit Transpondern ausgestattet. Welche Informationen werden aus der Benutzung der Transponder gewonnen und gespeichert?

5. Aus welchem Grund wird nur der Zugang zum Rathaus auf einer Seite gesichert, auf der anderen Seite aber nicht?

**Zu der Anfrage hat die Verwaltung auch die KID GmbH um Zuarbeit gebeten und nimmt wie folgt Stellung:**

zu Frage 1:
In Session und SessionNet (Gremieninformationssystem) können personenbezogene Daten gespeichert werden, die Erfassung der Daten erfolgt in Session. Dazu zählen Namen, Titel, Geburts-/Sterbedatum, Kommunikationsdaten, Adressen, Bankverbindung und Mitgliedschaften, Steuer ID, Beruf, Website, Nationalität, Staatsangehörigkeit, akademischer Grad, Kontaktdaten eines Sekretariates, Name und Position in der Firma, Device ID für die Mandatos App und Session App, Anmeldename.

Diese Daten werden - sofern diese vorliegen und benötigt werden - in Session hinterlegt. Nur falls eine Freigabe zur Veröffentlichung durch den Mandatsträger vorliegt, werden ausgewählte Daten auch im Bürger- und Gremieninformationssystem veröffentlicht.

Zusätzlich zu den oben genannten Informationen, werden im Gremieninformationssystem folgenden Daten generiert/ hinterlegt:
- Kennwörter (zur Anmeldung am System in Kombination mit dem Anmeldenamen)
- Datum der letzten Anmeldung (erforderlich für den zeitgesteuerten Ablauf der Kennwörter)
- Gremiennotizen
- wahlweise ein Foto zur Person
- Wasserzeichen

Der Zugriff auf diese Daten ist nur einem eingeschränkten, administrativen Personenkreis der LH MD und des technischen Dienstleisters, gemäß dem eingesetzten Rollen- und Berechtigungskonzept und den technischen- und organisatorischen Maßnahmen möglich.

Ausgenommen vom Zugriff bzw. der Speicherung der Daten ist das Wasserzeichen, welches auf nichtöffentliche Sitzungsunterlagen beim Abruf automatisch gedruckt wird. Die Wasserzeichen (versehen mit Name, Datum und Uhrzeit des Abrufs) auf Dokumenten werden zur Laufzeit generiert, d.h. im Moment des Abrufs für den jeweiligen Nutzer. Eine serverseitige Speicherung dieser Daten erfolgt **nich**t.

Der Softwarehersteller Somacos GmbH und Co. KG hat keine Möglichkeit, auf die oben genannten Daten zuzugreifen.

Auf dem iPad werden alle Daten innerhalb der Mandatos iPad iOS App verschlüsselt abgelegt. Dies betrifft sowohl alle Dokumente, sowie die persönlichen Bemerkungen.
Ein Zugriff ist nur mittels der korrekten Zugangsdaten für das iPad und die Mandatos App möglich.
Davon ausgenommen sind Kontaktdaten von Gremienmitgliedern, die optional in das persönliche Adressbuch übernommen werden können.
Die optionale Datensicherung aus der Mandatos App erfolgt ebenfalls verschlüsselt.

zu Frage 2:
Die an die Stadträte übergebenen Endgeräte (iPads) werden durch den IT-Dienstleister über ein Mobile Device Management (MDM) verwaltet.
Diese Verwaltung ermöglicht es, zentrale Restriktionen und Zugriffsschutzmaßnahmen zu setzen (u. a. Passwortvorgaben, Einschränkung des Funktionsumfangs, Entsperrcode-Änderungen, Rücksetzen des Gerätes auf Auslieferungszustand etc).
Ein Remotezugriff (*Remote-Desktop bezeichnet den Fernzugriff auf den Desktop eines Computers. Dabei werden Anwendungsprogramme auf einem Computer ausgeführt und auf einem anderen Computer dargestellt und bedient. Quelle: https://de.wikipedia.org/wiki/Remote-Desktop)* auf die Geräte über das MDM durch den IT-Dienstleister ist nicht möglich.

Der Zugriff Dritter bei Inbesitznahme des iPads wird durch den Entsperrcode des iPads und den Passwortschutz der Mandatos iPad iOS App gewährleistet.
Außerdem sind die Mandatsträger verpflichtet, bei Verlust des Gerätes entsprechende Stellen zu informieren, sodass die Löschung der Daten über das MDM erfolgen kann.

Zu Frage 3:
Die Verpflichtung, schutzbedürftige Angelegenheiten unter Ausschluss der Öffentlichkeit zu behandeln, ergibt sich aus § 52 KVG LSA.
Das Einführen der Wasserzeichen auf nichtöffentlichen/vertraulichen Dokumenten bedarf keiner gesetzlicher Grundlage.

Zu Frage 4:
Außer dem Namen des Transponderbesitzers werden keinerlei Informationen gewonnen oder gar gespeichert.
Insbesondere werden keine Schließvorgänge aufgezeichnet.

Zu Frage 5:
Da für die beiden linken Türen spezielle Schlösser mit einer entsprechend längeren Lieferzeit beschafft werden müssen, erfolgt der Einbau zu einem späteren Zeitpunkt.

Dr. Trümper
Oberbürgermeister