



EG: 21.08.25

über
Herrn Oberbürgermeister 302
Gert-Uwe Mende

feh 22.8.

Der Magistrat

Bürgermeisterin

Christiane Hinnerger

über
Magistrat

und
Herrn Stadtverordnetenvorsteher
Dr. Gerhard Obermayr

20. August 2025

Anfrage der Volt-Fraktion Wiesbaden vom 18.06.25, Nr.258-2025 nach § 45 der
Geschäftsordnung der Stadtverordnetenversammlung 1SV 25-V-02-0015

Informationssicherheit und vertrauliche Unterlagen in der Stadtverwaltung und im Stadtkonzern Wiesbaden

Immer wieder gelangen nicht-öffentliche Sitzungsunterlagen oder vertrauliche städtische Dokumente an die Öffentlichkeit. Solche Leaks verletzen geltendes Recht, untergraben Vertrauen und können - etwa bei sicherheitsrelevanten Inhalten - erheblichen Schaden anrichten.

Die Weitergabe durch Hinweisgeber*innen im Sinne des Hinweisgeberschutzgesetzes (HinSchG) ist hiervon ausdrücklich zu trennen - Whistleblower genießen Schutz, sofern sie Missstände im öffentlichen Interesse aufdecken. Dies schließt ein entschlossenes Vorgehen gegen unbefugte, schädliche Weitergaben jedoch nicht aus.

Wir bitten den Magistrat um die Beantwortung folgender Fragen:

1. Welche Einschätzung hat der Magistrat zu den potenziellen Schäden (rechtliche, finanziell oder sicherheitsbezogen), die durch solche Informationslecks entstehen können - sowohl für die Stadt als auch für die städtischen Gesellschaften?
2. Gibt es aktuell bereits präventive bzw. abschreckende Maßnahmen in Stadtverwaltung/Stadtkonzern oder existieren bereits Prüfaufträge oder Planungen für deren Einführung? Falls ja, welche Maßnahmen sind dies? Falls nein, woran scheiterte bislang die Einführung?
3. Welche technischen, organisatorischen und finanziellen Voraussetzungen wären für die Einführung von individuellen oder allgemeinen Sicherheitsmerkmalen erforderlich oder allgemein Sicherheitsmerkmalen erforderlich oder möglich (z.B. über die bestehende Nextcloud-Infrastruktur)?

Die Anfrage beantworte ich wie folgt:

Zu 1. Welche Einschätzung hat der Magistrat zu den potenziellen Schäden (rechtliche, finanziell oder sicherheitsbezogen), die durch solche Informationslecks entstehen können - sowohl für die Stadt als auch für die städtischen Gesellschaften?

Potenzielle Schäden durch Informationslecks können vielfältig und gravierend sein. Vertrauliche Informationen, die in die falschen Hände geraten, können Sicherheitsrisiken für die Stadt und ihre Bürgerinnen und Bürger darstellen.

Die Weitergabe von vertraulichen Informationen kann darüber hinaus zu rechtlichen Konsequenzen führen. Dies kann sowohl für die Stadt als auch für städtische Gesellschaften zu Klagen und weiteren rechtlichen Auseinandersetzungen führen, insbesondere wenn es um Datenschutzverletzungen oder die Verletzung von Verschwiegenheitspflichten geht.

Finanzielle Schäden können entstehen z.B. wenn vertrauliche Informationen über Ausschreibungen oder Angebote in falsche Hände gelangen, oder durch Schadensersatzforderungen die Betroffene Dritte, wie Bürger oder Unternehmen, geltend machen können, wenn ihnen durch die Veröffentlichung vertraulicher Informationen ein Nachteil entsteht.

Ein Informationsleck kann das Vertrauen der Bürger in die Stadtverwaltung und ihre Institutionen untergraben. Ein geschädigtes Image kann langfristige Auswirkungen auf die Beziehung zur Öffentlichkeit und zu wichtigen Stakeholdern haben.

Zu. 2. Gibt es aktuell bereits präventive bzw. abschreckende Maßnahmen in Stadtverwaltung/Stadtkonzern oder existieren bereits Prüfaufträge oder Planungen für deren Einführung? Falls ja, welche Maßnahmen sind dies? Falls nein, woran scheiterte bislang die Einführung?

Als präventive Maßnahme ist zu sehen, dass Mitarbeitende zur Verschwiegenheit verpflichtet werden. Der Verrat von Dienstgeheimnissen hat also für die Mitarbeitenden der Stadt dienstrechtliche Folgen. Die Grundlage für die Verschwiegenheitspflicht ist im TVÖ verankert. Hierzu heißt es in § 3 Absatz 1 TVöD: „[...] Die Beschäftigten haben über Angelegenheiten deren Geheimhaltung durch gesetzliche Vorschriften vorgesehen oder vom Arbeitgeber angeordnet ist, Verschwiegenheit zu wahren; dies gilt auch über die Beendigung des Arbeitsverhältnisses hinaus.“ Darüber hinaus sind Beamte und Tarifbeschäftigte verpflichtet, für die freiheitlich demokratische Grundordnung einzutreten.

Beamte unterliegen darüber hinaus einer Verschwiegenheitspflicht gemäß § 33 Beamtenstatusgesetz, so dass ein Verstoß Dienstvergehen disziplinarisch geahndet werden kann. Mögliche Maßnahmen reichen von einem Verweis bis zur Entlassung aus dem Beamtenverhältnis. Grundsätzlich gilt ein Aussageverbot ohne Genehmigung: Beamte dürfen über dienstliche Angelegenheiten nicht ohne ausdrückliche Genehmigung aussagen - weder vor Gericht noch außerhalb. Ein Verstoß kann ebenfalls dienstrechtlich geahndet werden.

Analog haben Angestellte mit arbeitsrechtlichen Konsequenzen zu rechnen, von einer Abmahnung bis zur Kündigung, je nach Schwere des Verstoßes.

Verdachtsfälle werden durch das Personalamt untersucht und abschließend durch den Oberbürgermeister als Dienstvorgesetzten entschieden.

Darüber hinaus kann ein Verstoß gegen die Verschwiegenheitspflicht strafbar sein etwa nach § 203 oder § 353b StGB. Bei besonders schwerwiegenden Verstößen drohen empfindliche Strafen.

Die Pflicht zur Verschwiegenheit endet nicht automatisch mit dem Ausscheiden aus dem Dienst. Auch ehemalige Beamte und Beschäftigte der Stadt sind weiterhin zur Geheimhaltung verpflichtet.

Eine Erhebung, wie viele Verstöße begangen wurden, kann zentral nicht erfolgen. Dem Personalamt ist aus den letzten vier Jahren kein Fall bekannt, der von der Schwere des Verstoßes eine dienst- oder arbeitsrechtliche Maßnahme gerechtfertigt hätte.

Zu 3: Welche technischen, organisatorischen und finanziellen Voraussetzungen wären für die Einführung von individuellen oder allgemeinen Sicherheitsmerkmalen erforderlich oder möglich (z.B. über die bestehende Nextcloud-Infrastruktur)?

Technische Maßnahmen zur Dokumentenabsicherung sind möglich, haben aber eine vergleichbar geringe Wirksamkeit bei hohem Einführungsaufwand. Sie erfordern die Verwendung von Spezialsoftware und / oder aufwändigeren Prozessabläufe für die Mitarbeitenden.

Beispielsweise könnte ein Informationsgeber an die Presse durch ein individualisiertes Wasserzeichen zur Dokumentenabsicherung enttarnt werden. Dadurch werden enthaltene Zahlen individualisiert (bspw. Wird die Nachkommastelle einer beliebigen darin vorkommenden Zahl in jedem Dokument verändert). Aber die Wirksamkeit ist gering: Nur wenn die Presse exakt diese Zahl in voller Länge in ihrem Bericht übernehmen würde, könnte diese Quelle enttarnt werden. Typischerweise wird die Presse ihre Quelle jedoch nicht bekanntgeben, ebensowenig das Quelldokument (mit dem individualisierten Wasserzeichen) zur Verfügung stellen.

Zudem sind im Entstehungsprozess der Dokumente bereits unterschiedliche Personen beteiligt, durch die vertrauliche Informationen an Externe weitergegeben werden könnten. Der Faktor Mensch, der sowohl Fehler macht als auch bestechlich sein kann, bleibt das größte Risiko. Technische Verfahren können Fehlverhalten schwieriger machen, aber nicht ausschließen. Wenn der Wille zum Missbrauch von Daten gegeben ist, finden sich Mittel und Wege. Gäbe es eine sichere technische Lösung, wäre heute Spionage bzw. das Leaken von geheimen Dokumenten weltweit nicht mehr möglich.

Eine Abschätzung der technischen, organisatorischen und finanziellen Voraussetzungen für die Einführung von individuellen oder allgemeinen Sicherheitsmerkmalen wäre erst dann sinnvoll, wenn die spezifischen Anforderungen geklärt sind: welche Dokumente mit welchem Empfängerkreis sollen besonders geschützt werden und kann erwartet werden, dass mit einer technischen Lösung ein wirksamer Schutz erreicht werden.

Wirksamer wäre ggfs. eine intensivere Information und Aufklärung der Stadtverordneten und der ehrenamtlichen Magistratsmitglieder auf die im Gesetz verankerte Verschwiegenheitspflicht. Dies könnte durch geeignete Maßnahmen durch Amt 16 z. B. bei der Neubesetzung nach der Kommunalwahl erfolgen.

Mit freundlichen Grüßen

Ulla Bai
Stadträtin

i.V. **Ulla Bai**

Digital
unterschrieben
von Ulla Bai
Datum: 2025.08.20
20:21:16 +02'00'