§ 21/2026/003/1

STADT : SALZBURG

Bürgermeister der
Landeshauptstadt Salzburg

Bernhard Auinger

Frau KO
Mag.a Delfa Kosic
ÖVP
Im Hause

5024 Salzburg, Schloss Mirabell
Telefon +43 662 8072 – DW 2100
Fax +43 662 8072 – DW
bgm@stadt-salzburg.at

Salzburg, 04.02.2026

Betreff
Anfrage gem. § 21 GGO – Datenpanne im Magistrat
Zahl: § 21/2026/003 vom 14.01.2026

Geschätzte Frau Klubobfrau, liebe Delfa!

Gerne beantworte ich Deine Anfrage „Datenpanne im Magistrat", die in meinem Büro am 15. Jänner 2026 eingegangen ist, wie folgt:

1. Wann genau wurde die Datenpanne festgestellt (Datum und Uhrzeit)?

Am Donnerstag, 18. Dezember 2025, am frühen Vormittag.

2. In welchen Bereichen bzw. Ämtern kam es zu dieser Fehlkonfiguration?

Betroffen war die Dienststelle Info-Z der MD/01 Service & Information.

3. Wie wurde diese Fehlkonfiguration genau festgestellt?

Ein Mitarbeiter meldete, dass im Rahmen einer Suche im hausinternen elektronischen Aktensystem e++ mehrere Dokumente abrufbar seien, die personenbezogene Daten zu seiner Person sowie Kolleg:innen der Dienststelle enthielten.

4. Welche personenbezogenen Daten waren genau betroffen und in welchem Umfang?

Diese Daten umfassten Vorname, Nachname, Geburtsdatum, Krankmeldungen, Mitgliedschaft der Gewerkschaft (erschließbar aus dem Zuschussansuchen zum Betriebsausflug).

5. Wie genau konnte auf diese Daten (Frage 4) zugegriffen werden?

Über das e++-Suchprogramm „mindbreeze". Dieses ist unmittelbar an die im e++ vergebenen Zugriffsrechte gekoppelt.

6. Welche Bereiche bzw. Ämter und wie viele Personen konnten auf diese Daten (Frage 4) zugreifen und wie lange?

Die mögliche Einsichtnahme war auf Mitarbeiter:innen der Dienststelle Info-Z beschränkt. 18 Personen hätten zugreifen können. Zugriffsmöglichkeiten außerhalb der Dienststelle waren zu keiner Zeit gegeben. Nach entsprechenden Sofortmaßnahmen war der Zugriff ab Freitagmittag, 19. Dezember 2025, nur mehr für befugte Personen (Amtsleitung und Sekretariat) möglich. Alle genannten Personen unterliegen zudem lt. MagBeG dienstrechtlichen Verschwiegenheitspflichten und sind im dienstlichen Umgang mit personenbezogenen Daten nachweislich geschult.

7. Wie viele Magistrats-Mitarbeiter sind vom Datenleck betroffen?

Siehe Antwort auf Frage 6

8. Wurden die betroffenen Magistrats-Mitarbeiter über das Datenleck informiert? a. Wenn ja, in welcher Form und zu welchem Zeitpunkt? b. Wenn nein, wieso nicht?

Ja, ebenfalls Freitagmittag via E-Mail.

9. Welche technischen und organisatorischen Ursachen haben zu dieser falschen Berechtigungsvergabe geführt?

Es handelte sich um die irrtümliche Zuordnung einer Berechtigungsgruppe und hatte keine technische Ursache.

10. Welche internen Kontrollen und Datenschutz-Prozesse haben versagt bzw. wurden nicht eingehalten?

Der gruppeninterne Zugriff auf die betreffenden Geschäftsstücke wurde nicht ausreichend eingeschränkt.

11. Gibt es Anzeichen, dass diese Panne auf strukturelle Defizite in der IT-Sicherheits- oder Personalverwaltung des Magistrats zurückzuführen ist? a. Falls ja, welche? b. Falls nein, was war die Ursache?

Nein, hierbei handelte es sich um einen individuellen Fehler.

12. Wurde die Panne fristgerecht und vollständig an die zuständige österreichische Datenschutzbehörde (DSB) gemeldet?

Ja

13. Welche rechtlichen Konsequenzen bzw. Prüfungen sind infolge dieser Meldung vorgesehen oder wurden bereits eingeleitet?

Der Vorfall wurde der Datenschutzbehörde gemeldet und die Zugriffsberechtigungen im e++ dieses Amtes wurden angepasst.

14. Welche Maßnahmen wurden ergriffen, um mögliche Schäden (z. B. Missbrauch der Daten) zu begrenzen bzw. auszuschließen?

Siehe Antwort auf Frage 6

15. Wie wird sichergestellt, dass keine weiteren unbefugten Zugriffe auf personenbezogene Daten möglich sind?

Durch korrekte Zuordnung der Zugriffsberechtigungen

16. Welche kurzfristigen und langfristigen Maßnahmen zur Verbesserung der IT-Sicherheit, Berechtigungsverwaltung und des Datenschutzes im Magistrat werden derzeit umgesetzt?

Die Erhaltung einer hohen IT-Sicherheit ist ein laufender Prozess, hierzu sind auf verschiedensten technischen wie organisatorischen Ebenen laufend Verbesserungen vorzunehmen. Eine wesentliche Voraussetzung für eine hohe IT-Sicherheit ist ein hoher Grad von Verschwiegenheit (mit entsprechenden Kenntnissen wären Hürden wesentlich leichter zu überwinden). Soweit derartige Maßnahmen hohe finanzielle oder personellen Aufwendungen verursachen, erfolgt dies durch Beschluss des entsprechenden politischen Gremiums (als Beispiel sei hier die Anschaffung der internen Firewall genannt).

Die Berechtigungen werden seitens der IKT nach dem Erforderlichkeitsprinzip (Need-to-know-Prinzip) via eines streng vorgegebenen Prozesses vergeben. Darüber hinaus haben Fachbereiche bei vielen Anwendungen die Möglichkeit, die Rechte an eigene Bedürfnisse anzupassen. Im Bereich der Berechtigungsvergabe ist seitens der IKT kein Handlungsbedarf erkennbar.

Im Bereich des Datenschutzes erfolgt eine laufende Begleitung und Weiterentwicklung unter Berücksichtigung der geltenden datenschutzrechtlichen Vorgaben sowie organisatorischer und technischer Rahmenbedingungen.

17. Werden zukünftige Fortschritte bzw. Ergebnisse dieser Maßnahmen (Frage 16) transparent und regelmäßig der Politik berichtet?

Wie bereits in Punkt 16 ausgeführt würde eine offene Kommunikation über einzelne Maßnahmen zur Verbesserung der IT-Sicherheit diese konterkarieren. Maßnahmen mit erheblichen finanziellen oder personellen Auswirkungen werden selbstverständlich via Amtsbericht vorgelegt.

Datenschutzaspekte werden im Rahmen der jeweiligen Projekte mitberücksichtigt und im Zuge der Berichterstattung über diese Projekte – soweit erforderlich und zulässig – der Politik dargestellt.

Mit freundlichen Grüßen,

Bürgermeister
Bernhard Auinger