Hausmitteilung

Dresden.

☐ vertraulich

Landeshauptstadt Dresden
Der Oberbürgermeister

Fraktion Team Zastrow
im Stadtrat der Landeshauptstadt Dresden
Mitglied des Stadtrates
Remo Liebscher

GZ: (OB) GB 5

Datum: 25. NOV. 2026

Datenschutz und Sicherheit von OctoWareNET
AF1834/26

Sehr geehrter Herr Stadtrat Liebescher,

Ihre oben genannte Anfrage beantworte ich wie folgt:

„Die Vorlage V1012/26 sieht die Umstellung des Fachverfahrens im Amt für Gesundheit und Prävention von OctoWareTN auf OctoWareNET und dessen Betrieb in einer zentralen Cloud-Umgebung vor.

1. **Welche Datenschutzbewertungen und Sicherheitsunterlagen liegen für den Dresdner Einsatz von OctoWareNET vor? Bitte stellen Sie den Bearbeitungs- und Prüfstand des Sicherheitskonzepts, der Datenschutz-Folgenabschätzung, des Löschkonzepts, des Verzeichnisses der Verarbeitungstätigkeiten so-wie des Rechte- und Rollenkonzepts dar. Welche Stellungnahmen der städtischen Daten-schutzbeauftragten liegen vor? Wurde die zuständige Datenschutzaufsichtsbehörde einbezogen beziehungsweise die Erforderlichkeit einer vorherigen Konsultation geprüft?"**

Für den Einsatz von OctoWareNET im Amt für Gesundheit und Prävention liegen zur Vorlage V1012/26 bislang keine abschließend fertigen und abgenommenen Datenschutz- oder Sicherheitsunterlagen vor. Da im Amt für Gesundheit und Prävention umfangreich besonders sensible Gesundheitsdaten nach Art. 9 DSGVO verarbeitet werden, stellen Datenschutzbeauftragte und Beauftragter für Informationssicherheit hohe Anforderungen an Nachweise und vertragliche Regelungen.

Dabei ist hervorzuheben, dass die städtische Datenschutzbeauftragte (DSB) und der Beauftragte für Informationssicherheit (ISB) bereits seit über 1,5 Jahren fest in die Projektstruktur eingebunden sind, an der Erstellung des Sicherheits- und Datenschutzkonzepts auf Landesebene für das Projekt mitgewirkt haben und durchgängig an allen Austauschrunden beteiligt waren. Unabhängig von dieser kontinuierlichen Mitwirkung befinden sich die für den konkreten Einsatz erforderlichen Dokumente – darunter das Sicherheitskonzept, die Datenschutz-Folgenabschätzung (DSFA), das Lösch- und Aufbewahrungskonzept, das Verzeichnis der Verarbeitungstätigkeiten (VVT) sowie das Rechte- und Rollenkonzept – noch in Erarbeitung bzw. Abstimmung und sollen

nach dem Produktivstart vervollständigt werden. In diesem Zusammenhang werden zudem offene Punkte bei den technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (etwa Zwei-Faktor-Authentisierung, Nutzer- und Rechteverwaltung sowie Passwortrichtlinien), bei der Verfahrensdokumentation und bei unterschriftsreifen vertraglichen Grundlagen einschließlich Auftragsverarbeitung benannt.

Das Sicherheitskonzept für den Einsatz von OctoWareNET in der Landeshauptstadt Dresden wird derzeit in Zusammenarbeit mit dem Eigenbetrieb IT erstellt.
Im Rahmen der Erstellung und Ausarbeitung des Sicherheitskonzepts werden die relevanten datenschutzrechtlichen und informationssicherheitsbezogenen Anforderungen berücksichtigt. Dies umfasst insbesondere folgende Aspekte:

- Erstellung und Prüfung einer Datenschutz-Folgenabschätzung,
- Erarbeitung eines Löschkonzepts,
- Erstellung bzw. Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten,
- Ausarbeitung eines Rechte- und Rollenkonzepts,
- Berücksichtigung der erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der verarbeiteten Daten.

Die jeweiligen Anforderungen und deren Umsetzung werden im weiteren Bearbeitungsverlauf betrachtet und dokumentiert. Ebenso werden die erforderlichen datenschutzrechtlichen Abstimmungen mit der städtischen Datenschutzbeauftragten vorgenommen.

2. **„Welche Zertifikate, Testate und Prüfberichte liegen für die vorgesehene Cloud-Umgebung und den Betrieb von OctoWareNET vor? Bitte nennen Sie Prüfstelle, Prüfzeitraum, Geltungsbereich und gegebenenfalls noch offene Anforderungen. Welche Nachweise beziehen sich auf die Anwendung, deren konkrete Konfiguration und die beteiligten Dienstleister, welche lediglich auf die Cloud-Infrastruktur? Welche ergänzenden Prüfungen und Maßnahmen muss die Stadt selbst durchführen?“**

Für die Cloud-Infrastruktur von OctoWareNET wird eine BSI-C5-Zertifizierung der Telekom MMS herangezogen. Weiterhin liegt bereits ein vom Projektträger MSG erarbeitetes Sicherheitskonzept vor. Dabei wurden sämtliche Konzepte, Zertifikate, Testate und Prüfberichte sorgfältig geprüft, während Detailangaben zu einzelnen Prüfstellen, Prüfzeiträumen und Geltungsbereichen sowie eigenständige Nachweise zur Anwendung, ihrer Konfiguration und der Dienstleisterkette in den vorliegenden Unterlagen noch weiter vervollständigt werden. Für die Gesamtlösung werden noch offene Punkte – darunter ein durchgängiges Gesamt-Sicherheitskonzept, ein Penetrationstest für das E-Portal, aktuelle Last- und Performancetests sowie ein erfolgreicher Migrationstest für Dresden – Schritt für Schritt abgeschlossen.

3. **„Wie werden unberechtigte Zugriffe auf Dresdner Daten verhindert und erkannt? Bitte erläutern Sie die Trennung der Datenbestände der beteiligten Gesundheitsämter, die Regelungen für Administrations- und Supportzugriffe, die Verschlüsselung sowie die Kontrolle und Protokollierung von Zugriffen. Wo werden die Daten einschließlich der Sicherungskopien verarbeitet und gespeichert?“**

Zur Trennung der Datenbestände der 13 beteiligten sächsischen Gesundheitsämter sind in der Risikoanalyse eine systemseitige Datenbank-Trennung, Rollen- und Berechtigungskonzepte, Firewalls, Dienstvereinbarungen sowie Schulungen und Verpflichtungen der Mitarbeitenden vorgesehen. Im laufenden Betrieb zeigen sich Abgrenzungen über Amts-Präfixe und Kunden- bzw. Namespace-Zuordnungen in Zammad und Grafana sowie über TenantID und Projekt-ID in der

...

Open Telekom Cloud (OTC).

Bei Administrations- und Supportzugriffen setzen die Unterlagen auf begrenzte Admin- und Protokollrechte, Mehr-Faktor-Authentifizierung (MFA), Vertraulichkeitsverpflichtungen, Auftragsverarbeitungsverträge und Regelungen zur Subauftragsverarbeitung nach Art. 28 DSGVO sowie das Vier-Augen-Prinzip bei kritischen Prozessen. Supportanfragen an den HoT laufen über Zammad und werden im OTC-Prozess anhand der Tenant-Mailadresse geprüft, während Logfiles aus REF und PROD nur anlassbezogen per GitLab-Pipeline (logcli-helper), GPG-verschlüsselt und ticketgebunden an easy-soft bereitgestellt werden.

Für die Verschlüsselung nennen die Dokumente Transportverschlüsselung und die Verschlüsselung gespeicherter Daten (unter anderem bei Diebstahl oder Verlust mobiler Endgeräte) sowie Pseudonymisierung und Anonymisierung, während bei der Logfile-Übergabe an easy-soft konkret eine GPG-Verschlüsselung greift.

Kontrolle und Protokollierung laufen über Eingabekontrolle und Protokollierung mit Manipulationsschutz, ergänzt durch Schutzmaßnahmen gegen unbefugten Zugriff auf Protokolldaten und unzulässige Mitarbeiterüberwachung wie begrenzte Einsichtsrechte, Dienst- oder Personalratsvereinbarungen sowie Löschkonzepte. Für das laufende Monitoring und Ticketmanagement werden Grafana, Zammad und Jira genutzt.

Verarbeitet und gespeichert wird in REF- und PROD-Umgebungen, der Open Telekom Cloud (OTC), Grafana-Umgebungen der Telekom MMS sowie über ein easy-soft-Transferverzeichnis, wobei exakte physische Rechenzentrums- und Backup-Standorte in den Dokumenten nicht ausgewiesen sind. Zugleich thematisieren die Unterlagen Backup-Konzepte mit zertifiziertem Hoster inklusive Frequenz, Löschfristen und Tests, ISO-Standards (27001, 27002, 27018 und 27701) sowie Risiken rund um Drittlandtransfer und weltweiten Einsatz von Unterauftragsverarbeitern.

4. **„Welche Datenschutz- und Sicherheitsnachweise müssen vor der Übertragung realer Gesundheitsdaten vorliegen, und wer erteilt die Freigabe? Laut Dringlichkeitsschreiben ist die Migration vom 27. bis 30. November 2026 vorgesehen. Bitte geben Sie den aktuellen Vorbereitungsstand an und teilen Sie mit, ob bereits reale Daten übertragen wurden. Werden reale Gesundheitsdaten auch in Test- oder Referenzumgebungen verwendet und wie werden sie dort geschützt?“**

Vor der Übertragung realer Gesundheitsdaten müssen die erforderlichen datenschutz- und sicherheitsrechtlichen Voraussetzungen sowie Nachweise vorliegen – darunter insbesondere eine wirksame Vereinbarung zur Auftragsverarbeitung einschließlich technischer und organisatorischer Maßnahmen, dokumentierte Weisungen durch benannte weisungsberechtigte Personen, Vertraulichkeits- und Geheimnisschutzverpflichtungen (§ 203 StGB) sowie Verpflichtungen nach dem Verpflichtungsgesetz. Hinzu kommen die im Vertrag, Kriterienkatalog und der DSFA vorgesehenen Sicherheits- und Prüfnachweise wie Verschlüsselung der Daten, ein ISMS- bzw. Sicherheitskonzept (u. a. auf Basis von ISO 27001 und BSI IT-Grundschutz), Testate bzw. Zertifikate (einschließlich C5-Kriterien bzw. Festlegungen aus Anlage 1), ein Rollen- und Berechtigungskonzept, ein Löschkonzept sowie ein Migrations-, Test- und Pilotierungskonzept. Die Freigabe erteilt die Amtsleitung des Amtes für Gesundheit und Prävention.

Mit Blick auf den im Dringlichkeitsschreiben genannten Migrationszeitraum vom 27. bis 30. November 2026 gilt für den aktuellen Vorbereitungsstand, dass durch den EB IT bereits eine Datenaufbereitung und Verschlüsselung für die REF-Umgebung vorgenommen und übermittelt wurde.

In den Test- beziehungsweise Referenzumgebungen erfolgt die Aufbereitung und Verschlüsselung der Daten durch den EB IT.

5. **„Wie werden die Löschfristen bei der Migration und im laufenden Betrieb umgesetzt? Anlage 2 erwähnt mögliche zusätzliche Speicherkosten im Zusammenhang mit fehlenden automatisierten Löschkonzepten. Welche Bedeutung hat dies für den Dresdner Datenbestand? Wie werden Löschpflichten bei übernommenen Altdaten, Testdaten und Sicherungs-kopien erfüllt und kontrolliert?"**

Die entsprechenden Lösch- und Aufbewahrungskonzepte befinden sich bereits in Bearbeitung bzw. liegen schon vor, sodass die fachlichen und datenschutzrechtlichen Vorgaben zur Datenminimierung und Speicherbegrenzung strukturiert umgesetzt werden. Im laufenden Betrieb wie auch im Rahmen der Migration stützt sich die Umsetzung auf definierte Aufbewahrungsrichtlinien, die fachliche Prüfung der Erforderlichkeit von Altdaten sowie die vertraglichen Regelungen mit dem Auftragsverarbeiter: Nach der Vereinbarung zur Auftragsverarbeitung (AVV) kann der Verantwortliche jederzeit die Löschung oder Einschränkung der Verarbeitung verlangen, und bei Beendigung der Leistungen oder auf Aufforderung sind sämtliche Daten – ausdrücklich einschließlich erstellter Kopien sowie von Test- und Ausschussmaterial – zurückzugeben oder datenschutzgerecht zu vernichten und durch ein Löschprotokoll nachzuweisen. Auch für Sicherungskopien sehen die Unterlagen verbindliche vertragliche Vorgaben mit dem zertifizierten Hoster einschließlich festgelegter Löschfristen und regelmäßiger Wiederherstellungstests vor. Etwaige Mehrbedarfe beim Speichervolumen können im Vertrag flexibel im laufenden Betrieb angepasst werden, wobei durch die in Umsetzung befindlichen Löschkonzepte einer unnötigen Speicherung und damit verbundenen zusätzlichen Speicherkosten gezielt entgegengewirkt wird. Die Einhaltung und Kontrolle der Löschpflichten ist zudem durch die Rechenschaftspflicht des Auftragsverarbeiters, umfassende Prüf- und Einsichtsrechte (unter anderem für die Datenschutzbeauftragten) sowie die Nachweispflicht per Löschprotokoll abgesichert.

6. **„Welche Übergangslösung besteht, wenn erforderliche Nachweise nicht rechtzeitig vorliegen oder wesentliche Risiken nicht ausreichend behoben sind? Bitte stellen Sie die Möglichkeiten, Kosten und betrieblichen Folgen einer Verschiebung beziehungsweise einer befristeten Fortführung des bisherigen Verfahrens dar. Auf welcher verbindlichen Regelung beruht die im Dringlichkeitsschreiben genannte Förderfrist Ende November 2026? Wurde eine Verlängerung geprüft oder beantragt?"**

Eine Übergangslösung durch Verschiebung oder befristete Fortführung des bisherigen Verfahrens scheidet aus förderrechtlichen und zeitlichen Gründen aus. Maßgeblich ist die verbindliche Förderfrist des Sächsischen Staatsministeriums für Soziales, Gesundheit und Gesellschaftlichen Zusammenhalt (SMS), das die Abrechnung zum 30.11.2026 vornimmt; eine Verlängerung über diesen Zeitpunkt hinaus wurde geprüft und ausdrücklich abgelehnt. Jede Verzögerung oder längere Weiternutzung des Altsystems würde die fristgerechte Umsetzung und Abrechnung der Fördermittel gefährden. Sämtliche erforderlichen Nachweise sowie die Bewältigung wesentlicher Risiken müssen daher innerhalb des vorgegebenen Zeitrahmens realisiert werden.

7. **„Wie wird bei Datenschutz- oder Sicherheitsvorfällen im neuen Verfahren vorgegangen? Bitte erläutern Sie die Verantwortlichkeiten, Melde- und Reaktionsfristen, die Information betroffener Personen, die Wiederherstellung des Betriebs sowie die Finanzierung gegebenenfalls erforderlicher zusätzlicher Schutzmaßnahmen."**

...

Verantwortlichkeiten:
Die datenschutzrechtliche Verantwortung liegt bei der Landeshauptstadt Dresden. Die Deutsche Telekom Business Solutions GmbH handelt als Auftragsverarbeiter weisungsgebunden, unterstützt den Verantwortlichen bei der Einhaltung der Sicherheits- und Meldepflichten (insbesondere nach Art. 32 bis 34 DSGVO) und übernimmt im operativen Betrieb sowie über das Ticketsystem (Zammad) und definierte Supportprozesse die Störungsbearbeitung und Koordination mit weiteren Beteiligten wie easy-soft oder dem Service Desk der Open Telekom Cloud.

Melde- und Reaktionsfristen:
Nach der AVV ist der Auftragsverarbeiter verpflichtet, die Landeshauptstadt Dresden unverzüglich über schwerwiegende Betriebsstörungen, Verstöße gegen Datenschutzbestimmungen oder die AVV sowie sonstige Unregelmäßigkeiten bei der Datenverarbeitung zu unterrichten. Auch über Anfragen, Ermittlungen oder Kontrollen von Aufsichtsbehörden hat der Auftragsverarbeiter unverzüglich zu informieren. Meldungen an die Aufsichtsbehörde nach Art. 33 DSGVO erfolgen durch den Verantwortlichen bzw. durch den Auftragsverarbeiter ausschließlich nach vorheriger dokumentierter Weisung. Im Kriterienkatalog (Anlage 2) sind zudem Vorgaben zur zeitnahen Einspielung von Sicherheitspatches nach CVSS-Schweregrad aufgeführt (sofern vereinbart bzw. gemäß Anlage 1: kritisch innerhalb von 3 Stunden, hoch 3 Tage, mittel 1 Monat, niedrig 3 Monate).

Information betroffener Personen
Auskünfte oder Benachrichtigungen gegenüber betroffenen Personen oder Dritten – einschließlich einer etwaigen Benachrichtigung nach Art. 34 DSGVO bei einem Datenschutzverstoß – dürfen durch den Auftragsverarbeiter nur nach vorheriger ausdrücklicher Zustimmung bzw. dokumentierter Weisung der Landeshauptstadt Dresden erfolgen, soweit keine zwingende gesetzliche Herausgabepflicht besteht. Der Auftragsverarbeiter ist verpflichtet, die Landeshauptstadt Dresden bei der Erfüllung ihrer Pflichten aus Art. 34 DSGVO angemessen zu unterstützen und unmittelbar eingehende Betroffenenanfragen unverzüglich weiterzuleiten.

Wiederherstellung des Betriebs
Für die Wiederherstellung nach physischen oder technischen Zwischenfällen greifen ein vertraglich geregeltes Backup-Konzept (inklusive festgelegter Backup-Frequenz, Speicherort und regelmäßiger Wiederherstellungstests, u. a. eingebettet in das Notfallmanagement nach C5 OPS-08), ein Notfall- und Krisenmanagement (u. a. nach BSI-Standard bzw. Anlage 1) sowie definierte Support- und Eskalationswege über Zammad, Monitoring-Werkzeuge (Grafana/Domon) und die Supportprozesse von easy-soft und Open Telekom Cloud. Bei Serverneustarts oder Störungen ist im Betriebshandbuch zudem eine anlassbezogene, ticketgebundene und GPG-verschlüsselte Logfile-Bereitstellung zur Fehleranalyse vorgesehen.

Finanzierung gegebenenfalls erforderlicher zusätzlicher Schutzmaßnahmen
Ergibt eine Prüfung des Verantwortlichen einen Anpassungsbedarf bei den technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO, ist der Auftragsverarbeiter nach der AVV verpflichtet, diese Anpassungen umzusetzen und den Stand der Technik sowie Maßnahmen zur Schadensminderung zu gewährleisten. Nach § 11 der AVV sind sämtliche Leistungen des Auftragsverarbeiters im Rahmen der AVV (einschließlich Informationsbereitstellung und Unterstützung bei Prüfungen) grundsätzlich mit der vereinbarten Vergütung aus der Leistungsvereinbarung vollständig abgegolten. Gehen Leistungen oder gewünschte Anpassungen über den typischen vertraglichen Rahmen hinaus (etwa bei Sonderinspektionen oder erheblichem Mehraufwand außerhalb der vereinbarten Leistungen), greifen die Regelungen zur vorherigen Abstimmung und Ver-

gütung nach § 11 Abs. 2 AVV sowie das im EVB-IT Cloudvertrag vorgesehene Änderungsverfahren (Change Request / CR gemäß Anlage 1 Ziffer 5 und Anlage 4) bzw. das vereinbarte Abrufbudget.

Mit freundlichen Grüßen

i.V. Jan Thum

Dirk Hilbert