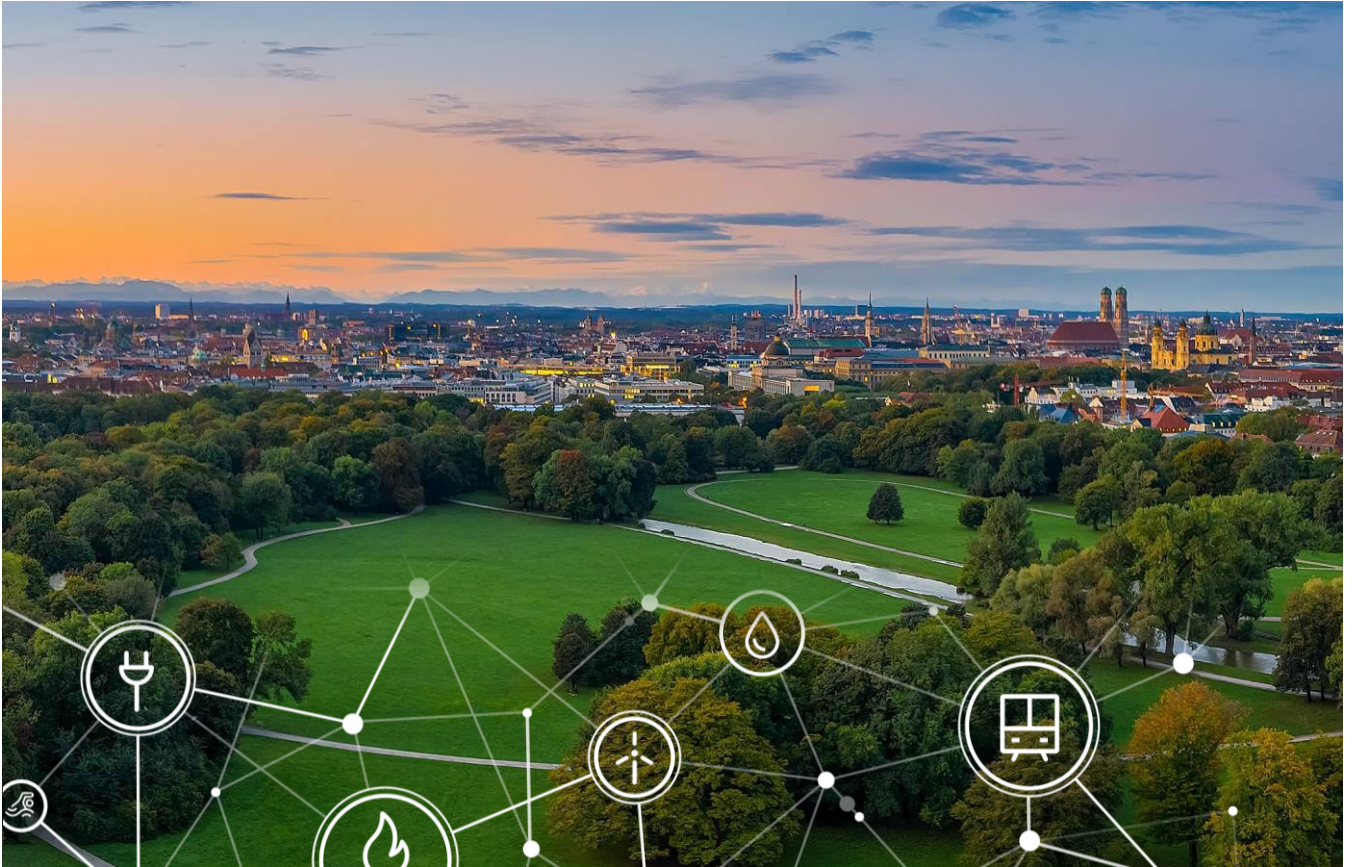




**Stellungnahme der Stadtwerke München GmbH
zum Beschluss der Bundesregierung für ein Gesetz zur Änderung
des Wärmeplanungsgesetzes (WPG)**

Lobbyregisternummer (national): R000611

I. Einleitung

Die Stadtwerke München (SWM) begrüßen grundsätzlich die Zielsetzung des Wärmeplanungsgesetzes (WPG), die kommunale Wärmeplanung zu vereinfachen, zu beschleunigen und auf eine belastbare Datengrundlage zu stellen. Gerade vor dem Hintergrund der notwendigen Transformation der Wärmeversorgung hin zu einer klimaneutralen Infrastruktur ist eine effiziente und praxisnahe Planung auf kommunaler Ebene von zentraler Bedeutung. Allerdings weist der vorliegende Gesetzentwurf aus Sicht der SWM erhebliche Defizite beim Umgang mit sensiblen Daten auf, insbesondere mit Betriebs- und Geschäftsgeheimnissen sowie Informationen zu kritischen Infrastrukturen (KRITIS).

Nachschärfungsbedarf besteht insbesondere bei folgenden Punkten:

Kernforderungen: Schutz kritischer Daten und Geschäftsgeheimnisse im Wärmeplanungsgesetz (WPG) stärken:

- **Der Gesetzentwurf verpflichtet Unternehmen nach § 11 Abs. 4 WPG zur Herausgabe auch hochsensibler KRITIS- und Geschäftsgeheimnisdaten, ohne ein wirksames Schutz- oder Verweigerungsrecht vorzusehen; die bloße Vertraulichkeitskennzeichnung und das Veröffentlichungsverbot bieten hierfür keinen ausreichenden Schutz.**
- **Die SWM fordern daher, dass solche Daten im Rahmen des § 11 WPG grundsätzlich nur aggregiert oder abstrahiert übermittelt werden dürfen und – sofern dies nicht möglich ist – ein ausdrückliches Recht zur Verweigerung der Datenübermittlung gesetzlich verankert wird.**

II. Fehlender Schutz kritischer Daten und Geschäftsgeheimnisse im Wärmeplanungsgesetz

Nach § 11 WPG sind Unternehmen und sonstige Akteure verpflichtet, umfangreiche Daten an die planungsverantwortlichen Stellen zu übermitteln. Diese Auskunftspflicht umfasst ausdrücklich auch solche Daten, die Betriebs- oder Geschäftsgeheimnisse betreffen oder als sicherheitsrelevante Informationen im Sinne des KRITIS-Dachgesetzes beziehungsweise der BSI-Kritisverordnung einzuordnen sind. Der Gesetzentwurf sieht dabei lediglich vor, dass entsprechende Daten von den Auskunftspflichtigen als vertraulich zu kennzeichnen sind und nicht veröffentlicht werden dürfen. Ein weitergehender Schutzmechanismus ist jedoch nicht vorgesehen. Insbesondere fehlt eine Regelung, die es den betroffenen Unternehmen ermöglicht, die Herausgabe besonders sensibler Daten zu verweigern, wenn deren Schutz nicht gewährleistet werden kann.

Diese Regelungslücke ist aus Sicht der SWM kritisch zu bewerten. Die bloße Kennzeichnung als vertraulich stellt keinen ausreichenden Schutz dar, da sie lediglich die Veröffentlichung der Daten untersagt, nicht jedoch deren interne Verfügbarkeit innerhalb der kommunalen Verwaltung einschränkt. In der Praxis bedeutet dies, dass potenziell eine Vielzahl von Mitarbeitenden Zugriff auf hochsensible Informationen erhalten kann, ohne dass hierfür klare, gesetzlich definierte Zugriffsbeschränkungen oder Sicherheitsanforderungen bestehen. Gerade im Bereich kritischer Infrastrukturen kann dies erhebliche Risiken für die Versorgungssicherheit sowie für die IT- und Datensicherheit mit sich bringen.

Hinzu kommt, dass der Gesetzentwurf die Möglichkeiten zur Weiterverarbeitung und Weitergabe der erhobenen Daten im Rahmen der Wärmeplanung und darüber hinaus ausweitet. In Kombination mit der fehlenden Differenzierung beim Schutz sensibler Informationen entsteht ein strukturelles Ungleichgewicht zwischen dem berechtigten Interesse an einer effizienten Datennutzung auf der einen Seite und dem ebenso wichtigen Schutz von Sicherheits- und Wettbewerbsinteressen auf der anderen Seite. Während der Gesetzgeber die Datentransparenz und -verfügbarkeit deutlich stärkt,

bleiben die Schutzmechanismen für besonders sensible Daten unzureichend ausgestaltet.

Positiv hervorzuheben ist, dass der Gesetzgeber eine Ausnahme für Liegenschaften der Bundeswehr und verbündeter Streitkräfte vorsieht. Diese Regelung erkennt grundsätzlich an, dass bestimmte Infrastrukturen eines besonderen Schutzes bedürfen. Allerdings ist diese Ausnahme aus Sicht der SWM sachlich zu eng gefasst, da auch Energieversorgungsinfrastrukturen zweifelsfrei zu den kritischen Infrastrukturen zählen und ein vergleichbares Schutzbedürfnis aufweisen.

Vor diesem Hintergrund sehen die SWM dringenden gesetzgeberischen Handlungsbedarf. Ein zentraler Ansatzpunkt ist die Einführung eines abgestuften Systems zur Datenbereitstellung. Sensible Daten, insbesondere solche mit Bezug zu kritischen Infrastrukturen oder Geschäftsgeheimnissen, sollten grundsätzlich nur in aggregierter oder abstrahierter Form übermittelt werden. Dies kann beispielsweise durch die Zusammenfassung von Daten, die Entfernung identifizierbarer Einzelinformationen oder die Darstellung auf einer übergeordneten Ebene erfolgen. Auf diese Weise kann der Informationsbedarf der planungsverantwortlichen Stellen gedeckt werden, ohne die Sicherheits- und Wettbewerbsinteressen der Unternehmen zu gefährden.

Sollte eine solche Aggregation oder Abstraktion im Einzelfall nicht möglich sein, muss es den betroffenen Unternehmen ermöglicht werden, die Herausgabe dieser Daten zu verweigern. Voraussetzung hierfür sollte eine nachvollziehbare Begründung sein, etwa wenn konkrete Sicherheitsrisiken bestehen oder Geschäftsgeheimnisse nicht ausreichend geschützt werden können. Eine entsprechende Klarstellung im Gesetz würde zu mehr Rechtssicherheit führen und zugleich das notwendige Vertrauen der betroffenen Akteure in den Prozess der Wärmeplanung stärken.

Darüber hinaus sollten die Anforderungen an den Umgang mit vertraulichen Daten auf Seiten der planungsverantwortlichen Stellen deutlich präzisiert werden. Dazu gehört insbesondere eine klare Begrenzung des Zugriffs auf einen eng definierten Personenkreis, die verpflichtende Protokollierung von Zugriffen sowie die Einhaltung hoher IT-Sicherheitsstandards, die sich an bestehenden KRITIS-Vorgaben orientieren. Nur so kann gewährleistet werden, dass sensible Daten nicht unkontrolliert innerhalb von Verwaltungen zirkulieren.

Zusammenfassend lässt sich feststellen, dass der vorliegende Gesetzentwurf in seiner aktuellen Form zwar einen wichtigen Beitrag zur Beschleunigung und Verbesserung der Wärmeplanung leisten kann, jedoch im Bereich des Datenschutzes und der Datensicherheit erhebliche Nachbesserungen erforderlich sind. Aus Sicht der SWM ist es zwingend notwendig, dass die verpflichtende Übermittlung von Daten nicht zu Lasten des Schutzes kritischer Infrastrukturen und von Geschäftsgeheimnissen geht. Der Gesetzgeber sollte daher klare Regelungen schaffen, die sicherstellen, dass sensible Daten entweder nur in geeigneter Form an berechnigte Stellen bereitgestellt werden oder deren Herausgabe in begründeten Fällen verweigert werden kann. Nur so lässt sich ein ausgewogenes Verhältnis zwischen Planungsanforderungen und Sicherheitsinteressen erreichen.

Formulierungsvorschlag für Gesetzestext – Ergänzung in § 11 WPG (neu):

„Die Verpflichtung zur Auskunftserteilung entfällt, soweit die übermittelten Daten

1. Betriebs- oder Geschäftsgeheimnisse betreffen oder
2. Informationen über kritische Infrastrukturen enthalten, und eine Weitergabe nicht in angemessen aggregierter oder abstrahierter Form möglich ist.

In diesen Fällen ist die Verweigerung der Auskunft auf Antrag zulässig und zu begründen.“

Konkret schlagen wir vor, um einen effektiven Schutz von KRITIS-Daten und Geschäftsgeheimnissen gesetzlich abzusichern:

- **Einführung eines abgestuften Datenzugangssystems**
 - Verpflichtende Bereitstellung sensibler Daten nur
 - aggregiert oder
 - abstrakt (z. B. geclustert/entpersonalisiert)
 - Nur wenn dies technisch nicht möglich ist:
 - Einzelfallprüfung mit Begründungspflicht
 - Möglichkeit zur Verweigerung der Datenübermittlung
- **Klarstellung eines Verweigerungsrechts durch Ergänzung in § 11 WPG:**
 - Auskunftspflicht besteht nicht, wenn
 - erhebliche Sicherheitsinteressen betroffen sind oder
 - Geschäftsgeheimnisse nicht ausreichend geschützt werden können
- **Stärkung des Zugriffsschutzes**
 - Zusätzliche Anforderungen:
 - Beschränkung des internen Zugriffs auf definierte Stellen
 - Protokollierung sämtlicher Zugriffe
 - IT-Sicherheitsstandards analog KRITIS-Anforderungen
- **Erweiterung der Ausnahmeregelung**
 - Gleichstellung von KRITIS-Infrastrukturen mit militärischen Einrichtungen
 - Ausnahmetatbestand für
 - Energieversorgungsnetze
 - kritische Anlagen
 - sicherheitsrelevante Betriebsdaten