

Herrn
Mag. Johannes Gungl
Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)
Mariahilfer Straße 77-79
1060 Wien

Ihr Zeichen / Ihre Nachricht von

Unser Zeichen
Gri

DW
31

Datum
18.10.2016

Stellungnahme des Fachverbands der Gas- und Wärmeversorgungsunternehmen zum Entwurf einer Verordnung der RTR-GmbH über die Abfrage von Daten aus der Zentralen Informationsstelle für Infrastruktur der RTR-GmbH – ZIS-AbfrageV

Sehr geehrter Herr Mag. Gungl,

zum o.a. Entwurf dürfen wir wie folgt Stellung nehmen:

Die FGW-Mitgliedsunternehmen gehen davon aus, dass weite Teile der von ihnen betriebenen Infrastruktur, soweit sie durch die ZIS-EinmeldeV sowie AbfrageV betroffen ist, als kritische Infrastruktur im Sinne dieses Begriffes zu verstehen ist.

Daher führen wir, wie schon bereits in unserer Stellungnahme zur Telekommunikationsgesetz-Novelle sowie zur ZIS-EinmeldeV wie folgt aus:

Im Allgemeinen

Gemäß Art 3 und 4 der RL 2014/61/EU und der TKG-Novelle ist sowohl die Datenbereitstellungspflicht als auch die Netzzugangspflicht umfassend gestaltet und wird nur unter bestimmten Voraussetzungen eingeschränkt. Als Ausnahme einer bestehenden umfassenden Verpflichtung sind diese Fälle dogmatisch daher eng auszulegen und bedürfen einer detaillierten Rechtfertigung. Diese wird nach der Richtlinie nur sehr allgemein im Fall der Betroffenheit von "kritischer Infrastruktur" gesehen, das TKG bleibt in diesem Punkt sogar hinter der Richtlinie zurück, indem darin keine klare Definition des Begriffes „kritische Infrastruktur“ vorgesehen ist. Gleichzeitig müssen wir wiederholt auf die Ausführungen zur kritischen Infrastruktur im Masterplan APCIP 2014 verweisen.

Als größter Mangel der TKG-Novelle und damit auch der ZIS-EinmeldeV sowie der ZIS-AbfrageV ist mit Nachdruck hervorzuheben, dass der denkbare Schutz durch Wahrung von Vertraulichkeit von Informationen und Vermeidung des Netzzutritts sogar hinter der Definition der Richtlinie zurückbleibt und eine Auseinandersetzung mit dem Begriff „kritische Infrastruktur“ in jeder Weise unterbleibt.

Unsere dringende Forderung nach einer angemessenen Definition über Vorliegen oder Nichtvorliegen von "kritischer Infrastruktur" bleibt auch weiterhin aufrecht. In der vorliegenden ZIS-AbfrageV bleibt der Begriff der „kritischen Infrastruktur“ indeterminiert, vielmehr wird der neue Begriff der „sensiblen Infrastruktur“ eingeführt, der zu weiteren Unklarheiten führt.

Im Besonderen

ad § 1

Es wird zwar auf den Stand der Technik verwiesen, allerdings sollten die Sicherheitsmaßnahmen selbst noch konkretisiert werden. Weiters ist anzumerken, dass sich der Stand der Technik laufend ändert, und daher müssen von einer entsprechenden Instanz die zu implementierenden Sicherheitsmaßnahmen festgelegt und deren korrekte Implementierung überprüft werden. Der Einsatz von TLS 1.2 für die Datenübertragung ist nur eine Maßnahme von vielen.

Folgende Themen sollten unter anderem noch adressiert werden:

- Sichere Speicherung der Daten – Die Vertraulichkeit und Integrität der gespeicherten Daten muss mittels geeigneter kryptografischer Methoden gewährleistet werden (z.B. mittels Verschlüsselung und Ablage entsprechender Prüfsummen).
- Sicherstellung, dass nur definierte Applikationen Zugriff auf die gespeicherten Daten haben (Netzwerkzugriff muss authentifiziert werden) · Absicherung des Frontends, über welches der Zugriff auf die Datenbank etabliert wird (z.B. bei einem Web-Frontend Beachtung der ÖNORM A7700, Beachtung OWASP Empfehlungen,...).

ad § 2

Gem § 2 Abs 2 sind Abfrageberechtigte ausschließlich Bereitsteller eines öffentlichen Kommunikationsnetzes. Aus unserer Sicht ist es unklar, ob der Begriff Bereitsteller eines öffentlichen Kommunikationsnetzes im Sinne des TKG auch den „Anbieter von öffentlichen Mietleitungsdiensten“ (als solcher bei der RTR gelistet) umfasst, wenn ja sollte eine diesbezügliche Klarstellung erfolgen. Weiters unklar ist, ob sonstige Einmeldeverpflichtete, welche nicht als Bereitsteller eines öffentlichen Kommunikationsnetzes im Sinne des TKG bzw. als Anbieter von öffentlichen Mietleitungsdiensten auftreten, abfrageberechtigt sind.

§ 2 Abs 3 sieht nach Beantragung eine unbefristete Abfrageberechtigung vor. Dies halten wir für kritisch, insbesondere in Hinblick auf die Absicherung der Wahrung der Vertraulichkeit der zugänglich gemachten Daten. Bevollmächtigungen sollten nur befristet auf ein Kalenderjahr beantragt werden können. Gleichzeitig ist neben dem Nachweis der Bevollmächtigung der Bevollmächtigte auch zur Wahrung der Vertraulichkeit im Sinne des § 48 Abs. 2 TKG zu verpflichten. Wir schlagen daher folgende Änderungen für Abs 3 vor:

„(3) Abfrageberechtigte haben jeweils befristet für ein Kalenderjahr die Erteilung von Zugängen zum ZIS-Abfrage-Portal für jede Person, die für sie Daten abfragen soll (Zugangsberechtigte), schriftlich bei der RTR-GmbH zu beantragen. Die Bevollmächtigung zur Datenabfrage ist der RTR-GmbH nachzuweisen und die Zugangsberechtigten sind nachweislich zur Wahrung der Vertraulichkeit im Sinne des § 48 Abs. 2 TKG zu verpflichten.“

Laut Gesetzgeber besteht das intendierte Ziel der Zentralen Informationsstelle darin, Erleichterungen beim Ausbau von Hochgeschwindigkeitsnetzen zu schaffen, in dem die Nutzung bestehender physischer Infrastruktur gefördert und ein effizienter Ausbau physischer Infrastruktur ermöglicht wird. Dabei ist die bestimmungs-gemäße Nutzung der abgefragten Daten sicherzustellen. Sämtliche Zugriffe (auch interne) auf die gespeicherten Informationen müssen lückenlos protokolliert werden, sodass nachvollziehbar und auswertbar ist, wer wann auf welche Informationen zugegriffen hat.

Im aktuellen Verordnungsentwurf befindet sich kein Hinweis zum Verwendungszweck der abgerufenen Daten. Es ist daher jedenfalls in der Verordnung festzuhalten, dass die gelieferten Daten ausschließlich für den gesetzlich vorgesehenen Zweck verwendet werden dürfen. Um zu verhindern, dass Antragssteller die übermittelten Daten für andere Zwecke (z.B.: Weitergabe an Dritte, etc.) nutzen oder kommerziell verwerten, schlagen wir vor, die Regelung in § 2 mit einem Abs 5 (neu) wie folgt zu ergänzen:

„(5) Die abgefragten Daten aus dem ZIS-Abfrage-Portal sind vom Abfrageberechtigten ausschließlich für den gesetzlich vorgesehenen Zweck und das in der Antragstellung gemäß § 4 Abs 1 beschriebene Vorhaben zu nutzen. Eine entgeltliche oder unentgeltliche Weitergabe der abgefragten Daten an Dritte ist nicht zulässig.“

ad § 3

Gemäß § 3 Abs 1 des Entwurfes der ZIS AbfrageV hat die RTR bei eingemeldeten geplanten Bauvorhaben gemäß § 13a Abs 4 TKG 2003 den Standort des Bauvorhabens, das Datum der Einmeldung sowie eine eindeutige Identifikationsreferenz in eine Liste aufzunehmen, die für am ZIS-Abfrage-Portal gemäß Abs 1 legitimierte Zugangsberechtigte einsehbar zu sein hat.

Durch die angeführte Bestimmung soll für alle legitimierte Zugangsberechtigten ohne weiteres Erfordernis, insbesondere ohne Glaubhaftmachung der Gründe für die Einsehbarkeit (wie sie § 4 vorsieht) die Möglichkeit zur Einsichtnahme in eine „Liste“ geschaffen werden.

Damit werden jedoch „strategische Abfragen“ ermöglicht, die ohne Bezug auf ein konkretes Projekt vorgenommen werden können. Auch steht durch die Implementierung einer „Liste“ die Gefahr der Schaffung eines Datenfriedhofes im Raum, weil zusätzliche Daten zu verwalten sind, dies jedoch ohne Schaffung eines Mehrwertes iS des TKG.

Die geplante „Aufweichung“ der Qualitätsstandards ist jedenfalls abzulehnen und es wird die Streichung des § 3 Abs 3 gefordert, da ohnehin durch § 4 die Standards für die Einsichtnahme geregelt werden. Eine diesbezügliche „Aufweichung“ mittels „nicht zu begründender Einsichtnahme in eine Liste“ ist im Übrigen weder dem Gesetz noch der ZIS-EinmeldeV zu entnehmen.

ad § 4

In Abs 1 sollte die „für Kommunikationslinien nutzbare Infrastruktur“ durch Verweis auf die Definition des § 3 Z 29 TKG 2003 und die in der ZIS-EinmeldeV normierten Ausnahmen konkretisiert werden.

Gemäß § 4 Abs 1 Z 1 des Entwurfes der ZIS AbfrageV ist im Zuge der Glaubhaftmachung „das Vorhaben zu beschreiben, im Rahmen dessen eine Mitbenützung abgestrebt wird“.

Wir sind der Meinung, dass diese Anforderung zu kurz greift. Um bereits im Vorhinein zu verhindern, dass sog. Scheinabfragen (Abfragen ohne realen wirtschaftlichen Background) durchgeführt werden, sollte der Passus wie folgt ergänzt werden:

„Dabei sind jedenfalls

1. das technisch und wirtschaftlich begründete Vorhaben zu beschreiben, im Rahmen dessen eine Mitbenutzung angestrebt wird, ...“

Damit wäre im Übrigen auch der RTR gedient, weil dem Antragsteller schon im Vorhinein klar sein muss, dass an die Glaubhaftmachung konkrete Erforderniskriterien geknüpft sind, die die Umsetzung des Vorhabens sowohl in technischer als auch in wirtschaftlicher Hinsicht möglich erscheinen lassen.

In § 4 Abs 1 Z 2 wird das Abfragegebiet mit 420 Rasterzellen in beliebig kombinierbaren quadratischen Rastergrößen angegeben, wobei die Rastergrößen von „500, 1.000 und 5.000 Metern“ ein Irrtum sein dürfte, da zu großflächig.

Gemäß § 4 Abs 4 Z 3 der ZIS-AbfrageV hat die RTR-GmbH die nach § 4 Abs 1 übermittelten Angaben und Unterlagen unverzüglich zu prüfen und gegebenenfalls den Antragsteller zu verständigen, dass die beantragten Informationen im Abfragegebiet bereits in elektronischer Form öffentlich zugänglich gemacht wurden. Hier stellt sich die Frage, wie diese öffentliche Zugänglichkeit definiert wird. Weiters ist in § 6b TKG 2003 normiert, dass die zentrale Informationsstelle den Berechtigten darüber informieren muss, WO die beantragten Mindestinformationen in elektronischer Form öffentlich zugänglich gemacht wurden. Im derzeitigen Entwurf der ZIS-AbfrageV ist aber nur vorgesehen, dass der Betroffene nur darüber informiert wird, DASS die Informationen öffentlich zugänglich sind. Dies sollte aus unserer Sicht noch korrigiert werden.

ad § 5

Überschrift des Kapitels **Sensible Infrastrukturen**:

Hier dürfte insofern ein Missverständnis vorliegen, als die Bezeichnung „sensible Infrastrukturen“ tatsächlich weder im Gesetz noch in der ZIS-Einmeldeverordnung abgebildet ist. Der Begriff „sensibel“ ist z.B. in den Materialien zum TKG lediglich auf „Informationen“ bezogen (siehe z.B. Erläuterungen zu §§ 6a und 6b TKG). Gemeint war hier wohl richtigerweise, dass bei der Antragstellung auch anzugeben ist, ob die Zugänglichmachung zu „besonders sensiblen Informationen“ gewünscht ist. Aber dies trifft eben nicht mehr den Kern der Sache, weil die Begrifflichkeit nicht im Kontext mit den umgebenden Bestimmungen steht. Wir ersuchen daher, sowohl in der Bezeichnung des § 5 als auch in dessen Abs 1 den korrekten Terminus „kritische Infrastrukturen“ aufzunehmen (wie bereits oben erwähnt), weil nur diese von den Einmeldepflichtigen auch als solche bezeichnet werden und somit nur diese Gegenstand einer bescheidmäßigen Erledigung sein können.

Gemäß § 5 Abs 1 hat der Antragssteller bekanntzugeben, ob Informationen von „sensiblen Infrastrukturen“ auch zugänglich gemacht werden sollen. Hier ist eine Ja/Nein-Angabe nicht ausreichend. Der Antragsteller sollte auch eine Begründung angeben, warum solche Informationen in diesem Fall von Relevanz sind. Wir schlagen daher folgende Ergänzung vor:

„§5 (1) Der Antragsteller hat bei jeder Antragsstellung gemäß § 4 Abs. 1 oder Abs. 2 bekanntzugeben und zu begründen, ob auch die Zugänglichmachung ...“

Wird gem § 5 Abs 3 vom Antragsteller die Zugänglichmachung von Informationen über „sensible“ Infrastrukturen nicht beantragt, hat die RTR-GmbH den Antragsteller ausschließlich darüber zu informieren, welche Einmeldeverpflichteten Standorte, Leitungswege oder Netzkomponenten gemäß § 3 Abs. 5 ZIS-EinmeldeV als „sensibel“ markiert haben. Hier sollte aus unserer Sicht noch klargestellt werden, dass nur die Einmeldeverpflichteten bekanntgegeben werden, die im Abfragegebiet Standorte, Leitungswege oder Netzkomponenten als sensibel markiert haben.

Im Übrigen ist die Regelung nicht nachvollziehbar: wenn eine Zugänglichmachung von Informationen über „sensible“ Infrastrukturen durch einen Antragsteller nicht beantragt werden, sollte es auch keine weiteren Informationen diesbezüglich geben. Es ist nicht nachvollziehbar, warum ein solcher Antragsteller dann - obwohl eben Informationen über „sensible“ Infrastrukturen nicht beantragt wurden - Informationen darüber bekommt, welche Einmeldeverpflichteten „sensible“ Infrastrukturen in diesem Bereich gemeldet haben.

ad § 6

Gemäß § 6 Abs 4 ZIS-AbfrageV hat die RTR-GmbH den Antragsteller darüber zu verständigen, dass die beantragten Informationen zum Abruf bereitgehalten werden. Zum Abruf der bereitgehaltenen Plandarstellungen hat sich ein Zugangsberechtigter zu legitimieren. Hier sollte aus unserer Sicht klargestellt werden, dass die beantragten Informationen nur über das ZIS-Portal abgerufen werden können und zwar nur von demjenigen Legitimierten, der den Antrag gestellt hat. Falls eine Versendung der Daten per E-Mail auch als "Abfrage" zulässig ist, sollte diese Versendung der Daten per E-Mail entsprechend dem Sicherheitshandbuch (siehe Anmerkungen zu § 1) jedenfalls mindestens mit TLS-Verschlüsselung und mit Signatur erfolgen. Wir schlagen daher folgende Änderung vor:

„(4) Die RTR-GmbH hat den jeweils legitimierten Antragsteller zu verständigen, dass die Daten gemäß Abs. 3 zum Abruf über das ZIS-Portal bereitgehalten werden. Zum Abruf der im ZIS-Portal bereitgehaltenen Plandarstellungen hat sich ein Zugangsberechtigter gemäß § 3 zu legitimieren. Die RTR-GmbH hat den Abruf von gemäß Abs. 3 im ZIS-Portal bereit gehaltenen Daten zu protokollieren.“

ad § 7

Im aktuellen Verordnungsentwurf ist gemäß § 7 lediglich festgehalten, dass die Einmeldeverpflichteten binnen zwei Wochen ab Zugänglichmachung der Daten über die Identität des Antragstellers, über das Abfragegebiet und gegebenenfalls über den Detaillierungsgrad verständigt werden.

Da es sich bei der Zugänglichmachung letztlich um einen Eingriff in das Eigentumsrecht der Einmeldeverpflichteten und um eine Weitergabe von relevanten Unternehmensinformationen an Dritte handelt, ist aus unserer Sicht eine unverzügliche Verständigung an die Einmeldeverpflichteten bereits bei Abfragen der Daten (Antragstellung) und zusätzlich auch unverzüglich im Fall der Zugänglichmachung vorzusehen. Aufgrund des automatisierten Prozesses und der elektronischen Übermittlung ist die derzeit vorgesehene Regelung im Verordnungsentwurf, die eine Frist von längstens zwei Wochen ab Zugänglichmachung und ein Ausbleiben der Verständigung zum Zeitpunkt der Abfrage vorsieht, nicht nachvollziehbar. Gerade durch den automatisierten Prozess ist eine unverzügliche Verständigung der

Einmeldeverpflichteten bei Antragstellung und Zugänglichmachung umsetzbar. Daher schlagen wir folgende Änderungen in § 7 Abs 1 vor:

„Die RTR-GmbH hat die Einmeldeverpflichteten gemäß § 1 ZIS-EinmeldeV, deren Daten gemäß § 4 Gegenstand einer Antragstellung sind oder gemäß § 6 einem Antragsteller zugänglich gemacht wurden, unverzüglich, längstens aber binnen zwei Wochen ab dem Zeitpunkt der Zugänglichmachung, über die Identität des Antragstellers, über das Abfragegebiet und gegebenenfalls über den Detaillierungsgrad gemäß § 6 Abs. 1, in dem Informationen über Infrastrukturen zugänglich gemacht wurden, zu verständigen.“

Abschließend halten wir fest, dass es für unsere Mitglieder von zentraler Bedeutung ist, dass Informationen über sog. „sensible“ Infrastruktur auch weiterhin im höchst möglichen Ausmaß geschützt werden müssen, um diese auch weiterhin vor mutwilliger Zerstörung zu schützen. In den Risikoanalysen der Netzbetreiber wird das Risiko von Sabotage/Terror große Bedeutung eingeräumt. Höchste Geheimhaltung stellt aus unserer Sicht eine besonders wirksame Risikominderungsmaßnahme dar.

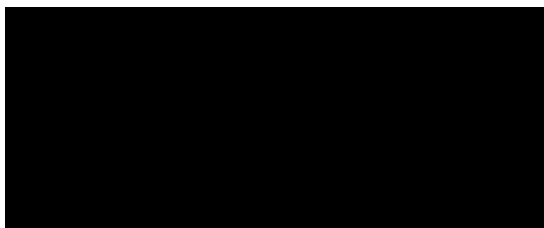
Die Zugänglichkeit von Daten in einem zentralen österreichweiten Register stellt ein klares Ziel für Angreifer dar. Entsprechende Vorkehrungen sind daher zu treffen, dass solche Daten vertraulich und mit größter Sorgfalt behandelt werden. Generell sollte daher der Umgang mit den Daten durch eine zwingend vom Antragsteller zu unterfertigende Vertraulichkeitserklärung sichergestellt werden, welche vor Bekanntgabe der Daten dem Einmeldeverpflichteten zu übermitteln ist (siehe auch Anmerkung zu § 2). Diese Vertraulichkeitserklärung sollte auch die Pflicht des Antragstellers, die Daten vor unberechtigten Zugriff Dritter zu schützen beinhalten.

Zudem sollten Maßnahmen bei Handlungen eines nicht den Erfordernissen entsprechenden Umganges mit den Informationen oder einer widerrechtlichen Nutzung der Informationen festgelegt werden:

1. Entzug der Abfrageberechtigung bei Verstoß gegen das Informationsgeheimnis sensibler Daten.
2. Überprüfung der Datenhaltung des Zugangsberechtigten durch die Behörde bei Verdacht auf nicht den Anforderungen entsprechenden Umgang der erhaltenen Daten.

Wir ersuchen um Berücksichtigung unserer Kommentare und stehen für Rückfragen sehr gerne zur Verfügung.

Freundliche Grüße,



Referentin Wärme