.BVT
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG

MR MAG. SIEGFRIED GRILL, MPA
BUNDESMINISTERIUM FÜR INNERES
Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung
Abteilung II/BVT/3
TEL +43-1 53126/4239
Mobil +43-664 8168902
Siegfried.grill@bvt.gv.at
SKI@bvt.gv.at

An die

Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77-79
1060 Wien

Per E-Mail an: ZIS@rtr.at

Schutz kritischer Infrastruktur, ZIS-AbfrageV, Begutachtung

Sehr geehrte Damen und Herren,

das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) bedankt sich für die Gelegenheit, zum vorliegenden Entwurf einer Verordnung zum Telekommunikationsgesetz wie folgt Stellung nehmen zu dürfen.

Grundsätzliches:

In Umsetzung des EU-Rechtsaktes in Form der Richtlinie 2008/114/EG, über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen (ECI) und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, nimmt Österreich sowohl an dem daraus resultierenden EPCIP als auch am nationalen Masterplan APCIP, teil.

Der sich daraus klar ergebende gesamtstaatliche Auftrag zur Steigerung der Resilienz der identifizierten kritischen Infrastrukturen in Österreich, ist sowohl in der von der Bundesregierung beschlossenen ÖSCS (Österreichische Strategie für Cyber-Sicherheit), als auch in der vom Nationalrat am 03.07.2013 verabschiedeten ÖSS (Österreichische Sicherheitsstrategie) definiert und findet sich darüber hinaus als prioritärer Bestandteil im Regierungsübereinkommen 2013.

Das BVT ist für die operative Gewährleistung der festgelegten Schutzziele verantwortlich und hat gemeinsam mit dem Bundeskanzleramt (BKA) etwa 400 Unternehmen als „kritische Infrastruktur“ definiert und klassifiziert, welche für die Gesellschaft einen essentiellen Beitrag zur Daseinsvorsorge leisten, oder eine sonstige Versorgungsleistung innehaben, die für eine funktionierende Gesellschaft unabdingbar ist.

In diesem Kontext möchten wir auf unseren gesetzlichen Auftrag verweisen, der seine kongruenten Verpflichtungen, Maßnahmen und Kompetenzen sowohl im PStSG (Polizeiliches Staatsschutzgesetz), als auch im SPG (Sicherheitspolizeigesetz), definiert hat.

Nahezu alle schutzwürdigen Sektoren der kritischen Infrastruktur weisen starke Interdependenzen auf und sind von den Auswirkungen der geplanten AbfrageV direkt betroffen. Insbesondere die Energieversorgungs- und die Cyber-Sicherheit stellen jedoch

darüber hinaus jene Bereiche dar, denen ein besonders großer Stellenwert beigemessen wird und welche von einem objektiv sehr hohen Schutzbedürfnis geprägt sind.

Die Geheimhaltung von objektspezifischen Daten kritischer Infrastrukturen stellt eine bewährte und wirksame Schutzmaßnahme für die Gesellschaft dar und ist geeignet, die Risiken hinsichtlich Sabotage, Terrorismus und sonstigen kriminellen Handlungen und einer damit einhergehenden Gefahr für die öffentliche Sicherheit zu mindern.

Aus diesem Grund wird die geplante Einmelde-Verpflichtung von Infrastrukturdaten im Zusammenhang mit der Speicherung dieser Daten und der Weitergabe an Dritte im Allgemeinen als widersprüchlich zur oben angeführten EU-RL zum Schutz kritischer Infrastruktur angesehen.

Zu § 5 Absatz 3 AbfrageV – Sensible Daten

Hat ein Antragsteller keine Zugänglichmachung von als „sensibel“ markierten Informationen gem. Abs. 1 beantragt, sollte er auch keine diesbezüglichen Informationen erhalten, wenngleich es sich nur um die Information handelt, welcher „Einmeldeverpflichtete“ dort eine sensible Infrastruktur betreibt. Dieser Absatz sollte daher entsprechend abgeändert werden.

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

Wien, am 20.10.2016

MR Mag. Günter POßEGGER

Abteilungsleiter
Bundesamt für Verfassungsschutz und
Terrorismusbekämpfung