

Energie-Control Austria für die Regulierung der Elektrizitäts-, Gas- und Wasserstoffwirtschaft (E-Control)
Rudolfsplatz 13a, 1010 Wien
E-Mail: recht-post@e-control.at

Stellungnahme zur IMA-V 2026 der Technologieplattform Smart Grids Austria

Die Technologieplattform Smart Grids Austria ist das Netzwerk aus Energiewirtschaft, Industrie, Forschung und öffentlichen Stellen, welches die wesentlichen Akteure zur Gestaltung der des Energiesystems der Zukunft vereint.

Die TP SGA begrüßt die IMA-V 2026 als wichtige Maßnahme für ein sicheres und effizientes Energiesystems, da es starke, leistungsfähige und digitale Netze für die Energiewende braucht. Dennoch möchten wir mit unserer Stellungnahme zur IMA-V 2026 auf Unklarheiten und notwendige Klarstellungen aufmerksam machen. Wesentliche Punkte sind die Speicherung und Fristen.

§ 2 und § 4

Im Entwurf der **IMA-V 2026** wird der **Anwendungsbereich** in **§ 2** dahingehend festgelegt, dass die Anforderungen auch jene intelligenten Messgeräte betreffen, „mit denen Endkunden auszustatten sind“, womit – wie in den Erläuterungen ausdrücklich ausgeführt – die **Einführungspflicht nun auch Zählpunkte umfasst, die bisher mit Lastprofilzählern ausgestattet sind**.

Gleichzeitig sieht **§ 4 Abs. 1** ein **Inkrafttreten mit 1. Juli 2026** vor; **§ 4 Abs. 2** knüpft die Anwendbarkeit der neuen Anforderungen an Vergaben, die nach Inkrafttreten abgeschlossen werden, ohne jedoch **für den neu einbezogenen Teilbereich „Lastprofilzähler“ eine spezifische Übergangs- bzw. Implementierungsphase** vorzusehen.

Aus Sicht der Praxis ist diese unmittelbare Wirksamkeit für die neu erfassten Lastprofil-Zählpunkte **nicht realistisch**: Der Entwurf verlangt unter **§ 3 Z 10** explizit, dass Messgeräte und Kommunikation „nach anerkanntem Stand der Technik abzusichern und zu verschlüsseln“ sind, einschließlich individueller Schlüssel für die Kommunikation (auch zu externen Geräten). Diese Anforderungen haben unmittelbare Auswirkungen auf **Hardware-/Firmware-Architektur, Schlüsselmanagement, Update-Mechanismen und**

Disclaimer: Wir möchten darauf hinweisen, dass die Mitglieder „E-Control“ und „BMIMI“ in der vorliegenden Stellungnahme der Technologieplattform Smart Grids Austria zur IMA-V 2026 nicht mitgewirkt und sich enthalten haben. Weiters widerspiegelt diese Stellungnahme die kollektive Ansicht eines Großteils unserer Mitglieder, jedoch möchten wir darauf hinweisen, dass nicht alle Punkte zwangsläufig mit sämtlichen individuellen Meinungen übereinstimmen.

Sicherheitsnachweise und erfordern bei Herstellern typischerweise **Entwicklungs-, Test- und Qualifikationszeiten** (insbesondere für Security-Anpassungen) sowie entsprechende Produkt- und Zertifizierungszyklen.

Anpassungsvorschlag:

Zur Sicherstellung der Umsetzbarkeit und zur Vermeidung von Beschaffungs- und Rollout-Risiken wird angeregt, in **§ 4** eine **explizite Übergangsregelung für Zählpunkte mit (bisherigen) Lastprofilzählern** aufzunehmen (z. B. gestaffeltes Inkrafttreten bzw. Übergangsfrist für die Anwendung der neuen Geräteanforderungen bei diesen Zählpunkten), sodass Herstellern und Marktteilnehmern ausreichend Zeit für **produktseitige Security-Adaptierungen** und die geordnete Markteinführung konformer Geräte zur Verfügung steht.

Damit würde die Zielsetzung des Entwurfs (technische Mindestfunktionalitäten und Sicherheitsanforderungen) gewahrt, ohne die praktische Beschaffbarkeit und fristgerechte Umsetzung ab **1.7.2026** für den neu erweiterten Anwendungsbereich zu gefährden.

§ 3 Z 6

§ 3 Z 6 IMA-V 2026 verlangt die Speicherung viertelstündlicher Messwerte für **jedenfalls 60 Kalendertage**. In den Erläuterungen wird klargestellt, dass nach Ablauf dieses Zeitraums die **ältesten Werte automatisch durch neue Werte ersetzt werden**, womit eine **rollierende Speicherung** vorgesehen ist.

Aus unserer Sicht zielt diese Regelung primär auf die Sichtanzeige (Display) sowie auf die zugängliche Darstellung der Messwerte ab und nicht auf eine zwingende Begrenzung der **physikalischen Speicherkapazität** im Messgerät. Maßgeblich ist, dass für den Endkunden bzw. über die bestimmungsgemäßen Anzeige- und Zugriffsmöglichkeiten höchstens Messwerte ab dem Installationszeitpunkt bzw. maximal für die letzten 60 Kalendertage darstellbar sind.

Anpassungsvorschlag:

Aus technischer Sicht wäre es daher ausreichend, festzulegen, dass eine **physikalische Speicherung von Messwerten über 60 Kalendertage hinaus zulässig** ist, sofern sichergestellt ist, dass die **Darstellung der Messwerte am Display zeitlich auf den Installationszeitpunkt bzw. auf maximal 60 Kalendertage begrenzt** ist. Dies würde eine höhere technische Flexibilität für die Hersteller ermöglichen, während das Regelungsziel des § 3 Z 6 IMA-V 2026 unverändert und vollumfänglich erreicht wird.

Weiters wird im letzten Satz angeführt, dass „Die Geräte müssen weiters gewährleisten, dass im Falle eines Ausfalls der Versorgungsspannung alle Daten so lange erhalten bleiben, dass eine lückenlose Rekonstruktion möglich ist.“

Anpassungsvorschlag: Ergänzung einer Frist **von mindestens 60 Tagen**. Da dies den angeführten Anforderungen §3 Z 6 entspricht und eine unbegrenzte Speicherdauer nicht gewährleistet werden kann.

§ 3 Z 09

„Die Kundenschnittstelle muss eine Spannungsversorgung für die Datenauslesung und -übermittlung an den Empfänger bereitstellen können.“

Die Verwendung des Begriffs „bereitstellen können“ lässt offen, ob eine tatsächliche Spannungsversorgung verpflichtend vorhanden sein muss. Für einen verlässlichen Betrieb externer Geräte zur Datenauslesung und -übermittlung ist jedoch eine verpflichtend bereitzustellende Stromversorgung erforderlich.

Anpassungsvorschlag:

„Die Kundenschnittstelle muss eine Spannungsversorgung für die Datenauslesung und -übermittlung an den Empfänger bereitstellen.“

Drüber hinaus sollte die Mindestleistung der Spannungsversorgung normativ festgelegt werden. Ohne eine entsprechende Leistungsdefinition wäre auch eine technisch unzureichende Versorgung formal konform (z. B. im Bereich weniger Zehntel Watt), was den praktischen Einsatz erheblich einschränkt.

Festlegung einer Mindestleistung, z. B. $\geq 2,5\text{ W}$ (entsprechend gängigen Industrie- und Consumer-Standards, etwa USB-A mit 5 V / 0,5 A), um den zuverlässigen Betrieb marktüblicher Endgeräte sicherzustellen.

§ 3 Z 09

„Die Kundenschnittstelle ist mit einer physikalischen Schnittstelle nach internationalem Standard auszuführen.“

Die ausschließliche Anforderung an eine physikalische Schnittstelle ist aus fachlicher Sicht nicht ausreichend. Für interoperable und zukunftsichere Anwendungen ist entscheidend, dass auch die digitale Kommunikationsschnittstelle einem internationalen Standard entspricht.

Anpassungsvorschlag:

„Die Kundenschnittstelle ist als digitale Schnittstelle nach internationalem Standard mit einem handelsüblichen physikalischen Interface auszuführen.“

Diese Formulierung stellt klar, dass sowohl die digitale Kommunikationsebene (z. B. Ethernet, IP-basierte Protokolle) als auch das physikalische Interface standardisiert sein müssen. Das physikalische Interface kann dabei kabelgebunden (z. B. RJ45 als physikalisches Interface mit Ethernet als digitalem Kanal) oder drahtlos (z. B. WLAN oder Bluetooth mit IP-basierter Kommunikation) umgesetzt werden, sofern ein international etablierter digitaler Standard verwendet wird.

§ 3 Z 10

Im Entwurf wird in § 3 Z 10 festgelegt, dass **intelligente Messgeräte sowie ihre Kommunikation nach anerkanntem Stand der Technik abzusichern und zu verschlüsseln** sind. Der Regelungsfokus liegt dabei ausschließlich auf der **Datensicherheit und dem Schutz der Kommunikation**.

Diese Ausrichtung greift aus unserer fachlichen Sicht zu kurz, da **moderne Bedrohungsszenarien im Bereich kritischer Infrastrukturen** über klassische IT- und Kommunikationssicherheitsaspekte hinausgehen. Intelligente Messgeräte sind komplexe elektronische Systeme mit weltweit verteilten Produktions- und Lieferketten, wodurch zusätzliche Risiken entstehen, insbesondere im Hinblick auf **Hardware-Integrität und Lieferkettensicherheit**.

Internationale Beispiele – etwa die umfassenden Vorgaben zur Lieferkettensicherheit in der Cybersecurity-Regulatorik der tschechischen Behörde **NÚKIB** – zeigen, dass Sicherheitsanforderungen zunehmend auch **Herstellungs-, Entwicklungs- und Lieferprozesse** umfassen. Risiken ergeben sich dabei insbesondere durch manipulierte Hardware-Komponenten, unsichere Produktions- oder Testumgebungen sowie durch staatliche Einflussnahme bei Herstellern aus Drittstaaten ohne vergleichbare Sicherheitsstandards. [\[portal.nukib.gov.cz\]](https://portal.nukib.gov.cz)

Erforderlichkeit einer erweiterten Sicherheitsbetrachtung: Globale Lieferketten und steigende Risiken manipulierter Hardware

Intelligente Messgeräte sind elektronische Systeme mit komplexen Hardware-Komponenten, die zunehmend weltweit produziert werden. Dadurch entsteht das Risiko:

- manipulierter Bauteile (z. B. Firmware-Manipulation, eingebettete Backdoors),
- unsicherer Produktions- und Testumgebungen,
- staatlicher Einflussnahme bei Herstellern aus nicht vertrauenswürdigen Drittstaaten.

Internationale Cyberregulierungsbehörden wie NÚKIB betonen explizit, dass Lieferkettenrisiken insbesondere dann steigen, wenn Herstellung oder Firmware-Entwicklung in Staaten erfolgt, die **keine vergleichbaren Sicherheitsstandards** garantieren.

Der vorliegende Entwurf der IMA-V 2026 berücksichtigt diese Aspekte bislang nicht, obwohl intelligente Messgeräte als wesentliche Bestandteile der **kritischen Infrastruktur** nach dem EIWG nachweislich sicher betrieben werden müssen. Aus unserer Sicht wäre daher eine **Erweiterung des § 3 Z 10 um verbindliche Anforderungen zur Lieferkettensicherheit und Hardware-Integrität** sachgerecht.

Darüber hinaus sprechen auch **industrie- und binnenmarktpolitische Zielsetzungen auf europäischer Ebene** für eine solche Erweiterung. Initiativen wie der **Cybersecurity Act** stärken Sicherheit, Resilienz und Standardisierung von IKT-Komponenten und -Systemen, die zunehmend auch in industriellen Wertschöpfungsketten eingesetzt werden. Und der Regulierungsansatz aus der Mobilfunkindustrie, der **EU 5G Toolbox Maßnahmenkatalog** zur Absicherung von 5G-Netzen, steht mit dieser Zielsetzung im Einklang.

Eine europäisch harmonisierte Betrachtung der Sicherheitsanforderungen an intelligente Messgeräte würde die **einheitliche Umsetzung hoher Sicherheitsstandards** fördern und zugleich das Regelungsziel der IMA-V 2026 wirksam unterstützen.

§ 3 Z 11

§ 3 Z 11 IMA-V 2026 sieht vor, dass intelligente Messgeräte eine **Ein- und Abschaltung der Kundenanlage mittels konfigurierbarer Schalttafel** unterstützen müssen. Diese Anforderung stellt aus unserer Sicht **keine generelle Mindestfunktionalität** dar, da sie **nur für einen begrenzten Teil der Endkunden** tatsächlich relevant ist.

Aus unserer Sicht sollte eine derartige, spezifische Funktionalität nicht verpflichtend in der IMA-V verankert werden, sondern bei Bedarf explizit durch jene Kunden angefordert werden, für die diese Funktion einen konkreten Mehrwert bietet.

Zudem ist festzuhalten, dass die Schaltung von Verbrauchern bereits über die zwei vorhandenen Relais des intelligenten Messgeräts möglich ist, auch unter Verwendung von Schalttabellen. Die in § 3 Z 11 vorgesehene Funktionalität ist daher **alternativ technisch umsetzbar**, ohne diese zwingend als allgemeine Mindestanforderung vorzusehen.

§ 3 Z 12

„Bei der Überschreitung der maximalen Bezugs- oder Einspeisungswerte innerhalb eines Zeitintervalls von 15 Minuten erfolgt die Ausschaltung der Anlage.“

Die Regelung wirft mehrere ungelöste Auslegungsfragen auf:

- Erfolgt die Ausschaltung unverzüglich oder erst nach einer Vorwarnung bzw. Frist?
- Wie wird der Netzkunde über Ursache und Zeitpunkt der Abschaltung informiert?
- Was bedeutet „innerhalb eines Zeitintervalls von 15 Minuten“ konkret:
 - eine einmalige kurzzeitige Überschreitung, oder
 - eine andauernde Überschreitung über das gesamte Intervall?

Die Interpretation als einmalige Überschreitung würde zu unverhältnismäßig häufigen Abschaltungen führen, etwa durch kurzzeitige hohe Einschaltströme (z. B. bei Aufzügen oder industriellen Anlaufprozessen). Dies kann sicherheitsrelevante Risiken für Dritte verursachen und die Verhältnismäßigkeit der Maßnahme infrage stellen.

Anpassungsvorschlag:

Klarstellung, dass eine Ausschaltung nur bei einer anhaltenden Überschreitung über ein gesamtes 15-Minuten-Intervall erfolgt, ergänzt um:

- Informationspflichten gegenüber dem Netzkunden (z. B. Ursache, Zeitpunkt, Wiederschaltung),
- optional eine Vorwarn- oder Reaktionsfrist.

Aus fachlicher Sicht erscheint es zudem zweckmäßiger, Sanktionsmechanismen systematisch mit § 3 Z 13 zu verknüpfen, anstatt eine unmittelbare Abschaltung vorzusehen.

§ 3 Z 13

„Dies erfolgt über potentialfreie Kontakte (zwei mechanische Relais) für externe Lastschaltung, die mit Kalenderzeitfunktionen ausgestattet sind.“

Die Formulierung ist widersprüchlich. Potentialfreie Kontakte bzw. mechanische Relais stellen per se keine Intelligenz oder Kalenderzeitfunktionen bereit. Diese Funktionen können nur durch eine übergeordnete Steuereinheit oder Logik realisiert werden.

Zudem bleibt offen,

- wo sich diese Logik befindet (Messgerät, externe Steuereinheit),
- ob die Ansteuerung verpflichtend oder freiwillig ist,
- und welche Konsequenzen sich aus einer Nichtbefolgung ergeben.

Anpassungsvorschlag:

Präzisere Trennung zwischen:

- der physikalischen Schaltebene (potentialfreie Kontakte / Relais) und
- der logischen Steuer- und Zeitfunktion (z. B. im intelligenten Messgerät oder einem zugeordneten Steuergerät).

Der Ansatz der Freiwilligkeit ist grundsätzlich zu begrüßen, könnte jedoch – in Kombination mit § 3 Z 12 – durch klar definierte, verhältnismäßige Sanktionen bei nachweislicher Missachtung von Steuersignalen ergänzt werden.

§3 Z17

„Zudem sind die Geräte mit einer Manipulationserkennung auszustatten.“

Die Formulierung ist sehr allgemein und lässt bereits rein mechanische Maßnahmen (z. B. Plombierung) als ausreichend erscheinen. Eine solche Auslegung wird den heutigen sicherheitstechnischen Anforderungen an intelligente Messsysteme nicht gerecht.

Anpassungsvorschlag:

Klarstellung des Schutzniveaus, etwa durch:

„Zudem sind die Geräte nach dem Stand der Technik mit analoger und digitaler Manipulationserkennung auszustatten.“

Optional könnte zusätzlich auf anerkannte Normen oder Sicherheitsstandards verwiesen werden, um ein einheitliches und überprüfbares Sicherheitsniveau sicherzustellen.

Wenn es Fragen oder Diskussionsbedarf zu dieser Stellungnahme gibt, steht Ihnen die Technologieplattform Smart Grids Austria mit ihren Experten jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Christoph Wanzenböck

Kontakt Daten

Christoph Wanzenböck, MA, MBA, Geschäftsführer
1060 Wien, Mariahilfer Straße 37-39

E: christoph.wanzenbieck@smartgrids.at

I: www.smartgrids.at