Statkraft

Statkraft zum Referentenentwurf eines Gesetzes zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastrukturen

Statkraft bedankt sich für die Möglichkeit zur Stellungnahme. Wir begrüßen das Ziel des Referentenentwurfs, Transparenz-, Veröffentlichungs- und Informationspflichten an die veränderte Sicherheitslage anzupassen. Im Folgenden erläutern wir unsere allgemeinen und konkreten Anmerkungen zum Entwurf.

1. Allgemeine Anmerkungen

Die vorgesehenen Änderungen des Energiewirtschaftsgesetzes (EnWG) und des Informationsfreiheitsgesetzes (IFG) sind wichtige Schritte. Für einen umfassenden Schutz kritischer Infrastrukturen und Anlagen müssen die Regelungen jedoch konkretisiert und ergänzt werden. Zudem sind klare, einheitliche Kontaktstellen für den Schutz zu benennen. Dabei ist zu prüfen, ob andere Veröffentlichungspflichten oder bereits veröffentlichte Informationen den geplanten Schutz unterlaufen. Möglicherweise sind deshalb weitere Änderungen nötig, etwa im Genehmigungsrecht und Umweltinformationsrecht.

Berechtigte Transparenz und der Schutz kritischer Infrastrukturen können miteinander in Konflikt stehen. Diese Konflikte lassen sich nicht immer vollständig lösen. Als Anlagenbetreiber und beim Ausbau von Windkraftanlagen sind wir und andere Stromerzeuger dringend auf Netzinformationen angewiesen. Einige dieser Informationen sollen erst künftig bereitgestellt werden. Es darf nicht zur Praxis werden, dass die Bereitstellung sinnvoller Daten für legitime Zwecke durch geringfügige oder lediglich vermeintliche Risiken vollständig unterbunden wird. Dies gilt aus unserer Sicht unter anderem für die Bereitstellung von Informationen mit Relevanz für die Projektentwicklung erneuerbarer Energien, bspw. für den Umfang freier Netzkapazität an einem Netzanschlusspunkt oder die jährlich dort im Rahmen des Redispatchs nach § 13a EnWG abgeregelte Strommenge je Technologie. Diese Daten können weiter öffentlich bereitgestellt bzw. über eine zugangsbeschränkte Plattform zugänglich gemacht werden.

2. Konkrete Anpassungsvorschläge

Zu Artikel 1 Nummer 1 – § 12f Absatz 2 EnWG: Daten vor Weitergabe schützen und Need-to-Know-Prinzip anwenden

Statkraft unterstützt, dass detaillierte Daten zu kritischen Anlagen nur an Personen mit nachgewiesener Fachkunde herausgegeben werden, die diese Daten für ihre Aufgabe benötigen. Dabei sollten aus unserer Sicht folgende Anforderungen gelten:

- Es muss einheitlich und nachvollziehbar festgelegt werden, welche Fachkunde erforderlich ist, für welche Aufgaben Daten benötigt werden und wie ihre Vertraulichkeit zu sichern ist.
- Daten und Informationen dürfen nur für einen festgelegten Zweck verwendet werden. Eine Weitergabe sollte höchstens in aggregierter und anonymisierter Form zulässig sein.
- Wir regen an, sicherheitsrelevante Daten und Informationen Privatpersonen nur im Ausnahmefall zugänglich zu machen.
- Sicherheitsrelevante Informationen dürfen nicht veröffentlicht oder allgemein zugänglich gemacht werden, wenn sie die Sicherheit oder Zuverlässigkeit von Energieanlagen gefährden können. Das gilt auch, wenn die Gefahr erst durch die Kombination mit anderen zugänglichen Informationen entsteht. Statt detaillierter Angaben sind vorrangig zusammengefasste, vereinfachte, nach Kategorien geordnete oder anonymisierte Angaben bereitzustellen. Voraussetzung ist, dass sich daraus tatsächlich keine sicherheitskritischen Informationen ableiten lassen.
- Bei der Sicherheitsbewertung ist zwischen statischen Informationen und aktuellen Betriebs- und Projektdaten, auch in Echtzeit, zu unterscheiden. Angaben zur aktuellen Netzauslastung, zu verfügbaren Kapazitäten und Engpässen sowie aktuelle Informationen aus Genehmigungsverfahren, Entwicklungsplänen und Projekten können die Betriebslage unmittelbar erkennen lassen. Für diese Daten muss ein besonders strenges Need-to-know-Prinzip gelten: Zugang erhält nur, wer nachweislich ein berechtigtes Interesse an den Daten hat. Datenumfang, Verwendungszweck, zugangsberechtigte Personen und Zugangszeitraum sind auf das Notwendige zu begrenzen. Diese Daten sollten vorrangig überprüft und ihre Zugänge beschränkt werden, da sich die Sicherheit hier kurzfristig verbessern lässt. Auch statische und bereits bekannte Daten bleiben schutzbedürftig, besonders wenn sie systematisch zusammengeführt werden.
- Auch bei typisierten Datensätzen, die als Ersatz für konkrete Daten bereitgestellt werden, muss die Sicherheit Vorrang haben. Aus diesen Ersatzdaten dürfen sich keine geschützten

Informationen rekonstruieren lassen. Daher sollten auch Ersatzdaten nur herausgegeben werden, wenn sich daraus keine sicherheitskritischen Informationen ableiten lassen.

- Auch Anlagen in der Planung oder Genehmigung sind als potentiell kritische Anlagen zu schützen.
- Aus Statkrafts Sicht sind die oben aufgeführten Konkretisierungen in der Begründung des Gesetzes festzuhalten. Alternativ könnte die Bundesnetzagentur eine entsprechende Festlegung erlassen. Bei deren Erstellung sind Betreiber kritischer Infrastrukturen und Anlagen dringend eng einzubinden.

Zu Artikel 1 Nummer 2 – § 111g Absatz 2 Satz 9 EnWG: Veröffentlichungsverbot auf der Transparenzplattform absichern

Statkraft begrüßt, dass sicherheitsrelevante Daten künftig grundsätzlich nicht veröffentlicht werden dürfen.

Vor jeder möglichen Veröffentlichung vermeintlich nicht sicherheitsrelevanter Daten durch die Bundesnetzagentur ist jedoch auch zu prüfen, wie detailliert die entsprechenden Daten sind und welche Risiken durch ihre Kombination mit anderen Informationen entstehen. Die betroffenen Betreiber sind dazu anzuhören. Der Schutz muss auch beim Abruf über Schnittstellen, bei Downloads und bei späteren Aktualisierungen gewährleistet sein.

Die Änderung des § 111g EnWG schützt nicht automatisch auch die Daten in anderen Registern und Plattformen. Deshalb ist dringend zu prüfen, ob dort entsprechende Schutzregelungen ergänzt werden müssen.

Zu Artikel 2 – § 3 IFG: Den Informationszugang rechtssicher begrenzen

Wir begrüßen ausdrücklich, dass sicherheitsrelevante Informationen über kritische Infrastrukturen und Anlagen künftig geschützt werden sollen. Richtig ist auch, schutzbedürftige Infrastrukturen und Anlagen einzubeziehen, die nicht formal als KRITIS eingestuft sind. Folgende Konkretisierungen sind aus unserer Sicht darüber hinaus vorzunehmen:

- Es ist aus unserer Sicht dringend zu konkretisieren, welche Arten von Informationen typischerweise schutzbedürftig sind und nach welchen verlässlichen Kriterien dies zu beurteilen ist. Dazu gehören insbesondere sicherheitsrelevante Angaben zu Standorten, Leitungen und Trassen, technischer Auslegung, Kapazitäten, Schwachstellen und Schutzvorkehrungen. Das ist in der Gesetzesbegründung zu ergänzen.
- Bevor Informationen herausgegeben werden, sind die betroffenen Betreiber einzubeziehen. Auch Begründungen und Nachweise zu Sicherheitsrisiken müssen vertraulich behandelt werden können. Wenn geschwärzte oder ausreichend vereinfachte Unterlagen den

Informationszweck erfüllen, ist diese Form zu wählen. So bleiben Informations- und Beteiligungsrechte gewahrt, ohne sicherheitsrelevante Details offenzulegen.

- Betreiber benötigen außerdem ein gesetzlich abgesichertes Recht, sicherheitsrelevante Informationen zurückzuhalten, wenn deren Offenlegung die geschützten Infrastrukturen gefährden kann. Dieses Recht muss mit den jeweiligen Informationspflichten abgestimmt werden. Auch hier ist sicherzustellen, dass Informationen nicht über andere Zugangswege angefordert werden.
- **Umweltinformationsrechte anpassen:** Unterlagen, die im Genehmigungsverfahren aus Sicherheitsgründen geschützt werden, dürfen nicht über einen anderen Informationszugang doch noch offengelegt werden. Die Änderung des IFG gilt für Bundesstellen. Sie ersetzt weder notwendige Änderungen des Umweltinformationsgesetzes (UIG) noch abgestimmte Regelungen der Länder. Deshalb brauchen umweltbezogene Informationen mit Sicherheitsbezug einen eigenen, praxistauglichen Schutz. Entsprechende Regeln sind auch im Geodatenrecht und im Landesrecht erforderlich.
-

Zu Artikeln 4 und 5 – § 172 Nummer 1 GVG und § 52 ArbGG:
Vertraulichkeit auch in Gerichtsverfahren gewährleisten

Statkraft hält es für richtig, die Öffentlichkeit von Gerichtsverhandlungen auszuschließen, wenn kritische Infrastrukturen gefährdet werden könnten. Zusätzlich ist zu prüfen, wie sensible Informationen bei der Akteneinsicht, der elektronischen Bereitstellung von Unterlagen und der Veröffentlichung gerichtlicher Entscheidungen geschützt werden können. Dieser Schutz muss durchgängig gelten.

3. Hinweise zur Umsetzung und bestehende Veröffentlichungen verbindlich regeln

Damit die Regeln einheitlich angewendet werden, braucht es einheitliche, klare Ansprechpartner und praktikable Verfahren zur Bewertung sensibler Daten. Das technische und betriebliche Wissen der Betreiber muss dabei einbezogen werden.

Aktuell fehlt noch ein Löschverfahren für öffentliche und private Stellen, mit dem sichergestellt wird, dass bereits veröffentlichte sicherheitsrelevante Daten gelöscht werden. Es muss dringend klar geregelt werden, wer bestehende Veröffentlichungen auf welcher Rechtsgrundlage prüft. Betreiber brauchen einen verlässlichen Weg, sicherheitskritische Veröffentlichungen zu melden und überprüfen und ggf. beschränken zu lassen.

Über Statkraft

Statkraft ist international führend in Wasserkraft und Europas größter Erzeuger erneuerbarer Energie. In Deutschland erzeugen wir Strom aus Wasser, Wind, Sonne und Gas, betreiben Batterien und sind ein wichtiger Akteur im Energiehandel.

Kontakt:

Claudia Gellert
Head of Political Affairs
Claudia.Gellert@statkraft.com

Miriam Brandes
Manager Political Affairs
Miriam.Brandes@statkraft.com

Lobbyregister: Statkraft Markets GmbH ist unter der Registernummer R003478 im Lobbyregister des Deutschen Bundestages registriert.