

8. Physische Sicherheit  
 9. Sicherheit von Informationssystemen; und  
 10. Netzwerksicherheit.

Das Einführen einer minimalen Reihe von Sicherheitsmaßnahmen erfordert den Konsens und die Kooperation von verschiedenen Interessenvertretern der Smart Grids. Eine Koordinationsinitiative könnte ermöglichen, dass eine einheitliche und allgemein akzeptierte Herangehensweise bei Sicherheitsvorfällen in Smart Grids gewährleistet wird. Darüber hinaus würde eine einheitliche Herangehensweise zum Thema Internetsicherheit sowohl den Regulatoren als auch Interessenvertretern zugutekommen, indem sie die komplexe Umgebung von Smart Grids in Einklang bringt und einen Anreiz bietet, die Internetsicherheit zu verbessern. Dieser Bericht kann die EU unterstützen durch:

- das Angleichen der unterschiedlichen Level an Sicherheit und Stabilität der Anbieter auf dem Markt an ein konsistentes Mindestmaß nationaler Rahmenbedingungen;
- das Bereitstellen von Anzeichen eines Mindestmaßes an Sicherheit und Stabilität in den Mitgliedsstaaten in Bezug auf die Smart Grids;
- das Sicherstellen eines Mindestmaßes an Anforderungen an Smart Grids in den Mitgliedsstaaten, wodurch die Einhaltung- und Betriebskosten reduziert werden;
- das Legen eines Grundsteins für ein Mindestmaß an Rahmenbedingungen überprüfbarer Kontrolle in Europa;
- das Generieren von Bereitschaft, Wiederherstellbarkeit, Rücklaufmaßnahmen und gegenseitiger Hilfe der Betreiber während einer Krise;
- das Beitragen, um ein angemessenes Level an Transparenz im internen Markt zu erreichen.

Der Geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, sagt: „Um die ehrgeizigen EU2020 Ziele zu erreichen: 20% erneuerbare Energie, eine Reduktion von CO2 Emissionen um 20% und eine Zunahme von Energieeffizienz um 20%, ist es wesentlich, dass das Bereitstellen von Smart Grids für verteilte Energieerzeugung in zukünftigen Stromnetzen auf sichere Art und Weise erfolgt. Beide innovativen technischen Lösungen sind notwendig, zusammen mit neuen regulierenden und ökonomischen Systemen der EU. Wir hoffen, Smart Grids in der bevorstehenden Internet-Sicherheitsstrategie der EU zu sehen.“

Den vollständigen Bericht finden Sie hier: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids/>

## Schaar zum Beschäftigtendatenschutzgesetz: „Kein großer Wurf“

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar hält den von den Koalitionsparteien im Januar 2013 vorgelegten Entwurf zum Beschäftigtendatenschutz nicht für ausreichend. Zudem bedauert er es, dass die meisten Anregungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus ihrer Entschließung vom 16./17. März 2011<sup>1</sup> nicht berücksichtigt wurden.

Peter Schaar: „Der von der Bundesregierung 2011 beschlossene Entwurf enthielt viele Schwachstellen. Die nunmehr vorgeschlagenen Änderungen sind ambivalent. Sie bringen Verbesserungen, überwiegend aber Verschlechterungen für den Datenschutz der Beschäftigten.“

- „Es ist erfreulich, dass es beim Verbot der heimlichen Videoüberwachung bleiben soll und dass nunmehr bei der offenen Videoüberwachung die Daten nicht für die allgemeine Leistungs- und Verhaltenskontrolle genutzt werden dürfen. Allerdings wird es auch nach dem Koalitionsentwurf gegenüber dem heutigen Recht zu deutlichen Erweiterungen der offenen Videoüberwachung im Arbeitsverhältnis kommen.“
- „Die im Regierungsentwurf vorgesehene Eingrenzung der Datenerhebung im Bewerbungsverfahren wird gelockert. So dürfen öffentlich zugängliche Daten über Bewerber generell genutzt werden, auch wenn sie aus sozialen Netzwerken stammen. Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll entfallen.“
- „Nicht akzeptabel ist auch, dass es auch im aktuellen Entwurf dem Arbeitgeber gestattet sein soll, nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn der Beschäftigte eingewilligt hat. Im Regelfall ist davon auszugehen, dass im Bewerbungsverfahren und im Beschäftigungsverhältnis derartige Zustimmungungen nicht wirklich freiwillig sind. Diese Regelung bleibt hinter der von der Europäischen Kommission vorgeschlagenen Datenschutz-Grundverordnung zurück, die in solchen Fällen eine Einwilligungslösung ausschließt.“
- „Schon der Regierungsentwurf enthielt weitgehende Befugnisse für den Arbeitgeber, die telefonische Kommunikation von Call-Center-Mitarbeitern mitzuhören, aufzuzeichnen und zu nutzen. Die dort vorgesehene zeitliche Eingrenzung und die darauf bezogene Pflicht, den Mitarbeiter darüber vorab zu informieren, sollen nach dem Willen der Regierungsfractionen nun entfallen. Damit wird für die Mitarbeiterinnen und Mitarbeiter ein nicht hinnehmbarer Überwachungsdruck erzeugt.“

Der Bundesdatenschutzbeauftragte bedauert es, dass in dem Entwurf weiterhin wichtige für den Arbeitnehmerdatenschutz bedeutsame Regelungen fehlen, etwa zur automatisierten Personalaktenführung, zur privaten Nutzung von Telekommunikationsdiensten oder zum Beweisverwertungsverbot bei unzulässiger Datenerhebung und -verwendung. Zudem hält er es für ein schlechtes Signal, dass der Entwurf an verschiedenen Punkten hinter der von der Europäischen Kommission vorgeschlagenen Datenschutz-Grundverordnung zurück bleibt.

Schließlich weist der Bundesdatenschutzbeauftragte darauf hin, dass die vorgeschlagenen Änderungen zur Auftragsdatenverarbeitung in Drittstaaten weit über den Beschäftigtendatenschutz hinaus bedeutsam sind, etwa für die Nutzung von Cloud-Diensten. Derartige Änderungen dürfen nicht ohne gründliche Analyse und Diskussion im Eilverfahren beschlossen werden.

## Europäische Datenschutzreform: BfDI begrüßt Änderungsvorschläge aus dem Europäischen Parlament

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Peter Schaar sieht in der vom Berichterstatter des Innenaus-

<sup>1</sup> DuD Heft 5 (2011), S. 356