

Management Summary

Die zunehmende Dezentralisierung der Stromproduktion, die grösseren Speichermöglichkeiten sowie die damit einhergehende Entwicklung von intelligenten Netzen und intelligenten Messsystemen ermöglichen neue Kooperationskonzepte, wie etwa das vom Internationalen Institut für Management und Technologie der Universität Fribourg entwickelte Crowd-Energy-Konzept.

Anwendungsfall eines solchen Konzeptes, beziehungsweise dessen Grundelement, die iGSL-Zelle, sind Eigenverbrauchsgemeinschaften (EVG). Zur technischen Umsetzung von EVGs werden eine oder mehrere Stromerzeugungsanlagen, eventuell ein Batteriespeicher, intelligente Messsysteme und gegebenenfalls Wärmepumpen und weitere Elemente der Gebäudetechnik eingesetzt. Intelligente Überwachungs-, Visualisierungs- und Regelungsanwendungen (Software oder Apps) verbinden die Komponenten und unterstützen die Bewirtschaftung.

Mit dem ersten Massnahmenpaket der Energiestrategie 2050, welches am 1. Januar 2018 in Kraft trat, werden EVGs in der Schweiz gefördert und umfassend gesetzlich geregelt. Gemäss Art. 15 Energieverordnung vom 1. November 2017 (E-EnV) ist der Zusammenschluss zum Eigenverbrauch zulässig, sofern die Produktionsleistung der Anlage bei mindestens 10 % der maximalen Netzanschlusskapazität liegt. EVGs können am geöffneten Markt teilnehmen, sofern der jährliche Stromverbrauch der EVG die Schwelle von 100 MWh übersteigt.

Crowds verlangen nach einer Vielzahl von Daten (zum Beispiel Mess und Ab-rechnungsdaten und Prognosedaten). Diese werden mittels Informations- und Kommunikationstechnologie (IKT) aufgezeichnet, ausgetauscht und verknüpft.

Durch die vermehrten Schnittstellen im Netz steigen allerdings die Verletzlichkeit und Verwundbarkeit sowie die Gefahr, durch gezielte Angriffe geschädigt zu werden. Aufgrund beispielsweise einer Distributed-Denialof-Service-Attacke oder einer Infektion mit Malware könnte die Kontrolle über die Crowd verloren gehen und zu einem lokalen Blackout führen. Aus den gesammelten Prosumer-Daten können aber auch Informationen über das Nutzerverhalten der Mitglieder einer Crowd abgeleitet werden, was die Crowd zu einer Quelle für zahlreiche Risiken wie etwa Betrug oder Einbrüche macht. Der Schutz und die Sicherheit von Daten spielt deshalb eine zentrale Rolle für Crowds.

Für Privatpersonen und Gewerbebetriebe sind Crowds eine Herausforderung. Sie verfügen kaum über Kompetenzen, um sich vor den genannten Risiken zu schützen. Crowds sollten deshalb, analog zu Datenschutz- und Datensicherheitsrichtlinien in Unternehmen, minimal



erforderliche Empfehlungen und Massnahmen zum Schutz und zur Sicherheit von Daten zu definieren, an die sich alle Akteure halten müssen.

Nach Ausführungen zu den (rechtlichen) Grundlagen zum Datenschutz im nationalen, europäischen und internationalen Umfeld, umschreibt die vorliegende Masterarbeit die wesentlichen Eckpunkte einer Datenschutzrichtlinie, wie sie für eine Crowd zu erarbeiten ist. Das sind insbesondere Regelungen zu den Bearbeitungsgrundsätzen, wie Rechtmässigkeit, Treu und Glauben, Verhältnismässigkeit, Zweckbindung, Transparenz, Richtigkeit sowie die Vorschriften mit Bezug auf die Datenbearbeitung durch Dritte sowie der Bekanntgabe ins Ausland und zur Organisation in einer Crowd. Thematisiert werden auch die Massnahmen zur Gewährleistung der Datensicherheit. Unter Berücksichtigung des revidierten Datenschutzgesetzes beinhaltet sie auch die Anforderungen an das Verzeichnis der Bearbeitungstätigkeiten sowie an die Datenschutz-Folgenabschätzung und die Rechte der betroffenen Personen insbesondere auf Auskunft, Berichtigung und Löschung.



Table of Contents

Danksagung	I
Zusammenfassung	II
Inhaltsverzeichnis	IV
Abbildungsverzeichnis	VII
Abkürzungsverzeichnis	VIII
1 Einleitung	1
1.1 Ausgangslage	1
1.1.1 Energiepolitisches Umfeld	1
1.1.2 Von zentraler zu dezentraler Stromproduktion	3
1.1.3 Entwicklung von intelligenten Netzen und intelligenten Messsystemen	5
1.1.4 Änderung der Rolle des Verbrauchers	8
1.2 Das Crowd Energy Konzept	9
1.2.1 Definition und Zielsetzungen	9
1.2.2 iGSL-Zelle als Grundelement	11
1.2.3 Akteure der Crow Energy	13
1.2.4 Anwendungsbeispiele	14
1.2.5 Rechtsgrundlagen in der Schweiz	16
1.3 Die Bedeutung von Datenschutz und Datensicherheit im Crowd Energy Umfeld	21
2 Begriffliche Grundlagen	24
2.1 Information	24
2.2 Daten	25
2.3 Informationssicherheit, IT-Sicherheit, Cyber-Sicherheit	25
2.4 Datenschutz	26
2.5 Datensicherheit und Informationssicherheit	28
3 Schutzziele	29
3.1 Schutzziele des Datenschutzes	29
3.2 Schutzziele der Daten- bzw. Informationssicherheit	29
3.2.1 Allgemeines	29
3.2.2 Vertraulichkeit	30
3.2.3 Integrität	30
3.2.4 Verfügbarkeit	31
3.2.5 Nachvollziehbarkeit	31



3.2.6	<u>Authentizität</u>	32
4	<u>Rechtliche Rahmenbedingungen</u>	33
4.1	<u>Einleitung</u>	33
4.2	<u>Internationales Umfeld</u>	34
4.2.1	<u>Vereinte Nationen</u>	34
4.2.2	<u>Europarat</u>	39
4.2.3	<u>Organisation für wirtschaftliche Zusammenarbeit und Entwicklung</u>	42
4.3	<u>Europäisches Umfeld</u>	45
4.3.1	<u>Grundlagen des europäischen Rechtssystems</u>	45
4.3.2	<u>Datenschutzrecht und Datensicherheit</u>	47
4.3.3	<u>Energiewirtschaftliche Regulierungen</u>	59
4.3.4	<u>Exkurs: NIS-Richtlinie</u>	63
4.4	<u>Nationales Umfeld</u>	65
4.4.1	<u>Bundesgesetz über den Datenschutz</u>	65
4.4.2	<u>Energiewirtschaftliche Regulierungen</u>	83
4.4.3	<u>Exkurs: Entwurf Informationssicherheitsgesetz</u>	87
5	<u>Selbstregulierungsstandards</u>	89
5.1	<u>Begriff und Bedeutung</u>	89
5.2	<u>Regelungsinhalt</u>	90
5.3	<u>Mandat M/490 und Mandat M/441</u>	90
6	<u>Leitlinie für die Crowd Akteure</u>	92
6.1	<u>Grundlagen</u>	92
6.2	<u>Gegenstand</u>	93
6.3	<u>Zweck</u>	94
6.4	<u>Schutzziele</u>	94
6.5	<u>Geltungsbereich</u>	94
6.6	<u>Organisation</u>	95
6.6.1	<u>Aussenverhältnis</u>	95
6.6.2	<u>Innenverhältnis</u>	95
6.6.3	<u>Datenschutzverantwortliche</u>	95
6.7	<u>Bearbeitung durch Auftragsbearbeiter</u>	96
6.8	<u>Bekanntgabe von Personendaten ins Ausland</u>	96
6.9	<u>Verzeichnis der Bearbeitungstätigkeiten</u>	97
6.10	<u>Grundsätze der Bearbeitung von Personendaten</u>	97
6.10.1	<u>Rechtmässigkeit</u>	97
6.10.2	<u>Zweckbestimmung</u>	98
6.10.3	<u>Verhältnismässigkeit</u>	98



6.10.4	Treu und Glauben	98
6.10.5	Datenrichtigkeit	99
6.11	Technische und organisatorische Massnahmen	99
6.12	Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen	100
6.13	Datenschutz-Folgeabschätzung	100
6.14	Auskunftsgesuche, Recht auf Berichtigung und Löschung	101
6.15	Sanktionen	101
7	Schlussbetrachtung und Ausblick	102
	Literaturverzeichnis	VIII
	Materialienverzeichnis	VIII
	Anhang 1: Wertaustausch der an der Crowd beteiligten Mitglieder und Akteure	XI
	Anhang 2: Schematischer Überblick der grösstern Cyber-Bedrohungen	XII
	Anhang 3: Selbstregulierungsstandardisierungen im Bereich intelligenter Netze, Netzsysteme und Gebäude	XIII
	Anhang 4: SGAM-Modell	XIV
	Anhang 5: Crowd Energy-Leitlinie zur Informationssicherheit	XVII