ARTIKEL-29-DATENSCHUTZGRUPPE

00678/13/DE
WP205

Stellungnahme 4/2013 zum Muster für die Datenschutzfolgenabschätzung („Muster“) für intelligente Netze und intelligente Messsysteme, erstellt durch die Sachverständigengruppe 2 der Taskforce der Kommission für intelligente Netze

Angenommen am 22. April 2013

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 sowie auf Artikel 30 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung −

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 Kontext

1.1 Einleitung

Hintergrund

Am 9. März 2012 veröffentlichte die Europäische Kommission eine Empfehlung zu Vorbereitungen für die Einführung intelligenter Messsysteme (im Folgenden „Empfehlung der Kommission"), um den Mitgliedstaaten Hilfestellung bei der Einführung intelligenter Messsysteme auf den Strom- und Gasmärkten zu geben. Ziel der Empfehlung der Kommission ist es, Orientierungshilfen in Datenschutz- und Sicherheitsfragen, zu einer Methode für die wirtschaftliche Bewertung der langfristigen Kosten und Nutzeffekte der Einführung intelligenter Messsysteme[1] und zu den gemeinsamen Mindestfunktionsanforderungen an intelligente Messsysteme im Stromsektor zu bieten.

In Bezug auf den Datenschutz und die Sicherheit von intelligenten Messsystemen und intelligenten Netzen vermittelt die Empfehlung der Kommission den Mitgliedstaaten Orientierungshilfen für den konzeptionsbedingten und standardmäßigen Datenschutz und für die Anwendung bestimmter Datenschutzgrundsätze, die in der Richtlinie 95/46/EG[2] verankert sind. In der Empfehlung der Kommission ist außerdem festgelegt, dass die Mitgliedstaaten ein Muster für die Datenschutzfolgenabschätzung (im Folgenden das „Muster") annehmen und einsetzen, das von der Kommission innerhalb von zwölf Monaten nach der Veröffentlichung der Empfehlung der Kommission zu entwickeln und der Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten („Datenschutzgruppe") zur Stellungnahme vorzulegen ist. Anschließend sollten die Mitgliedstaaten dafür Sorge tragen, dass

---

1 Die Einführung und die Kosten-Nutzen-Analyse sind erforderlich gemäß (i) Richtlinie 2009/72/EG über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt (ABl. L 211 vom 14.8.2009, S. 55) und (ii) Richtlinie 2009/73/EG über gemeinsame Vorschriften für den Erdgasbinnenmarkt (ABl. L 211 vom 14.8.2009, S. 94). Richtlinie 2012/27/EU zur Energieeffizienz (ABl. L 315 vom 14.11.2012, S. 1) enthält zusätzliche Bestimmungen zu intelligenten Messsystemen. Wenn die Einführung intelligenter Zähler auf dem Strommarkt positiv bewertet wird, sollten laut Richtlinie 2009/72/EG mindestens 80 % der Verbraucher bis 2020 mit intelligenten Messsystemen ausgestattet sein. Für den Gasmarkt ist kein genauer Zeitplan festgelegt.

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31–50.

Netzbetreiber und Betreiber intelligenter Messsysteme geeignete technische und organisatorische Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten gemäß dem Muster einleiten und die Stellungnahme der Datenschutzgruppe zum Muster entsprechend berücksichtigen.[3]

In der Empfehlung der Kommission heißt es weiter: „*Die Datenschutzfolgenabschätzung sollte eine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren enthalten, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis für die Einhaltung der Richtlinie 95/46/EG erbracht werden soll; dabei trägt sie den Rechten und den berechtigten Interessen der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung.*“

Vorbereitung

Im Februar 2012 verlängerte die Kommission den Auftrag der Sachverständigengruppe 2 ihrer Taskforce für intelligente Netze, ein Muster für die Datenschutzfolgenabschätzung in intelligenten Netzen zu erarbeiten. Die Sachverständigengruppe 2, der in erster Linie Vertreter der Industrie angehören, führte im Jahr 2012 vier Workshops durch. Die CNIL[4], der EDSB[5] und die ICO[6] nahmen an diesen Workshops als Beobachter im Namen der Datenschutzgruppe teil.

Am 26. Oktober 2012 übermittelte die Datenschutzgruppe ein Schreiben an die Generaldirektion Energie der Europäischen Kommission (GD ENER), in dem sie die Kommission auf verschiedene Aspekte in der Entwurfsfassung des Musters aufmerksam machte, bei denen ihrer Ansicht nach erheblicher Verbesserungsbedarf besteht. Für das Muster wurden unter anderem folgende Verbesserungen empfohlen:

(i) eindeutige Benennung der Akteure und ihrer Zuständigkeiten,

(ii) Konzentration auf die Risiken für den Datenschutz und die Privatsphäre der betroffenen Personen,

(iii) bessere Hilfestellung für die Akteure bei der Erfassung der einzelnen Risiken und bei der Zuordnung angemessener Kontrollen,

(iv) konkretere und praxisorientierter Hilfestellung bei der Bewältigung der Risiken für den Datenschutz und die Privatsphäre im Zusammenhang mit intelligenten Netzen.

Diese Kommentare wurden unbeschadet der abschließenden Bewertung des Musters durch die Datenschutzgruppe vorgelegt.

---

[3] Die Sachverständigengruppe 2 stützte sich bei ihrer Arbeit auf die Erfahrungen mit der Entwicklung des „Vorschlags der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen“ sowie dessen Überarbeitung nach Kommentaren und Stellungnahmen der Artikel-29-Datenschutzgruppe.

[4] Commission Nationale de l'Informatique et des Libertés (nationale Aufsichtsbehörde für den Schutz personenbezogener Daten in Frankreich).

[5] Europäischer Datenschutzbeauftragter, Aufsichtsbehörde für den Schutz personenbezogener Daten durch die Organe und Einrichtungen der EU.

[6] Information Commissioner's Office (nationale Aufsichtsbehörde für den Schutz personenbezogener Daten im Vereinigten Königreich).

Das Muster für die Datenschutzfolgenabschätzung („Muster“)

Am 8. Januar 2013 legte die Kommission der Datenschutzgruppe die endgültige Fassung des von den beteiligten Akteuren der Sachverständigengruppe 2 erarbeiteten Musters vor. Im Begleitschreiben zum Muster teilte die Kommission mit, dass sie vorbehaltlich der Kommentare der Datenschutzgruppe und der entsprechenden Abstimmung mit diesen Kommentaren in Erwägung zieht, das von den beteiligten Akteuren der Sachverständigengruppe 2 erarbeitete Muster in Form einer Empfehlung der Kommission anzunehmen.[7]
Die vorliegende Stellungnahme enthält Kommentare zum vorgeschlagenen Muster.

Aufbau der vorliegenden Stellungnahme

In Abschnitt 1.2 wird die Bedeutung des Datenschutzes und des Schutzes der Privatsphäre für den erfolgreichen Aufbau intelligenter Netze hervorgehoben. In Abschnitt 1.3 werden die Ziele einer Datenschutzfolgenabschätzung genannt. Abschnitt 2 enthält die Bewertung des Musters durch die Datenschutzgruppe. In Abschnitt 3 werden die Schlussfolgerungen dargelegt. Anhang I ist eine Ergänzung zu Abschnitt 2 und enthält detailliertere Kommentare und Vorschläge.

1.2 Intelligente Netze und Datenschutz

Die Datenschutzgruppe verweist auf ihre frühere Stellungnahme zur intelligenten Verbrauchsmessung (WP183)[8] sowie auf die Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB) vom 8. Juni 2012 zur Empfehlung der Kommission[9].

Beide Stellungnahmen unterstreichen die Bedeutung des Datenschutzes im Zusammenhang mit intelligenten Netzen und intelligenten Messsystemen und geben Hilfestellungen und Empfehlungen, wie die Rechte auf den Schutz personenbezogener Daten bei der Einführung intelligenter Messsysteme und intelligenter Netze in Europa geschützt werden können. Daher werden in diesem Abschnitt der Kontext und die wichtigsten datenschutzrechtlichen Bedenken nur kurz umrissen.

Intelligente Messsysteme und intelligente Netze sollen eine intelligente und rationelle Erzeugung, Verteilung und Nutzung von Energie fördern.

---

[7] Am 17. Januar 2013 wurde das Muster für die Datenschutzfolgenabschätzung auch dem Rat der europäischen Energieregulierungsbehörden (CEER) vorgelegt. In seinem Antwortschreiben vom 5. März begrüßte der CEER-Präsident die von der Sachverständigengruppe 2 durchgeführten Arbeiten und den von ihr erarbeiteten Entwurf des Musters. In seinem Schreiben bekräftigte er, dass die Sicherheit und der Datenschutz einen hohen Stellenwert einnehmen und die Kontrolle der Kunden über ihre Daten notwendig sei. Er verwies auf die im Jahr 2011 veröffentlichte Stellungnahme der CEER und forderte zu raschem Handeln bei der Fertigstellung des Musters auf.

[8] Artikel-29-Datenschutzgruppe: Stellungnahme 12/2011 zur intelligenten Verbrauchsmessung („Smart Metering“), angenommen am 4. April 2011 (WP183).

[9] Die Stellungnahme des Europäischen Datenschutzbeauftragten ist auf der EDBS-Website verfügbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_DE.pdf.

Zentrales Merkmal der intelligenten Gas- und Stromverbrauchsmessgeräte ist, dass sie die Möglichkeit für eine Fernkommunikation zwischen dem Messgerät und Energieversorgern, Netzbetreibern und anderen Dritten bieten. Außerdem kann durch intelligente Verbrauchsmessgeräte die Kommunikationshäufigkeit erhöht werden. Mit intelligenten Messsystemen ist es möglich, den Energieverbrauch sehr viel häufiger, z. B. alle 15 Minuten, zu erfassen.

Intelligente Messsysteme sind wichtige Bausteine für das intelligente Stromversorgungsnetz („Smart Grid"). Bei intelligenten Stromversorgungsnetzen handelt es sich um für die bidirektionale Kommunikation ausgelegte Elektrizitätsnetze, in denen Informationen der Verbraucher im Netz kombiniert werden, womit unter anderem der Zweck verfolgt wird, die Stromversorgung wirksamer und wirtschaftlicher planen zu können.

Die europaweite Einführung intelligenter Verbrauchsmessgeräte ermöglicht eine weitreichende Erhebung personenbezogener Daten europäischer Haushalte mit einem Detaillierung- und Erfassungsgrad, wies es ihn bisher noch nie gegeben hat: Die intelligente Verbrauchsmessung bietet die Möglichkeit, den Alltag der Menschen in ihren eigenen Wohnungen nachzuvollziehen und für jede Person auf Basis ihrer häuslichen Tätigkeiten detaillierte Profile zu erstellen.

Aus den detaillierten Energieverbrauchsdaten, die über die intelligenten Messsysteme erfasst werden, können zahlreiche Informationen in Bezug auf die Nutzung bestimmter Güter oder Geräte, die Alltagsgewohnheiten, Wohnsituation, Aktivitäten, Lebensführung und Verhaltensweisen abgeleitet werden.[10]

Die Nutzung intelligenter Netze und intelligenter Messsysteme schafft somit für die betroffenen Personen neue Risiken mit potenziellen Auswirkungen in unterschiedlichen Bereichen (z. B. Preisdiskriminierung, Erstellung von Profilen für verhaltensbezogene Werbung, Besteuerung, Zugang für Strafverfolgungsbehörden, Sicherheit des Haushalts), die es im Energiesektor bisher noch nicht gab und die nur in anderen Umgebungen (Telekommunikation, elektronischer Handel und Web 2.0) typischerweise vorhanden waren.

Die intelligente Verbrauchsmessung zählt außerdem zu den ersten weit verbreiteten Anwendungen, die das zukünftige „Internet der Dinge" erkennen lassen. Die mit der Erhebung und Verfügbarkeit detaillierter Energieverbrauchsdaten verbundenen Risiken werden in Zukunft vermutlich weiter zunehmen, da immer mehr Daten aus anderen Quellen − z. B. Geopositionsdaten, Daten aus der Verfolgung des Verbraucherverhaltens und der Profilerstellung im Internet, Videoüberwachungssysteme und Systeme zur Funkfrequenzidentifikation (RFID) – zur Verfügung stehen werden, mit denen Daten aus der intelligenten Verbrauchsmessung kombiniert werden können.[11]

---

[10] Es wurde beispielsweise nachgewiesen, dass mit einem Ableseintervall von zwei Sekunden ein Rückschluss auf die im Haushalt konsumierten Multimedia-Inhalte möglich ist: http://www.its.fh-muenster.de/greveler/pubs/preprint_online.pdf.

[11] Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling (angenommen vom Ministerkomitee am 23. November 2010).

1.3 Mit dem Muster verfolgte Ziele

Mit ihrer Empfehlung will die Europäische Kommission die für die Datenverarbeitung Verantwortlichen dazu anhalten, eine Datenschutzfolgenabschätzung durchzuführen, mit der die folgenden positiven Ergebnisse erreicht werden sollen:

- Eine Datenschutzfolgenabschätzung sollte eine Beschreibung der geplanten Verarbeitungsvorgänge, eine Bewertung der hinsichtlich der Rechte und Freiheiten der betroffenen Personen bestehenden Risiken, der geplanten Maßnahmen, die im Zusammenhang mit den Risiken ergriffen werden, der Garantien, Sicherheitsvorkehrungen und der Verfahren enthalten, mit denen der Schutz personenbezogener Daten gewährleistet und die Einhaltung der Richtlinie 95/46/EG nachgewiesen wird.

- Eine Datenschutzfolgenabschätzung sollte außerdem den nationalen Datenschutzbehörden Hilfestellung dabei geben, die Übereinstimmung der Verarbeitung mit den einschlägigen Rechtsvorschriften und insbesondere die Risiken für den Schutz personenbezogener Daten der betroffenen Personen und die damit zusammenhängenden Garantien zu beurteilen, wenn die für die Datenverarbeitung Verantwortlichen diese Behörde – wie in der Empfehlung der Kommission vorgesehen – vor der Datenverarbeitung konsultieren.[12] Die Datenschutzfolgenabschätzungen sollten somit also den für die Datenverarbeitung Verantwortlichen bei dem Nachweis unterstützen, dass die Vorschriften der Richtlinie 95/46/EG eingehalten werden.[13]

Darüber hinaus können Datenschutzfolgenabschätzungen dazu beitragen, dass Verbraucher, die für die Datenverarbeitung Verantwortlichen, Datenschutzbehörden, Energieregulierungsbehörden, Verbraucherschutzorganisationen und weitere beteiligte Akteure tieferen Einblick in die konkreten Datenschutzaspekte von intelligenten Messsystemen und Anwendungen für intelligente Netze erhalten. Anhand der Informationen aus Datenschutzfolgenabschätzungen können die Datenschutzbehörden eventuell auch bewährte Vorgehensweisen und mögliche mit hohen Risiken behaftete Bereiche aufzeigen, bei denen eine Prüfung in Betracht zu ziehen ist.

In Mitgliedstaaten, die eine Vorabmitteilung/Vorabprüfung für intelligente Messsysteme und Anwendungen für intelligente Netze vorschreiben, kann durch die Datenschutzfolgenabschätzung der Prozess für die Datenschutzbehörden und die für die Datenverarbeitung Verantwortlichen vereinfacht werden. Datenschutzfolgenabschätzungen sollen den für die Datenverarbeitung Verantwortlichen also auch bei dem Nachweis unterstützen, dass die Vorschriften der Richtlinie 95/46/EG eingehalten werden.

---

[12] Diese Empfehlung gilt unbeschadet einer rechtlichen Verpflichtung zur Vorabprüfung in den Mitgliedstaaten entsprechend den Merkmalen der Verarbeitungsabläufe.

[13] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl. L 281 vom 23.11.1995, S. 31.

Abschließend sei besonders darauf hingewiesen, dass der Vorschlag für eine Datenschutz-Grundverordnung[14] die Bedeutung des Prozesses der Datenschutzfolgenabschätzung unterstreichen würde, der als wichtiges Instrument gilt, mit dem die Rechenschaftspflicht der für die Datenverarbeitung Verantwortlichen gewährleistet werden soll.

1.4 Zusammenfassung des vorgeschlagenen Musters

Wie die Sachverständigengruppe 2 erläutert, griff sie auf die Erfahrungen aus der Entwicklung des „Vorschlags der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen“ sowie dessen Überarbeitung im Nachgang zu Kommentaren und Stellungnahmen der Artikel-29-Datenschutzgruppe („Datenschutzgruppe“) als Ausgangspunkt für ihre Arbeit zurück.

In dem von der Sachverständigengruppe 2 vorgeschlagenen Muster werden zunächst die Ziele, der Umfang, die Vorteile und die an dem Prozess beteiligten Akteure erläutert. Anschließend wird ein Konzept für die Durchführung einer Datenschutzfolgenabschätzung in acht Schritten entwickelt, das dem für die Datenverarbeitung Verantwortlichen Schritt für Schritt Hilfestellung bei der Durchführung der Datenschutzfolgenabschätzung bietet.

2 Analyse des Musters

Die Datenschutzgruppe würdigt die umfangreichen Arbeiten, die von den beteiligten Akteuren der Sachverständigengruppe 2 geleistet wurden, und begrüßt die in den einleitenden Abschnitten des Musters genannten Hauptziele.

Die Datenschutzgruppe hält das im vorgeschlagenen Muster skizzierte Konzept in acht Schritten zwar grundsätzlich für geeignet, macht jedoch in Bezug auf die Methode und den Inhalt des Musters gewisse wesentliche Bedenken geltend, die in den folgenden Abschnitten detailliert dargestellt werden.

2.1 Mangelnde Klarheit in Bezug auf den Charakter und die Ziele der Datenschutzfolgenabschätzung

Gemäß Abschnitt 3 Buchstabe c der Empfehlung der Kommission bezeichnet eine Datenschutzfolgenabschätzung *„ein systematisches Verfahren zur Bewertung der potenziellen Auswirkungen von Risiken in Fällen, in denen Verarbeitungen*,“ die von dem für die Verarbeitung Verantwortlichen oder vom Auftragsverarbeiter oder von dem im Namen des Verantwortlichen handelnden Auftragsverarbeiter durchzuführen sind, *„aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können*.“

[14] Am 25. Januar 2012 nahm die Kommission ein Paket zur Reform des europäischen Datenschutzrahmens an. Das Paket umfasst (i) eine Mitteilung (KOM(2012) 9 endgültig, (ii) einen Vorschlag für eine Datenschutz-Grundverordnung (KOM(2012) 11 endgültig) und (iii) einen Vorschlag für eine Datenschutzrichtlinie (KOM(2012) 10 endgültig).

Die Datenschutzgruppe unterstützt diese Definition und betont, dass das Ziel einer Datenschutzfolgenabschätzung folglich darin bestehen sollte, die Auswirkungen der Risiken auf die betroffenen Personen zu beurteilen.

Die Datenschutzgruppe bedauert jedoch, dass sich das vorgelegte Muster nicht direkt mit den tatsächlichen Auswirkungen auf die betroffenen Personen befasst, beispielsweise finanzielle Verluste wegen fehlerhafter Gebührenabrechnungen, Preisdiskriminierung oder Straftaten, die durch eine zu Unrecht erfolgte Profilerstellung begünstigt werden. Auch wenn die in Anhang I aufgeführten Ziele in Bezug auf den Datenschutz und die Privatsphäre sehr hilfreich sein können, um die Einhaltung der einschlägigen Vorschriften zu vereinfachen, reichen sie für einen risikogesteuerten Ansatz nicht aus. Die Bewertung der potenziellen Auswirkungen auf die betroffenen Personen ist ein unerlässlicher Bestandteil eines derartigen Konzepts.

Die Datenschutzgruppe hält das Muster in der gegenwärtigen Form somit für nicht geeignet, das in der Empfehlung der Kommission vorgegebene Ziel zu erreichen. Das Muster bietet kein praktisches Hilfsmittel für die Bewertung der Auswirkungen auf die betroffenen Personen.

Wenn die Risiken und ihre Auswirkungen auf die betroffenen Personen nicht in ihrer Gesamtheit berücksichtigt werden, können die notwendigen Kontrollen und Garantien nicht einwandfrei ermittelt und eingeführt werden.

2.2 Methodische Mängel im Muster

Nach Ansicht der Datenschutzgruppe enthält das Muster neben der oben genannten zentralen Schwachstelle eine Reihe methodischer und gelegentlich mit dieser zentralen Schwachstelle im Zusammenhang stehender Mängel, welche die Anwendung des Musters gefährden.

Erstens werden Risiken und Bedrohungen im vorgeschlagenen Muster oftmals verwechselt.[15]

Zweitens findet keine Gegenüberstellung der zu mindernden Risiken und der Liste der möglichen Kontrollen in Anhang II statt. Auch wenn jedes Risikoszenario eigene Besonderheiten aufweist, die es bei der Bewertung zu berücksichtigen gilt, können oftmals bestimmte Kontrollkategorien aufgezeigt werden, die wirksam für die Minderung bestimmter Risikokategorien sind. Ein typisches Beispiel dafür findet sich

[15] Siehe ISO/IEC 27005:2008 Darin wird das Risiko im Bereich der Informationssicherheit wie folgt definiert: „the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization“ (die Möglichkeit, dass eine Bedrohung Schwachstellen in Anlagen ausnutzt und dadurch dem Unternehmen Schaden zufügt). Für Bedrohungen gibt es keine explizite Definition, jedoch kann aus ISO/IEC 27001:2005 eine Arbeitsdefinition abgeleitet werden. Demzufolge beziehen sich Bedrohungen auf die Fähigkeit, Schwachstellen in den zu schützenden Anlagen auszunutzen. Dies führt bei diesen Anlagen zu einem Verlust der Sicherheitseigenschaften. Beispiele für typische sicherheitsrelevante Bedrohungen sind in Anhang C der internationalen Norm ISO/IEC 27005:2008 aufgeführt.
Siehe auch die Methodik der CNIL unter http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf und die Bedrohungslage laut ENISA-Bericht unter https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport).

in der internationalen Norm für Informationssicherheit (ISO/IEC 27002:2005), in der Kontrollen als bewährte Vorgehensweise zur Minderung der Risiken in bestimmten Bereichen dargestellt werden. Die vorgeschlagenen Maßnahmen zur Risikominderung ersetzen zwar keinen risikogesteuerten Prozess, können jedoch einen Bezugsrahmen für ein effektives und kohärentes Konzept abgeben. Beispielsweise kann das Risiko, dass über einen ungeschützten Kanal übermittelte Energieverbrauchsdaten der Verbraucher abgefangen werden, im Allgemeinen durch Verschlüsselungstechniken gemindert werden. Die spezifische Risikobewertung könnte dazu führen, dass bestimmte Verschlüsselungsalgorithmen und Schlüssellängen oder alternative oder ergänzende Maßnahmen zur Risikominderung eingeführt werden oder gar Risiken in Kauf genommen oder transferiert werden (durch Verzicht auf risikomindernde Maßnahmen).

Darüber hinaus enthält das vorgeschlagene Muster keine ausreichend detaillierten und spezifischen Leitlinien zum Begriff der Schwachstelle, zur Berechnung und Priorisierung von Risiken, zur Festlegung angemessener Kontrollen und zur Beurteilung der Restrisiken nach der Einführung der Kontrollen. Es wird zwar auf ein externes Dokument verwiesen, doch hätte die Datenschutzgruppe weiter gehende Hilfestellungen und Erläuterungen im Muster selbst begrüßt, um dem Leser ein eigenständiges Dokument an die Hand zu geben. Außerdem ist nicht klar, wie die vorgeschlagenen Formulare auszufüllen sind.

Zudem enthält das Muster keine ausreichenden Orientierungshilfen für die Festlegung der Aufgaben und Zuständigkeiten der verschiedenen Akteure aus Sicht des Datenschutzes. Das Muster verweist an dieser Stelle lediglich auf ein anderes Dokument der Sachverständigengruppe 2. Die künftigen Anwendungen für intelligente Netze werden vielfältige Formen annehmen und von unterschiedlichen Akteuren angeboten. Daher erscheint es sehr wichtig, der Branche Leitlinien an die Hand zu geben, die eine Bestimmung der für die Datenverarbeitung Verantwortlichen und der Auftragsverarbeiter ermöglichen. Beispielsweise könnte im Muster im dritten Schritt ein vierter Abschnitt angefügt werden, mit dem die Zuständigkeiten der an der Datenverarbeitung beteiligten Akteure aufgezeigt werden sollen.

Weitere Einzelheiten zu diesen und weiteren methodischen Mängeln sind in Anhang 1 aufgeführt.

2.3 Das Muster enthält zu wenig sektorspezifische Informationen: Branchenspezifische Risiken und entsprechende Kontrollen zur Minderung dieser Risiken sollten festgestellt und einander gegenübergestellt werden

Das Muster enthält zu wenig sektorspezifische Inhalte. Die im Muster aufgeführten Risiken und Kontrollen sind sehr allgemein gehalten und enthalten nur gelegentlich branchenspezifische Leitlinien, etwa bewährte Vorgehensweisen, die von echtem Nutzen sein könnten. In den Risiken und Kontrollen kommen somit nicht die Erfahrungen der Branche mit den zentralen Fragestellungen und bewährten Vorgehensweisen zum Ausdruck.

Nach dem Kenntnisstand der Datenschutzgruppe stellt die Sachverständigengruppe 2 derzeit so genannte „beste verfügbare Techniken“ zusammen, aus denen eine

Organisation, die eine Datenschutzfolgenabschätzung durchführen will, bei Bedarf geeignete Maßnahmen auswählen könnte, womit einige der im vorigen Abschnitt genannten Kritikpunkte gegenstandslos würden. Damit könnte. Die Datenschutzgruppe unterstreicht den hohen Stellenwert dieses Dokuments als Ergänzung zum Muster.

Das Dokument mit den besten verfügbaren Techniken kann jedoch nicht die Benennung der häufigsten branchenspezifischen Risiken und die Gegenüberstellung zu den möglichen Kontrollen im eigentlichen Muster ersetzen. Dies gilt umso mehr, als – anders als das Muster – das Dokument mit den besten verfügbaren Techniken der Datenschutzgruppe nicht zur weiteren Evaluierung und Beratung vorgelegt wird und auch keine Annahme durch die Kommission geplant ist. Angesichts der im Muster festgestellten Mängel sollte die Kommission in Erwägung ziehen, die besten verfügbaren Techniken in das Muster aufzunehmen, und das integrierte Dokument der Datenschutzgruppe zur Stellungnahme vorlegen.

Außerdem besteht ein Unterschied zwischen einem „Muster für die Datenschutzfolgenabschätzung“ und einem „Rahmen für die Datenschutzfolgenabschätzung“. In einem derartigen Rahmen sollten Ziele formuliert, eine Methode skizziert und der Umfang der Bewertung im Hinblick auf die Grenzen des analysierten Systems/Prozesses festgelegt werden. Ein Muster sollte darüber hinausgehen und mit ihm sollte ein funktionierendes Instrument zur Steuerung der Risiken der konkreten Systeme/Prozesse und ihrer Anwendungsfällen bereitgestellt werden sowie mögliche Kontrollen und die besten verfügbaren Techniken zur Minderung dieser Risiken unterbreitet und ein konkreter Orientierungsrahmen vermittelt werden. Dies ist insbesondere in Fällen notwendig, in denen nicht auf spezifisches Fachwissen zurückgegriffen werden kann (z. B. in KMU oder − wie im Falle der intelligenten Netze − in einer Branche, in der Fragen der Privatsphäre und des Datenschutzes bisher nur wenig Beachtung geschenkt wurde).

Ziel des Musters sollte die Entwicklung von Leitlinien sein, die einfacher anwendbar und stärker auf die einzelnen Sektoren zugeschnitten sind. Vor allem ist es notwendig, die möglichen Auswirkungen auf die betroffenen Personen im Zusammenhang mit intelligenten Netzen besser zu definieren und präzisere Leitlinien für die Art der anwendbaren Kontrollen zu formulieren.

Die Kommission hätte der Sachverständigengruppe 2 eine allgemeingültige Methode zur Abschätzung der Risiken für die Privatsphäre und den Datenschutz vorlegen können[16]. Die Sachverständigengruppe 2 hätte diese Methode wiederum anwenden und auf dieser Basis das Muster sektorspezifischer gestalten können. Bei dieser Vorgehensweise hätte sich die Sachverständigengruppe 2 auf relevante Fragestellungen wie spezifische Risiken und Kontrollen in intelligenten Netzen konzentrieren und sich bei grundlegenden methodischen Aspekten auf diesen Bezugsrahmen stützen können. Die Datenschutzgruppe schlägt vor, dass die Sachverständigengruppe 2 und die Kommission bei der Weiterentwicklung dieses Musters und bei weiteren sektorspezifischen Mustern diese Vorgehensweise verfolgen.

[16] Siehe z. B. die bereits oben angeführte Methodik der CNIL.

3 Schlussfolgerung und Empfehlungen

Die Datenschutzgruppe begrüßt die gegenüber den früheren Versionen erzielten Fortschritte und die zweckdienlichen Elemente, die das Muster bereits enthält. Dennoch vertritt sie die Ansicht, dass das Muster in seiner gegenwärtigen Form noch nicht genug ausgereift und entwickelt ist.

Daher empfiehlt die Datenschutzgruppe der Kommission, die notwendigen Schritte einzuleiten, um sicherzustellen, dass die Arbeiten am Muster weitergeführt werden und das endgültige Muster den für die Datenverarbeitung Verantwortlichen ausreichend konkrete, nützliche und eindeutig praxisbezogene Hilfestellung bietet.

Zur Erleichterung der weiteren Arbeiten gibt die Datenschutzgruppe in Anhang 1 dieser Stellungnahme verschiedene konkretere Empfehlungen ab. Angesichts dessen, dass das Dokument methodische Mängel aufweist und im Zusammenhang mit intelligenten Netzen nicht hinreichend spezifisch aufgebaut ist, ist die Datenschutzgruppe gegenwärtig nicht in der Lage, weitere, detailliertere und schlüssige Kommentare dazu zu unterbreiten.

Angesichts der im Muster festgestellten Mängel empfiehlt die Datenschutzgruppe außerdem, dass die Kommission die Aufnahme der besten verfügbaren Techniken in das Muster in Betracht ziehen und das integrierte Dokument der Datenschutzgruppe zur Stellungnahme vorlegen sollte.[17]

Außerdem empfiehlt die Datenschutzgruppe der Kommission ganz allgemein, eine Bestandsaufnahme der bisherigen und laufenden Arbeiten auf dem Gebiet der Datenschutzfolgenabschätzungen[18] durchzuführen und zu prüfen, ob es sinnvoll wäre, eine allgemeingültige Methode für Datenschutzfolgenabschätzungen festzulegen, die für branchenspezifische Aktivitäten von Nutzen wäre.

In Bezug auf die Notwendigkeit einer verbindlichen Folgenabschätzung verweist die Datenschutzgruppe abschließend auf die Erfahrungen, die mit dem Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen gesammelt wurden, und erinnert daran, dass Folgenabschätzungen für RFID-Anwendungen laut den in den Mitgliedstaaten vorhandenen Statistiken nur sehr selten durchgeführt wurden. Dafür können zwar mehrere Ursachen in Betracht kommen, doch einer der wichtigsten Gründe dürfte eindeutig darin bestehen, dass die Durchführung einer derartigen Folgenabschätzung derzeit nicht zwingend vorgeschrieben ist.

Brüssel, den 22. April 2013

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

---

[17] Dies schließt nicht aus, dass das Dokument mit den besten verfügbaren Techniken regelmäßig aktualisiert werden könnte, um technische Änderungen und den neuesten Stand der Technik darin aufzunehmen.

[18] Siehe z. B. das PIAF-Projekt unter http://www.piafproject.eu/Index.html sowie die zuvor genannten Methoden.

Anhang 1: Besondere Anmerkungen zum Muster

Der vorliegende Anhang ergänzt Abschnitt 2 der Stellungnahme. Die Kommentare folgen dem Aufbau des Musters.

→ Umfang der Datenschutzfolgenabschätzung

- Das Muster enthält keine genaue Definition und Beschreibung der Arten der Datenverarbeitungstätigkeit, die einer Datenschutzfolgenabschätzung unterliegen. Außerdem wird der Umfang der Datenschutzfolgenabschätzung in Abschnitt 1.2 des Musters nicht genau festgelegt. In der Empfehlung der Kommission wird eine Datenschutzfolgenabschätzung klar definiert als „ein systematisches Verfahren zur Bewertung der potenziellen Auswirkungen von Risiken in Fällen, in denen Verarbeitungen […] aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten können". Diese Definition schließt die in Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union („die Charta") verankerten Grundrechte bzw. das Recht auf Achtung der Privatsphäre und das Recht auf den Schutz personenbezogener Daten ein. Hierbei ist zu berücksichtigen, dass sich das Muster auf den Schutz personenbezogener Daten gemäß Richtlinie 95/46/EG bezieht.[19]
- Wie bereits in den allgemeinen Bemerkungen angeführt, sollte sich das Muster hauptsächlich mit den Auswirkungen auf die betroffenen Personen befassen. Die Erfüllung der in Anhang I genannten Vorgaben für den Schutz der Privatsphäre und den Datenschutz sowie die Beachtung des Rechts auf Datenschutz sind zwar wichtig, allerdings stellt die Einhaltung datenschutzrechtlicher Bestimmungen für sich genommen keinen Selbstzweck dar. Der Prozess der Datenschutzfolgenabschätzung zielt letztlich darauf ab, Kontrollen aufzuzeigen, die etwaige negative Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen so gering wie möglich halten.
- Die folgenden Beispiele dienen zur Veranschaulichung des Unterschieds zwischen einer Vorgehensweise, die sich auf eine reine Prüfung der Einhaltung von Vorgaben beschränkt, und einer Vorgehensweise, die auf einer Abschätzung der realen Risiken mit ebenso realen Auswirkungen auf das Leben der betroffenen Personen basiert.
    - Kriminalitätsbezogene Risiken: sind die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit von Energieverbrauchsdaten unzureichend, besteht die Gefahr des unrechtmäßigen Zugriffs auf die Energieverbrauchsdaten einzelner Haushalte. Dadurch kann das Risiko des betroffenen Verbrauchers steigen, Opfer einer Straftat zu werden. Die Kenntnis der Verhaltensmuster, die sich aus den Energieverbrauchsdaten ableiten lassen, insbesondere, ob ein Haus zu bestimmten Zeiten unbewohnt ist, könnte z. B. das Einbruchs- und Diebstahlrisiko erhöhen.

[19] Jegliche Verweise auf den Begriff „Schutz der Privatsphäre" (engl. data privacy) oder Versuche einer *Ad-hoc*-Definition für „Privatsphäre" (engl. privacy) in Abschnitt 1.2 oder im Glossar sind nicht notwendig und könnten irreführend sein. Es sollte nach Möglichkeit stets die Terminologie der Richtlinie 95/46/EG verwendet werden. Artikel 7 und 8 der Charta können zitiert und zur weiteren Orientierung angeführt werden.

- Die Manipulation von Energieverbrauchsdaten könnte dazu führen, dass den betroffenen Personen Gebühren zu Unrecht in Rechnung gestellt werden.[20]
- Profilerstellung, Ausgrenzung, Diskriminierung, unerbetene Marketingmaßnahmen: Mit der steigenden Verfügbarkeit von Daten über Verbraucher in intelligenten Netzen könnten immer mehr Datenprofile erstellt werden. Dies könnte wiederum zu Preisdiskriminierung und Ausgrenzung (z. B. Aufnahme in Schwarze Listen, höhere Tarife), unerbetene, auf das Verbraucherverhalten zugeschnittene Werbung sowie zu einem allgemeinen Ungleichgewicht in der wirtschaftlichen Lage des Verbrauchers gegenüber den Dienstleistern/für die Datenverarbeitung Verantwortlichen führen, das die Gefahr eines späteren Missbrauchs birgt.
- Risiken der mit den Rechtsvorschriften unvereinbaren und unrechtmäßigen Nutzung der Daten durch Strafverfolgungsbehörden oder sonstige Dritte, Risiko einer erhöhten staatlichen Überwachung (das z. B. gemindert werden könnte, indem die Verarbeitung personenbezogener Daten auf ein Minimum beschränkt wird).

- Diese und weitere Beispiele für Risiken und mögliche Auswirkungen auf die betroffenen Personen sollten berücksichtigt und in die Folgenabschätzung aufgenommen werden.

→Beteiligte Akteure

- Im Muster wird nicht auf die Aufgaben und Funktionen der verschiedenen Akteure im Zusammenhang mit intelligenten Netzen eingegangen, folglich werden auch nicht ihre Zuständigkeiten nicht gegeneinander abgegrenzt. Intelligente Netze können ihre Ziele jedoch nur mit durch organisierte Zusammenarbeit und den Datenaustausch zwischen den beteiligten Organisationen erreichen. Für eine aussagekräftige Datenschutzfolgenabschätzung ist die Zusammenarbeit aller Beteiligten erforderlich. Das vorgeschlagene Muster gibt keine ausreichende Hilfestellung dabei, wie eine Datenschutzfolgenabschätzung vorzunehmen ist, wenn mehrere Betreiber beteiligt sind, die entsprechende Datenverarbeitungen durchführen.
- Abschnitt 1.3.3: „Betreiber intelligenter Netze“ ist eine sehr allgemeine Bezeichnung, die nicht berücksichtigt, dass verschiedene Akteure unterschiedliche Funktionen in intelligenten Netzen wahrnehmen können, wodurch die Grenzen und der Umfang der durchgeführten Datenschutzfolgenabschätzung erheblich beeinflusst werden.[21] Bei der Beschreibung dieser Funktionen sollte der Schwerpunkt auf ihrer Aufgabe beim Austausch personenbezogener Daten liegen, die für die Ausführung der Geschäftsprozesse in intelligenten Netzen notwendig sind. Das Muster sollte eine prägnante und aktuelle Definition der Aufgaben aller am Prozess der

[20] Ähnliche Risiken bei der Gebührenabrechnung bestehen eventuell auch bei Eigentümern von Solarmodulen oder Mikroanlagen zur Erzeugung von Wärme und Strom.

[21] Siehe z. B. http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGConceptualModel#Smart_Grid_Conceptual_Model_Doma.

Datenschutzfolgenabschätzung Beteiligten enthalten (siehe z. B. den Bericht der Sachverständigengruppe vom 16. Februar 2011[22]).

- Außerdem sollte nochmals ausdrücklich auf die Notwendigkeit, die geltenden Rechtsvorschriften einzuhalten, hingewiesen werden.
- Im Muster sollten auch (i) die Empfänger der Daten und (ii) die Datenschutzbeauftragten (sofern vorhanden) der Organisation als beteiligte Akteure erwähnt werden.

→ Schritt 1

- Die Kriterien für die Vorabbewertung müssen erneut auf den Prüfstand gestellt werden. Dementsprechend ist auch der Fragebogen in Abschnitt 3.1 zu überarbeiten. Dies ist auch zur Gewährleistung der Übereinstimmung mit Abschnitt 2.1 notwendig.
- Die Reihenfolge der Kriterien sollte entsprechend der logischen Reihenfolge geändert werden, in der sie untersucht werden:
    1. Werden personenbezogene Daten verarbeitet?
    2. Ist die Organisation der für die Datenverarbeitung Verantwortliche?
    3. Wirkt sich die Datenverarbeitung auf die Rechte und Freiheiten aus?
    4. Wann ist der richtige Zeitpunkt, und wie lässt sich dieser begründen?
- Im Muster sind unter den Arten von Daten, die als personenbezogene Daten gelten können, auch eindeutig nicht personenbezogene Daten aufgeführt (Bedarfsprognose für Gebäude, Campus und Organisation). Demgegenüber sind Daten, die auch personenbezogen sein können, entweder nicht oder an der falschen Stelle aufgeführt (z. B. kann die Innentemperatur eines Hauses den personenbezogenen Daten zugerechnet werden, da sie einen Rückschluss darauf zulässt, ob das Haus bewohnt wird; die Abfolge der Standorte, an denen ein Elektrofahrzeug aufgeladen wurde, sind personenbezogene Daten, da sie Aufschluss über den Standort des Fahrzeugführers geben usw.). Es sollte mehr Hilfestellung gegeben werden, um die Organisation bei der Identifizierung der personenbezogenen Daten zu unterstützen, die einer Verarbeitung unterzogen werden.
- Des Weiteren sollte auch bei Kriterium 1 eine Datenschutzfolgenabschätzung für bestehende Systeme ohne konzeptionsbedingten Datenschutz („data protection by design“) durchgeführt werden, die bisher noch keiner Datenschutzfolgenabschätzung unterzogen wurden. Dies sollte im Text hervorgehoben werden, indem z. B. ein zusätzlicher Aufzählungspunkt in die Liste der auslösenden Ereignisse aufgenommen wird, die bereits unter der Überschrift „Right timing“ (Wahl des richtigen Zeitpunkts) oder in einem gesonderten Absatz nach der Liste mit den Aufzählungspunkten aufgeführt sind.

[22] Siehe http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

→ Schritt 2

- Sofern die Ressourcen der Organisation dies erlauben, sollte unbedingt dafür gesorgt werden, dass das Team, das die Datenschutzfolgenabschätzung durchführt, von dem mit der eigentlichen Anwendung für intelligente Netze arbeitenden Team unabhängig ist. Dies trägt zur Fairness und Objektivität der Datenschutzfolgenabschätzung bei: Diese Vorgabe ist im Dokument nicht enthalten.

→ Schritt 3

- In der Beschreibung des Systems fehlt eine klare Angabe der Anlagen (Assets), auf die sich die Verarbeitung personenbezogener Daten stützt (z. B. eine Datenbank, die als Speicherort für die in einem bestimmten Bereich erhobenen Daten dient). Dies wäre jedoch wichtig, da bestimmte Bedrohungen auch auf diese Anlagen zielen. Außerdem sind die verschiedenen Arten der verarbeiteten personenbezogenen Daten, ihre Zweckbestimmung und die Art ihrer Verarbeitung umfassend zu identifizieren. Ihre vorgeschlagene Aufbewahrungsdauer ist ebenfalls anzugeben.

→ Schritt 4

- Dieser Schritt basiert hauptsächlich auf der Liste der Bedrohungen, die in den Fragebogen des Musters aufgeführt sind. Bedrohungen und Risiken scheinen gelegentlich miteinander verwechselt zu werden (siehe Abschnitt 2.2 dieser Stellungnahme). Bei einigen der genannten Punkte handelt es sich eher um „fehlende Maßnahmen“ (z. B. unzureichender Erfassungsmechanismus, uneinheitliche Mechanismen für Ersuchen um Dateneinsichtnahme durch die betroffene Person) als um Bedrohungen.

→ Schritt 5

- Die Bedrohungen für den Datenschutz werden im Hinblick auf die in Anhang I genannten Auswirkungen auf die Privatsphäre und Datenschutzziele gewichtet, und nicht im Hinblick auf die Auswirkungen für die betroffenen Personen. Außerdem gibt das Muster keine angemessene Hilfestellung zur Art der Auswirkungen und zur Methode.
- Die Eintrittswahrscheinlichkeit des Risikos wird beschrieben als Kombination aus der Anfälligkeit und der Leichtigkeit, mit der eine Schwachstelle ausgenutzt werden kann. Da die Anlagen, auf denen personenbezogene Daten gespeichert sind, in Schritt 3 jedoch nicht benannt werden, gibt es keinen Anhaltspunkt dafür, worauf sich die Anfälligkeit oder Schwachstelle bezieht.

→ Schritt 6

- Es ist sehr wichtig, dass im Muster jedem Risiko eine oder mehrere angemessene Kontrollen zur Risikominderung gegenübergestellt werden (und zugleich verdeutlicht, dass bestimmte Risiken in hinreichend begründeten Fällen auch übertragen oder in Kauf genommen werden können). Diese Gegenüberstellung sollte als zentraler Bestandteil in das Dokument

aufgenommen werden. Die gegenwärtige Struktur des Musters lässt diese integrierte Vorgehensweise jedoch nicht zu, wie die Datenschutzgruppe bereits in ihrem Schreiben vom Oktober 2012 anmerkte.

- In Bezug auf die Restrisiken (Abschnitt 6) wurde von der Datenschutzgruppe bereits in ihren Kommentaren vom Oktober 2012 erwähnt, dass das Recht auf den Schutz personenbezogener Daten ein Grundrecht darstellt und die Einhaltung datenschutzrechtlicher Anforderungen als klare gesetzliche Vorgabe auf hoher Ebene zu verstehen ist. Dies sollte beim Verweis auf die Möglichkeit, gewisse Restrisiken in Kauf zu nehmen, noch deutlicher herausgestellt werden: Hier könnte erläutert werden, dass unabhängig vom Ergebnis der Risikobewertung die Ziele des Datenschutzes und der Achtung der Privatsphäre auf jeden Fall einzuhalten sind: Beispielsweise müssen die betroffenen Personen in allen Fällen entsprechend informiert werden, und es müssen rechtlich fundierte Gründe für die Verarbeitung vorliegen (z. B. eine rechtliche Verpflichtung oder rechtswirksame Einwilligung durch die betroffene Person). Es muss deutlich betont werden, dass das Datenschutzvorschriften in jedem Fall einzuhalten sind. Die Risikobewertung kann als Hilfestellung dienen, wie datenschutzrechtliche Bestimmungen am besten eingehalten werden. Sie kann z. B. Anhaltspunkte dafür geben, welche Art der Datenverschlüsselung verwendet werden sollte, um eine angemessene Datensicherheit zu gewährleisten, welche Aufbewahrungsfristen als angemessen gelten oder wie der Umfang der erhobenen und weiterverarbeiteten Daten so gering wie möglich gehalten wird. Die Risikobewertung sollte jedoch nicht als Vorwand für die Nichteinhaltung gesetzlicher Vorgaben in Fällen dienen, in denen die Risiken als relativ gering eingeschätzt werden. In diesem Zusammenhang werden auch keine Hinweise gegeben, wie die Höhe des hinnehmbaren Restrisikos bestimmt werden kann.

Anhang II: Liste der möglichen Kontrollen

Die in Anhang II genannten Kontrollen sind nicht hinreichend konkret und bieten den für die Verarbeitung Verantwortlichen somit keine nützliche Hilfestellung. Die meisten Kontrollen gehen nicht auf die Besonderheiten im Zusammenhang mit intelligenten Netzen ein und berücksichtigen nicht die Erfahrungen der Branche mit den zentralen Problemstellungen und bewährten Vorgehensweisen.

Zur Verdeutlichung der Erwartungen, die die Datenschutzgruppe an den Detaillierungsgrad und an Beispiele aus der Praxis stellt, werden nachfolgend einige der wichtigsten Aspekte genannt, die nach Ansicht der Datenschutzgruppe im Muster angesprochen werden sollten.

Rechtsgrundlage und Wahlmöglichkeiten

Die Datenschutzgruppe erwartet vom Muster genauere Hilfestellung bei der Wahl der Rechtsgrundlage der Verarbeitung und den Wahlmöglichkeiten für betroffene Personen. Das Muster sollte insbesondere klare Leitlinien dafür vermitteln, welche Verarbeitungen ohne Einwilligung der betroffenen Person zulässig sind und welche Verarbeitungen die Einwilligung der betroffenen Person erfordern. Besondere Aufmerksamkeit sollte der Möglichkeit zur Fernausschaltung und der Erhebung differenzierter Daten zukommen.[23]

In den meisten Fällen ist eine ohne Zwang, in Kenntnis der Sachlage und für den konkreten Fall erteilte ausdrückliche Einwilligung für alle Verarbeitungen notwendig, die über Verarbeitungen hinausgehen, die erforderlich sind für (i) die Versorgung mit Energie, (ii) die entsprechende Rechnungsstellung, (iii) die Aufdeckung von Betrugsfällen in Form nicht bezahlter Nutzung der bereitgestellten Energie[24] und (iv) die Aufbereitung aggregierter Daten für eine energieeffiziente Instandhaltung des Netzes (Prognosen und Abrechnung).[25] Eine Einwilligung ist beispielsweise bei der Verfolgung und Profilerstellung für zielgerichtete Werbung erforderlich.

Damit die Einwilligung rechtsgültig ist, müssen die Verbraucher verstehen, was mit ihren Daten geschieht. Bei der Erstellung von Datenprofilen sollten sie das Recht auf Zugang zu ihren individuellen Profilen erhalten und auch über die Logik der für das *Data Mining* verwendeten Algorithmen informiert werden. Ebenso wichtig sind Informationen über das Vorhandensein einer Fern-Ein-/Ausschaltungsfunktion: Die Kunden müssen wissen, welche Ereignisse einen Abschaltvorgang auslösen können.

Datenminimierung und Technologien zum besseren Schutz der Privatsphäre

Durch das Muster sollten die betreffenden Unternehmen auch dazu aufgefordert

---

[23] Siehe z. B. Ziffer 48 der Stellungnahme des Europäischen Datenschutzbeauftragten vom 8. Juni 2012, auf die in Fußnote 3 verwiesen wird.

[24] Natürlich muss die Datenverarbeitung zum Zwecke der Betrugsaufdeckung weiterhin alle anderen relevanten Datenschutzgarantien einhalten und unter anderem die Forderung nach Verhältnismäßigkeit und den Grundsatze der Datenminimierung erfüllen.

[25] Diese Zweckbestimmungen, für die keine Einwilligung erforderlich ist, decken sich gewöhnlich mit den gesetzlich geregelten Aufgaben der für die Datenverarbeitung Verantwortlichen.

werden, dafür zu sorgen, dass personenbezogene Daten nur im unbedingt notwendigen Umfang erhoben und verarbeitet werden. Um dieses Ziel zu erreichen, können mehrere Methoden in Betracht kommen. Die Datenschutzgruppe empfiehlt dazu, dass zumindest die gängigsten Technologien zum besseren Schutz der Privatsphäre und weitere „beste verfügbare Techniken" zur Datenminimierung jeweils kurz und technologieneutral im Muster beschrieben und anschließend in dem von der Sachverständigengruppe 2 zu erstellenden Begleitdokument zu den besten verfügbaren Techniken detailliert erläutert werden, so dass die datenschutzfreundliche Einführung von Technologien für intelligente Messsysteme und intelligente Netze gefördert werden kann.

In Forschung und Entwicklung wird gegenwärtig in unterschiedlichen Stadien an innovativen Technologien zum besseren Schutz der Privatsphäre gearbeitet, mit denen sich die grundlegenden Ziele intelligenter Messsysteme (Gebührenabrechnung, energieeffiziente Instandhaltung des Netzes [Prognose und Abrechnung] und Aufrechterhaltung der Sicherheit (einschließlich Verhütung von Betrug)) möglicherweise so erreichen lassen, dass zumindest im Hinblick auf diese grundlegenden Ziele vermieden werden kann, dass extrem differenzierte Messwerte das intelligente Messgerät oder den Haushalt, in dem es installiert ist, überhaupt verlassen müssen. Als weitere erwägenswerte Punkte sind zu nennen:

- Häufigkeit der Ablesung der Messgeräte: Je häufiger die Messgeräte abgelesen werden, desto stärker wird in die Privatsphäre des Betreffenden eingegriffen. Die Datenschutzgruppe würde in dieser Frage mehr Hilfestellung, einschließlich Verweisen[26] und Beispielen, im Muster begrüßen.
- Stichproben: Mit Stichproben (also der Erhebung von Daten nur von einem repräsentativen Prozentsatz aller Haushalte) ließe sich die Erhebung und Verarbeitung von Daten aller Haushalte für bestimmte Zwecke (wie Prognosen) vermeiden. Beispiele dafür sollten ebenfalls in das Muster aufgenommen werden.
- Aggregierung in Verbindung mit Datenlöschung: Für bestimmte Zwecke, zu denen auch Prognosen gehören, sollte es ausreichen, die differenzierten Messwerte nur solange aufzubewahren, bis die Berechnung der Aggregierung abgeschlossen ist. In diesen Fällen können die Daten unmittelbar nach Abschluss der Berechnung dauerhaft gelöscht werden. Auch dies sollte durch Beispiele belegt werden.
- Erhebung aggregierter Daten von vornherein (anstatt der Erhebung von Einzeldaten mit anschließender Aggregierung): Für bestimmte Zwecke (einschließlich Prognosen, Instandhaltung des Netzes und Aufdeckung von Betrug) sollte es für den Betreiber des Strom- oder Erdgasverteilungsnetzes ausreichen, Daten von Zählern zu erheben, die nicht den Verbrauch einzelner Haushalte messen; stattdessen sollte er Daten von Zählern erheben, die an Stellen im Verteilungsnetz angebracht sind, an denen sie nur den aggregierten Verbrauch einer ganzen Reihe von Haushalten messen (z. B. großer

[26] Siehe Sachverständigengruppe 2 (EG2.P.1) in „Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection" (Grundlegende Regulierungsvorgaben und Empfehlungen für die Datenverarbeitung, die Datensicherheit und den Verbraucherschutz) (http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_deliverable.pdf).

Wohnblöcke, einer Straße oder eines Bezirks). In diesen Fällen lässt sich zu diesen Zwecken die Erhebung differenzierter Daten einzelner Haushalte insgesamt vermeiden. Auch hier wären anschauliche Beispiele aus der Praxis im Muster hilfreich, damit die Einhaltung datenschutzrechtlicher Bestimmungen und bewährter Vorgehensweisen gefördert werden kann.

- Um nicht nur den Umfang der erhobenen Daten, sondern auch die Aufbewahrungsfristen der Daten zu minimieren, sollte das Muster auch zusätzliche Leitlinien für die Aufbewahrungsfristen bieten. Nach Ansicht der Datenschutzgruppe sollte grundsätzlich die Speicherung differenzierter Verbrauchsdaten einzelner Haushalte, die für Abrechnungszwecke erhoben werden, nur bis zum Ablauf der Frist zulässig sein, innerhalb derer die Rechnung rechtmäßig angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann (unbeschadet des Rechts des Verbrauchers auf eine längere Speicherfrist, in die er eingewilligt hat, beispielsweise für gezielte Beratung in Energiefragen oder für andere rechtmäßige Zwecke).

Glossar

Die Datenschutzgruppe empfiehlt eine sorgfältige Überprüfung des Glossars, um sicherzustellen, dass die Terminologie im Einklang mit dem allgemeinen Sprachgebrauch der Richtlinie 95/46/EG steht und mit dem vorgeschlagenen neuen Datenschutzrahmen vereinbar ist.