ARTIKEL-29-DATENSCHUTZGRUPPE

2064/13/DE
WP209

Stellungnahme 7/2013 zum Muster für die Datenschutzfolgenabschätzung für intelligente Netze und intelligente Messsysteme, erstellt durch die Sachverständigengruppe 2 der Taskforce der Kommission für intelligente Netze

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 die Empfehlung 2012/148/EU 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 „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 (im Folgenden „Datenschutzgruppe") zur Stellungnahme vorzulegen ist. Anschließend sollten die Mitgliedstaaten dafür Sorge tragen, dass Netzbetreiber und Betreiber intelligenter Messsysteme geeignete technische und organisatorische Maßnahmen zur

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 23.11.95, S. 31-50.

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 seitdem mehrere Workshops durch, an denen Vertreter der Datenschutzgruppe als Beobachter teilnahmen.

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.

Erste Fassung des Musters

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.[4]

Die Datenschutzgruppe veröffentlichte ihre Stellungnahme 4/2013 am 22. April 2013. Die Datenschutzgruppe würdigte die umfangreichen Arbeiten, die von den beteiligten

---

[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] 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.

Akteuren der Sachverständigengruppe 2 geleistet wurden, und begrüßte die genannten Hauptziele. Andererseits machte sie wesentliche Bedenken geltend, die wie folgt zusammengefasst werden können:

i. mangelnde Klarheit in Bezug auf den Charakter und die Ziele der Datenschutzfolgenabschätzung;

ii. methodische Mängel im Muster;

iii. Mangel an sektorspezifischen Informationen: branchenspezifische Risiken und entsprechende Kontrollen zur Minderung dieser Risiken sollten festgestellt und einander gegenübergestellt werden.

Die Datenschutzgruppe zog die Schlussfolgerung, dass das Muster noch nicht genug ausgereift und entwickelt ist und forderte die Kommission auf, dafür zu sorgen, dass die Arbeiten am Muster weitergeführt werden, um schließlich eine ausreichend konkrete, nützliche und eindeutig praxisbezogene Hilfestellung für die für die Datenverarbeitung Verantwortlichen sicherzustellen.

Die Datenschutzgruppe hat die Kommission außerdem dazu aufgefordert, die Aufnahme der besten verfügbaren Techniken (wie in Punkt 3 f der Empfehlung definiert) in das Muster in Betracht zu ziehen und der Datenschutzgruppe das integrierte Dokument zur Stellungnahme vorzulegen. Darüber hinaus empfahl die Datenschutzgruppe der Kommission, eine Bestandsaufnahme der bisherigen und laufenden Arbeiten auf dem Gebiet der Datenschutzfolgenabschätzungen durchzuführen und zu prüfen, ob es sinnvoll wäre, eine allgemeingültige Methode für Datenschutzfolgenabschätzungen festzulegen, die für branchenspezifische Aktivitäten von Nutzen wäre.

Zweite Fassung des Musters

Die Kommission antwortete am 27. Mai 2013 auf die Stellungnahme der Datenschutzgruppe. Der Brief enthielt die Aufforderung der Kommission an die Sachverständigengruppe 2, das Muster zu überarbeiten und bestätigte, dass die Datenschutzgruppe die Arbeiten der Sachverständigengruppe 2 im Rahmen ihrer speziellen Rolle teilweise unterstützen könne. Darüber hinaus zog es die Kommission vor, die besten verfügbaren Techniken nicht in das Muster zu integrieren. Als Gründe nannte sie den begrenzten Anwendungsbereich der besten verfügbaren Techniken auf die gemeinsamen Mindestfunktionsanforderungen an intelligente Messsysteme und ihre evolutive Natur[5]. Auf den Vorschlag, eine allgemeingültige Methode für

[5] „*I consider this that would not be as beneficial as you intend for the following reasons: (i) In line with the Commission Recommendation 2012/148/EU, the BATs focus only on the common minimum functional requirements for smart metering, whereas the DPIA template's scope of application strives to go beyond the last mile and include the whole smart grid spectrum; and (ii)Should the BATs be enshrine in the DPIA template, their evolutive and illustrative nature would ipso facto condemnthe template to be ephemeral and possibly subject to impractically frequent revisions*."
[*„Ich ziehe es in Betracht und es wäre aus den folgenden Gründen nicht so vorteilhaft, wie Sie wünschen: (i) Entsprechend der Empfehlung der Kommission 2012/148/EU konzentrieren sich die besten verfügbaren Techniken lediglich auf die gemeinsamen Mindestfunktionsanforderungen an intelligente Messsysteme, während der Anwendungsbereich das Muster für die Datenschutzfolgenabschätzung auch den letzten Schritt geht und das gesamte Spektrum intelligenter Netze umfasst; (ii) Sollten die besten verfügbaren Techniken in das Muster für die Datenschutzfolgenabschätzung festgeschrieben werden, würde ihre evolutive und illustrative Natur das*

Datenschutzfolgenabschätzungen festzulegen, die für branchenspezifische Aktivitäten von Nutzen wäre, wurde in dem Brief eine andere Dienststelle der Kommission hinzugezogen, von der bislang keine Antwort einging.

Die Sachverständigengruppe 2 bildete ein Redaktionsteam für den zweiten Entwurf des Musters, das am 4. Juni und am 3. Juli 2013 zusammenkam. Am ersten Treffen nahmen einige Vertreter der Datenschutzgruppe als Beobachter teil und beantworteten die Fragen der Vertreter der Sachverständigengruppe 2 zu verschiedenen, im Muster aufgeworfenen Fragestellungen.

Am 20. August 2013 legte die Kommission der Datenschutzgruppe die endgültige Fassung des von den beteiligten Akteuren der Sachverständigengruppe 2 überarbeiteten Musters vor.

Aufbau der vorliegenden Stellungnahme

In Abschnitt 1 werden die Ereignisse dargelegt, die zu dem überarbeiteten Muster geführt haben. Dieser Abschnitt bezieht sich auf Abschnitte der Stellungnahme 4/2013 und auf die Frage des Datenschutzes in intelligenten Netzen und die diesbezüglichen Ziele der Datenschutzfolgenabschätzung.

Abschnitt 2 enthält die Bewertung des überarbeiteten Musters durch die Datenschutzgruppe.

In Abschnitt 3 werden die Schlussfolgerungen dargelegt.

1.2 Datenschutz in intelligenten Netzen und die mit dem Muster verfolgten diesbezüglichen Ziele

Abschnitte 1.2 und 1.3 der Stellungnahme 4/2013 haben die Fragen des Datenschutzes in intelligenten Netzen und die mit dem Muster verfolgten diesbezüglichen Ziele bereits angesprochen. Die Datenschutzgruppe hat diesen Fragestellungen nichts Neues hinzuzufügen.

2 Analyse des Musters

Die Datenschutzgruppe begrüßt die Arbeiten, die die Mitglieder der Sachverständigengruppe 2 durchgeführt haben, um auf die Kommentare der Datenschutzgruppe einzugehen und die Bereitschaft der Sachverständigengruppe, den Rat der Datenschutzgruppe als wertvolle Unterstützung zu berücksichtigen.

Diese Analyse folgt hauptsächlich den Kommentaren, die in der Stellungnahme 4/2013 gemacht wurden. Sie umfasst auch Verbesserungen und Optimierungen, die für die endgültige Festlegung des Musters berücksichtigt werden sollten. Die nachfolgenden Abschnitte berücksichtigen beide Aspekte.

Muster ipso facto dazu verurteilen, vergänglich zu sein und möglicherweise unpraktisch häufiger Überprüfungen zu bedürfen."] (Schreiben ener.b.3 VL/cv(2013)1506536 vom 27. Mai 2013 an Herrn Kohnstamm).

Für ein umfassendes und klares Verständnis muss die Analyse vor dem Hintergrund des Inhalts und der Terminologie der Stellungnahme 4/2013 gelesen werden.

2.1 Das Muster und die Empfehlung der Kommission 2012/148

Die Datenschutzgruppe hat die Gelegenheit ergriffen, diese zweite Ausgabe des Musters für die Datenschutzfolgenabschätzung in intelligenten Netzen vor dem Hintergrund der Empfehlung der Kommission genau zu prüfen, die hierfür Zweck, Umfang und Anwendbarkeit vorgibt.

2.1.1 Zur Ermessensfrage bezüglich der Durchführung einer Datenschutzfolgenabschätzung in intelligenten Netzen

Das Vorliegen einer Empfehlung der Kommission stellt zwar keine rechtlich verbindliche Verpflichtung dar, zeigt aber andererseits, dass bestimmte Maßnahmen sehr empfohlen werden. Empfehlung 2012/148/EU legt fest, dass die Vorgänge der Verarbeitung personenbezogener Daten in intelligenten Messgeräten/Netzen *„aufgrund ihres Charakters, ihrer Tragweite oder ihrer Zweckbestimmungen für die Rechte und Freiheiten der betroffenen Personen (…) ein systematisches Verfahren zur Bewertung der potenziellen Auswirkungen von Risiken"* benötigen. Die Datenschutzgruppe möchte erneut die Notwendigkeit eines solchen Prozesses bestätigen, die bereits in der Stellungnahme 12/2011 der Datenschutzgruppe zur intelligenten Verbrauchsmessung („Smart Metering“) im Zusammenhang mit dem Ansatz des „eingebauten Datenschutzes“ (privacy by design) festgestellt wurde. Eine solche Notwendigkeit wird weitgehend gerechtfertigt durch die Komplexität der technischen Infrastruktur und der Verwaltungsinfrastruktur von intelligenten Netzen, durch die potenziellen Anwendungs- und Entwicklungsmöglichkeiten und durch die speziellen Risiken für die Grundrechte und Grundfreiheiten des Einzelnen, zu denen unter anderem die Risiken für das Leben zählen (beispielsweise, das Abschalten der Stromversorgung, wenn durch Strom betriebene Maschinen lebenswichtige Funktionen unterstützen).

Darüber hinaus hat die Datenschutzgruppe die Tatsache begrüßt, dass die Kommission eine Datenschutz-Grundverordnung vorgeschlagen hat, die Datenschutzfolgenabschätzungen unter bestimmten Bedingungen verbindlich vorschreiben würde. Es sollte den beteiligten Akteuren des Musters für die Datenschutzfolgenabschätzung in intelligenten Netzen - d. h. den für die Verarbeitung Verantwortlichen und den Auftragsverarbeitern - bewusst sein, dass die Nutzung des Musters als Mittel gesehen werden sollte, in Zukunft eine rechtliche Verpflichtung einzuhalten. Angesichts der immensen Investitionen und des langen Planungshorizonts für Netzwerke sollte es als im ureigensten Interesse der beteiligten Akteure angesehen werden, bereits Erfahrungen mit dem Ansatz der Datenschutzfolgenabschätzung zu sammeln und ihn von Anfang an bei der Entwicklung ihrer Systeme anzuwenden, so dass sie keine Probleme mit der Einhaltung bekommen, wenn die anhängigen Rechtsvorschriften in Kraft treten. Wo der Sprachgebrauch im vorliegenden Muster den Unternehmen einen weiten Ermessensspielraum bei der Auslegung lässt, wie insbesondere in Abschnitt 2.1, sollte die Kommission klarstellen, dass dieser Ermessensspielraum strikt ausgelegt wird, um sicherzustellen, dass die tatsächliche Datenschutzfolgenabschätzung auf die umfassendste Weise durchgeführt wird. Hierzu könnte dieser Ansatz beispielsweise in einer Empfehlung der Kommission erklärt werden, die das Muster begleiten und

unterstützen könnte. Basierend auf den verarbeiteten Informationen, dem Umfang des analysierten (Teil)netzes, dem Status des Projekts usw. bewertet die Datenschutzgruppe die Rolle der Vorabbewertung als zweckmäßig, um alle möglichen Situationen zu berücksichtigen, in denen sich zukünftige Verantwortliche und Auftragsverarbeiter befinden könnten. Sie wird nicht als Schritt in der Methodik angesehen, der die Ziele der Empfehlung der Kommission schwächt.

2.1.2 Die Datenschutzfolgenabschätzung und die Datenschutzbehörden

Punkt 8 der Empfehlung der Kommission legt fest, dass die Mitgliedstaaten sicherstellen sollten, dass die Stelle, die personenbezogene Daten verarbeitet, vor der Verarbeitung die Datenschutzbehörde zu der Datenschutzfolgenabschätzung konsultiert. Die Datenschutzgruppe stellt fest, dass das Muster diesen Ansatz in vielen Bereichen noch nicht vollständig widerspiegelt. Einige Zitate: „im Zweifelsfall" (Abschnitt 2.1.4) oder konsultieren Sie einfach den Datenschutzbeauftragten (und nicht die Datenschutzbehörde) „sofern verfügbar" (Abschnitt 2.6.2) oder der Datenschutzbehörde „auf Aufforderung" vorzulegen, sobald der endgültige Bericht angenommen ist (Abschnitt 2.7). Während es vorzuziehen wäre, dass das Muster durchwegs verdeutlicht, dass gemäß der Empfehlung der Kommission die nationalen Datenschutzbehörden vor der Verarbeitung konsultiert werden sollten, sofern das nationale Datenschutzrecht und/oder die Politik der nationalen Datenschutzbehörden keine ausdrücklichen Ausnahmen bereitstellen, sollte die Kommission auf geeignete Weise sicherstellen, dass die beteiligten Akteure wissen, dass das gemäß der Empfehlung angenommene Muster die durch die Empfehlung selbst angenommenen Grundsätze nicht ändern kann. Die Textstellen, auf die hingewiesen wurde, können nur als Empfehlung für zusätzliche Möglichkeiten zur Einholung von Rat verstanden werden, die eine Ergänzung zu der von der Kommission empfohlenen Konsultation der Datenschutzbehörden sind.

2.2 Klarheit in Bezug auf die Natur und die Ziele der Datenschutzfolgenabschätzung

2.2.1 Berücksichtigung der abschließenden Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen

Die Datenschutzgruppe begrüßt, dass der im Muster (Abschnitt 2.5) dargelegte Schritt der Risikobewertung in der Methode darauf abzielt, die tatsächlichen Auswirkungen auf die Grundrechte und Grundfreiheiten sowie auf die Bürgerrechte der betroffenen Personen (wie beispielsweise finanzielle Verluste, Preisdiskriminierung oder Straftaten, die durch eine zu Unrecht erfolgte Profilerstellung begünstigt werden) als Folgen der „befürchteten Ereignisse" aufgrund einer unrechtmäßigen und nicht nach Treu und Glauben erfolgten Verarbeitung personenbezogener Daten zu bewerteten und nicht länger die Auswirkungen auf die Ziele in Bezug auf die Privatsphäre als solche.

Dennoch scheint noch einige Verwirrung in dem Text zu bestehen, der die Methode der Risikobewertung betrifft (siehe den entsprechenden Abschnitt in dieser Stellungnahme) und insbesondere in Abschnitt 2.5.1.1 des Musters, in dem beschreiben wird, wie die Auswirkungen von befürchteten Ereignissen zu bewerten sind. Insbesondere der Satz, mit dem die Elemente herausgestellt werden sollen, um „*die Auswirkungen und den Schweregrad einer bestimmten identifizierten*

Bedrohung“ zu bewerten, bringt keine Klarheit. Er erwähnt die Ziele in Bezug auf die Privatsphäre als Elemente dieser Bewertung (siehe Abschnitt 2.2.2 der vorliegenden Stellungnahme) und greift, ohne näher darauf einzugehen und zu erklären, wie sie passen und ohne ersichtlichen Grund „*mit Kriminalität verbundene Risiken*“ heraus und greift einzelne Elemente wie „*Freizügigkeit, Verlust der Unabhängigkeit, Verlust der Gleichheit*“ heraus und bezeichnet sie als „*andere Grundsätze des Schutzes der Privatsphäre“*[6].

Die Datenschutzgruppe möchte betonen, dass die Datenschutzfolgenabschätzung immer und konsequent die Auswirkungen auf die „*Rechte und Freiheiten der betroffenen Personen*“ bewertet, worauf in Abschnitt 2.1 der Stellungnahme 4/2013 hingewiesen wird und wie es korrekt an verschiedenen Stellen des Musters festgestellt wird. Wenn das Muster eine andere Terminologie verwendet und beispielsweise nur auf das Recht auf Privatsphäre verweist, muss dies als Verweis auf das umfassendere Konzept interpretiert werden. Dies sollte in zukünftigen Überprüfungen des Musters angesprochen werden.

Wenn es stimmt, dass dasselbe befürchtete Ereignis zu vielen Auswirkungen auf betroffene Personen führen kann, könnte es darüber hinaus sinnvoll sein, die wichtigsten Auswirkungen auf die betroffenen Personen in Bezug auf die in Abschnitt 3.4.1 genannten befürchteten Ereignisse aufzulisten, um das Bewusstsein zu schärfen und die Auswirkungen einzuordnen. Diese Verbindung zwischen dem befürchteten Ereignis und den Auswirkungen auf die Grundrechte und Grundfreiheiten der betroffenen Personen charakterisiert die Anstrengungen im Zusammenhang mit dem Schutz der betroffenen Personen in Bezug auf die Verarbeitung personenbezogener Daten im Gegensatz beispielsweise zu einer reinen Bewertung der Risiken in Bezug auf die Informationssicherheit.

2.2.2 Der Umgang mit Zielen in Bezug auf die Privatsphäre

Die Art des Umgangs mit den Zielen in Bezug auf die Privatsphäre ist eine der wichtigsten Fragen einer Datenschutzfolgenabschätzung. Tatsächlich soll mit einer Datenschutzfolgenabschätzung sichergestellt werden, dass die Ziele in Bezug auf die Privatsphäre richtig berücksichtigt wurden.

Derzeit werden Ziele in Bezug auf die Privatsphäre:

- in „2.5.1.1 Auswirkungen befürchteter Ereignisse“ als Elemente genannt, die bei der Bewertung der Auswirkungen und des Schweregrads einer bestimmten identifizierten Bedrohung zu berücksichtigen sind;
- in „2.6.3 Restrisiken und Inkaufnahme von Risiken" als zu erreichende Ziele genannt;

[6] Ein Vorschlag könnte sein, den letzten Satz des ersten Absatzes von „2.5.1.1 Auswirkungen befürchteter Ereignisse“ um andere Elemente zu erweitern und ihn folgendermaßen zu formulieren: „Diese potenzielle Auswirkung wird definiert durch die Folgen, die jedes befürchtete Ereignis auf die Privatsphäre und auf andere Grundrechte und Grundfreiheiten der betroffenen Personen haben könnte. Dazu zählen beispielsweise Risiken in Verbindung mit Kriminalität wie Identitätsdiebstahl und Betrug oder Freizügigkeit, Unabhängigkeit, Gleichbehandlung, soziale Beziehungen, finanzielle Interessen usw. beispielsweise aufgrund einer Profilerstellung, aufgrund unerbetener Werbung, Diskriminierung oder individueller Entscheidungen über Fehlinformationen...“.

- in „Anhang 1 Privatsphäre und Datenschutzziele“ aufgeführt und beschrieben.

Die Richtlinie 95/46/EC[7] legt in den meisten ihrer Bestimmungen spezifische Bedingungen für die Verarbeitung personenbezogener Daten sowie ein Paket an Verpflichtungen fest, die die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter zu erfüllen haben. Die Richtlinie sieht keinen Ermessensspielraum oder ein annehmbares Maß der Nichteinhaltung dieser Bestimmungen vor. Während die Gewährleistung der Sicherheit der Verarbeitung eine dieser Verpflichtungen ist, sieht die Richtlinie in Artikel 17 für ihre Umsetzung einen Risikomanagementansatz vor, indem sie Folgendes feststellt: „Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.“ Im Zusammenhang mit einem Muster zur Bewertung der Auswirkungen muss berücksichtigt werden, dass Risikomanagementstrategien, wie diejenigen, die im Bereich der Sicherheit entwickelt wurden, zwar auf den Datenschutz angewendet werden können, aber nur in Bezug auf Sicherheitsfragen und dass für die Mehrheit der Verpflichtungen die vollumfängliche Einhaltung erforderlich ist. Das Muster verwendet den Begriff „Ziele in Bezug auf die Privatsphäre“, um die Verpflichtung zur Einhaltung zu bezeichnen und klärt in Abschnitt 2.6.3, dass die Konzepte der Restrisiken und der Inkaufnahme von Risiken nicht auf diese Ziele in Bezug auf die Privatsphäre Anwendung finden, die „erreicht werden müssen“ (S. 33).

Die Datenschutzgruppe begrüßt, dass diese Unterscheidung zwischen Risikomanagement und Einhaltung in dem Muster erkannt wird, hätte jedoch eine deutlichere und sichtbarere Darstellung befürwortet.

Dementsprechend sollten stets zwei abgegrenzte und ergänzende Maßnahmen vorliegen, um die Ergebnisse einer Datenschutzfolgenabschätzung zu behandeln. Die erste Maßnahme bezieht sich auf Risiken für personenbezogene Daten. Sie sollten einem Risiskomanagement unterliegen (bewertet, behandelt usw.). Die zweite Maßnahme bezieht sich auf die Einhaltung von Zielen in Bezug auf die Privatsphäre als rechtliche Verpflichtung. Dies sollte als Fragestellung der Einhaltung betrachtet werden (Maßnahmen, die durchgeführt oder geplant werden, um die Ziele in Bezug auf die Privatsphäre einzuhalten, Rechtfertigung, wenn dies nicht getan wird, rechtliche Risiken, wenn es nicht getan wird, geplante Kontrollen zur Überprüfung ob und wie dies getan oder nicht getan wird...).

In Bezug auf die Risikoanalyse sollte betont werden, dass die befürchteten Ereignisse, die in „2.4.1 Einführung“ beschrieben sind, systematisch bewertet werden sollten. Ihre potenziellen Auswirkungen auf die betroffenen Personen sollten identifziert und die Abschätzung der nachteiligen Auswirkungen sollte auf diese potenziellen Auswirkungen gestützt werden. Dennoch möchte die Kommission möglicherweise überprüfen, was das letzte befürchtete Ereignis (Umleitung personenbezogener Daten ... zu Personen, die diese nicht benötigen) vom dritten (unrechtmäßiger Zugang zu personenbezogenen Daten ... durch unbefugte Personen) unterscheidet.

[7] 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.

Die Datenschutzgruppe möchte einige Hilfsmittel zur Ergänzung der in dem Muster vorgeschlagenen Methode vorschlagen, um ihre Anwendbarkeit zu vereinfachen. Sie ruft die Kommission dazu auf, diese Vorschläge den potenziellen Nutzern des Musters bekannt zu machen, beispielsweise indem die vorliegende Stellungnahme zusammen mit dem Muster verfügbar gemacht wird oder indem in einem dazugehörigen Instrument auf sie verwiesen wird. Die ergänzenden Hilfsmittel werden im Anhang der vorliegenden Stellungnahme beschrieben.

2.3 Die in dem Muster für die Datenschutzfolgenabschätzung verwendete Methode

Die in dem Muster dargelegte Methode wurde insgesamt verdeutlicht und ist besser zu handhaben. Dennoch bleiben viele unklare und verwirrende Elemente bestehen, einschließlich der Liste der allgemeinen Bedrohungen, die in Abschnitt 3.4.1, in den Formularen des Musters und dem vorgelegten Fragebogen genannt werden.

Einige dieser Elemente wurden in Abschnitt 2.1 behandelt, als die Frage zur Klarheit der Natur und zu den Zielen der Datenschutzfolgenabschätzung geklärt wurde. Die anderen werden hier behandelt werden.

2.3.1 Die Methode der Risikobewertung (Managment)

Die meisten Elemente der Methode des Risikomanagements basieren den Angaben zufolge größtenteils auf ISO 31 000, auf der Methode von EBIOS sowie auf der Synthese, die von der CNIL bereitgestellt wurde[8].

Identifizierung der Anlagen (Assets)

Es liegt eine Definition der primären und unterstützenden Anlagen als Ziele der allgemeinen Risikobewertung vor.

Identifizierung und Bewertung der Bedrohungen und Anfälligkeiten

Nun ist der Unterschied zwischen Bedrohungen und Risiken definiert. Zum Konzept der Anfälligkeit gibt es eine größere Orientierungshilfe.

Dennoch ist die Datenschutzgruppe besorgt, dass die Darstellung verfehlter Ziele in Bezug auf die Privatsphäre als allgemeine Bedrohungen in Abschnitt 3.4.1 insbesondere in Abschnitt 3.4.1.4 zu dem Missverständnis führen könnte, dass das Muster „ein verfehltes Ziel in Bezug auf die Privatsphäre als Bedrohung definiert“, damit die Bewertung der Ziele in Bezug auf die Privatsphäre in den Kontext der Risikobewertungsmethode passt. Diese Fragestellung wurde bereits in Abschnitt 2.2.2 der vorliegenden Stellungnahme diskutiert.

Die Datenschutzgruppe erkennt jedoch an, dass einschlägige Beispiele und die Orientierungshilfe (für die Datensätze in den Tabellen in Abschnitt 3.4.1, die vefehlte Ziele in Bezug auf die Privatsphäre beschreiben), in den anderen Zeilen nach einer Verbesserung nach wie vor hilfreich sind, um genau die Ziele in Bezug auf die Privatsphäre zu erreichen. Die Datenschutzgruppe schlägt vor, dass diese Informationen in einem weiter gefassten und grobkörnigeren Ansatz an die Ziele in

[8] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf.

Bezug auf die Privatsphäre genutzt werden (siehe auch die Überlegungen am Ende des Abschnittes 2.2.2 dieser Stellungnahme), um eine Orientierungshilfe zu geben, wie diese erfüllt werden können. Dies könnte entweder in Tabellenform dargestellt werden oder vielleicht besser in einem eigenen Abschnitt, in dem auch eine Orientierungshilfe im Zusammenhang mit riskanten Verarbeitungen gegeben werden kann (wie die Profilerstellung oder Entscheidungen, die basierend auf automatisierten Verarbeitungen über Personen getroffen werden).

Risikoberechnung / Risikopriorisierung

Es gibt deutlichere Hilfestellungen zur Berechnung und Priorisierung von Risiken. Im Abschnitt zur Risikoberrechnung (2.5.1.3) werden eine bessere Formulierung und mehr Klarheit benötigt.

Risikobehandlung

„2.6.1. Risikoänderung: durchgeführte und geplante Kontrollen“ sollte in „2.5. Schritt 5 - Bewertung des Datenschutzrisikos“ integriert und bei der ersten Risikoabschätzung berücksichtigt werden. Der Titel sollte jedoch nicht „Risikoänderung“ beinhalten, da dies eine der Risikobehandlungsoptionen ist. Der Titel könnte einfach „Durchgeführte und geplante Kontrollen“ lauten. In „2.6. Schritt 6 - Identifizierung und Empfehlung von Kontrollen und Restrisiken“ und insbesondere in „2.6.2. Risikobehandlung“ werden dann zusätzliche Kontrollen bestimmt und Risiken wieder als Restrisiken eingeschätzt.

Die Datenschutzgruppe hat in der Stellungnahme 4/2013 angemerkt, dass es in der ersten Fassung des Musters keine Gegenüberstellung zwischen den zu mindernden Risiken und der Liste der möglichen Kontrollen in Anhang II gab. Die Datenschutzgruppe begrüßt, dass die Beschreibung des Ziels der möglichen Kontrollen in der neuen Fassung des Musters häufig die Art der Risiken umfasst, die es allgemein mindern soll. Darüber hinaus verknüpft die nicht erschöpfende Liste allgemeiner Bedrohungen in Abschnitt 3.4.1. diese Bedrohungen mit den möglichen Kontrollen in Anhang II.

Restrisiken

Für ein ausgewogenes Abwägen der Restrisiken am Ende des Risikomanagementprozesses ist es gleichermaßen wichtig, bereits zu einem frühen Zeitpunkt alle betroffenen Interessen zu identifizieren. Diese können dem Gesamt-Risikomanagementprozess des Unternehmens entnommen werden, sofern ein solcher besteht. Es können nicht nur wirtschaftliche oder andere rechtmäßige Interessen angegeben werden, sondern auch andere Herausforderungen wie beispielsweise die soziale Verantwortung oder die Einhaltung sonstiger rechtlicher Anforderungen.

Die Datenschutzgruppe schlägt vor, dass ein neuer Abschnitt eingefügt wird, um die Herausforderungen der Verarbeitung zu identifizieren. Dieser Abschnitt könnte sich zwischen 2.3.1 und 2.3.2 befinden und „2.3.2. Herausforderungen der Verarbeitung“ betitelt werden. Hier sollte nach einer Beschreibung der Möglichkeiten für eine Verarbeitung in intelligenten Netzen gefragt werden (Marketing / wirtschaftliche, gesellschaftliche, rechtliche Einhaltung usw.).

Nach dem ersten Absatz von „2.6.4. Beschluss“ könnte eine Bewertung der Restrisiken angesichts der Herausforderung hinzugefügt werden. In diesem Absatz könnte erklärt werden, dass der Beschluss darin besteht, die Restrisiken angesichts der in 2.3 identifizierten Herausforderungen entweder anzunehmen oder nicht anzunehmen.

2.3.2 Aufgaben und Zuständigkeiten

Die Datenschutzgruppe begrüßt die Einbindung (Abschnitt 1.4.2) einer Liste der verschiedenen Arten von Betreibern intelligenter Netze, einschließlich einer allgemeinen Beschreibung der Zwecke, für die sie personenbezogene Daten verarbeiten könnten.

Durch das Vorliegen des spezifischen Unterabschnitts 2.1.2 wird nun die Notwendigkeit einer eindeutigen Zuweisung der Zuständigkeiten der für die Datenverarbeitung Verantwortlichen und der Auftragsverarbeiter unterstrichen. Das im Text genannte Beispiel für die Verantwortung für die Verarbeitung und die möglichen Zuständigkeiten des Auftragsverarbeiters in intelligenten Messsystemen sollte durch weitere Beispiele ergänzt werden, die komplexere Situationen darstellen. Im Text gibt es ein weiteres Beispiel (Mikronetzbetreiber und betroffene Versicherungsgesellschaft), in dem das Vorliegen eines Problems festgestellt, aber keine Orientierungshilfe gegeben wird.

Wie bereits in Stellungnahme 4/2013 vorgeschlagen wurde, „könnte im Muster im dritten Schritt ein vierter Abschnitt angefügt werden, mit dem die Zuständigkeiten der an der Datenverarbeitung beteiligten Akteure aufgezeigt werden sollen“ (dort liegt in Abschnitt 3 bereits ein entsprechendes Formular vor).

2.3.3 Die Formulare des Musters

Neben anderen Überlegungen in anderen Abschnitten dieser Stellungnahme, möchte die Datenschutzgruppe auf einige andere Mängel hinweisen, die die Abschnitte betreffen, in denen die zur Durchführung der Datenschutzfolgenabschätzung zu verwendenden Formulare beschrieben sind.

In Abschnitt 3.3 ist beispielsweise die Beziehung zwischen verschiedenen Mustern nicht klar, die für die Identifizierung intelligenter Messsysteme, ihre Charakterisierung und Beschreibung verwendet werden oder die Reihenfolge und die genaue Weise, in der sie genutzt werden sollten. Es liegt ein Verweis auf ein externes Dokument vor, ohne dass gesagt wird, worauf verwiesen wird. Und in der Methode scheint kein Hinweis darüber vorzuliegen, wann das Formular in Abschnitt 3.3.5 verwendet werden muss.

Auf der anderen Seite ist eine Tabelle mit den pirmären und entsprechenden unterstützenden Anlagen als Anleitung der Risikobewertung wichtig.

Allgemein sollte mehr Orientierungshilfe in Bezug auf die Verwendung der Formulare gegeben werden. Es wäre sehr hilfreich, wenn in einem Anhang mindestens ein Beispiel gegeben würde.

2.4 Sektorspezfischer Inhalt des Musters

Eines der wichtigsten Themen in der Stellungnahme 4/2013 war, dass die in der ersten Fassung des Musters ausgearbeiteten Risiken und Kontrollen die Erfahrungen der Branche mit den zentralen Fragestellungen und bewährten Vorgehensweisen nicht zum Ausdruck brachten.

Die Datengruppe stellt fest und begrüßt, dass einige spezifische Inhalte in die nicht erschöpfende Liste allgemeiner Bedrohungen aus Abschnitt 3.4.1.1 eingefügt wurden, insbesondere unter der Spalte, die mit „Spezifische, die Energieindustrie betreffende Beispiele zur Unterstützung von Anfälligkeiten der Anlagen“ überschrieben ist. Die Datenschutzgruppe ist jedoch nach wie vor der Ansicht, dass einige Verbesserungen und mehr Orientierungshilfen sowohl im Text als auch im Muster benötigt werden, insbesondere um die Ziele in Bezug auf die Privatsphäre zu erfüllen (Siehe auch Abschnitt 2.2.2).

Wie bereits in Abschnitt 1.1 erwähnt wurde, hat die Kommission den Vorschlag der Datenschutzgruppe zurückgewiesen, die besten verfügbaren Techniken, an denen die Sachverständigengruppe 2 gearbeitet hat, in das Muster zu integrieren. Den Angaben zufolge wurde der Vorschlag zurückgewiesen, da die Anwendung der besten verfügbaren Techniken auf intelligente Messgeräte beschränkt und ihre Natur evolutiv ist.

Die Datenschutzgruppe bestätigt ihre Ansicht, dass untrennbar mit dem Muster verbundene, beste verfügbare Techniken einer Organisation, die eine Datenschutzfolgenabschätzung durchführen will, die Möglichkeit eröffnen würden, bei Bedarf geeignete Maßnahmen auszuwählen. Die evolutive Natur der besten verfügbaren Techniken steht ihrer Funktion als Ergänzung zum Muster nicht im Wege. Darüber hinaus wird das Muster selbst nach der ersten Anwendungsphase sowie in regelmäßigen Abständen eine Überprüfung benötigen, damit die Methode gepflegt und verfeinert werden kann. Die Tatsache, dass der Anwendungsbereich der besten verfügbaren Techniken auf intelligente Messsysteme beschränkt und folglich nicht erschöpfend ist, ist auch kein Grund, ihre Anwendung aus der Datenschutzfolgenabschätzung auszuschließen. Intelligente Messsysteme stellen die Subsysteme dar, in denen personenbezogene Daten in erster Linie erhoben und verarbeitet werden und es ist in jedem Fall besser, eine gewisse Orientierungshilfe zu haben, als keine. Die Datenschutzgruppe nutzt die Gelegenheit außerdem, um vorzuschlagen, dass die Kommission und die Industrie die Möglichkeit prüfen, die wertvolle Arbeit der besten verfügbaren Techniken auch auf den breiteren Anwendungsbereich der intelligenten Netze auszudehnen.

In der Stellungnahme 4/2013 und insbesondere in Anhang II hat die Datenschutzgruppe empfohlen, 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 Begleitdokument zu den besten verfügbaren Techniken detailliert erläutert werden. Dies ist nicht geschehen. Die Datenschutzgruppe vertritt nach wie vor die Ansicht, dass es sehr hilfreich für die Industrie wäre, sowohl einen Bestand an Maßnahmen zu haben, die für die Durchführung bereit stehen als auch besser über Technologien zum Schutz der Privatsphäre informiert zu sein, um weitere angemessene Kontrollen entwickeln zu können.

2.5 Notwendigkeit der Prüfung/Validierung des Musters

Die Datenschutzgruppe schlägt vor, dass auf der Grundlage der bestehenden Fassung eine bestimmte, angemessene Prüfung/Validierung des Musters durchgeführt wird, bei der die vorstehenden Kommentare so weit wie möglich berücksichtigt werden. Die Datenschutzgruppe schlägt vor, dass das Muster und die Methode nach dieser Prüfung überprüft werden und angesichts der Erfahrungen und unter Berücksichtigung der vorgenannten Kommentare verbessert werden. Diese Prüffälle, über die die Datenschutzgruppe informiert werden sollte und in Bezug auf die einzelne Datenschutzbehörden ihre Unterstützung in Betracht ziehen könnten, können auch der Bereitstellung wertvoller Beispiele dienen, die den Anhängen des Musters für ein besseres Verständnis der vorgeschlagenen Methode beigefügt werden.

2.6 Andere Erwägungen

2.6.1 Das Konzept der personenbezogenen Daten

Abschnitt 2.1 beschreibt, wie festgestellt wird, ob personenbezogene Daten im geprüften intelligenten Teilnetz verarbeitet werden. Die Datenschutzgruppe stellt fest, dass die Einstufung als personenbezogene Daten in den aufgeführten Beispielen richtig zu sein scheint, auch wenn die Begründung für die Identifizierung einer Information als personenbezogene Daten nicht immer strikt der Rechtsterminologie folgt.

Die Daten, die als „Nutzungsdaten“ bezeichnet werden, werden beispielsweise als personenbezogene Daten angesehen, weil „sie einen Einblick in das tägliche Leben des Einzelnen geben“. Dabei handelt es sich bei ihnen um personenbezogene Daten, da sie sich auf den Vertragsinhaber und möglicherweise auf seine Familie beziehen. Die Tatsache, dass sie Einblick in das tägliche Leben geben, ist eine Auswirkung auf die Privatsphäre. Diese Erwägung gilt auch für die anderen hier aufgeführten Punkte. Während die Beispielliste für potenzielle Nutzer des Musters gewiss hilfreich ist, entsteht der Eindruck, dass eine solche beträchtliche Auswirkung auf die Privatsphäre erforderlich ist, damit Daten als personenbezogene Daten angesehen werden. Darüber hinaus sollte klar sein, dass die Beispielliste nicht erschöpfend ist.

2.6.2 Weitere Anmerkungen zur Datenschutzterminologie

In einigen Abschnitten verwendet das Muster Terminologie wie „Eigentümer des Systems“, die im Anwendungsbereich Bedeutung hat, die Beziehung zur möglicherweise anzuwendenden Datenschutzerminologie (wie für die Datenverarbeitung Verantwortlicher,…) (S. 14, 18, 32,...) aber nicht immer klärt. Weitere Beispiele sind „der Einzelne“, „der Verbraucher“, „der Kunde“ ohne klare Verknüpfung zu der betroffenen Person (Seiten 10, 15,...).

Darüber hinaus könnten einige der verwendeten Begriffe wie „mit dem Kunden vereinbart“ (S. 10), „Kunden müssen die Wahl haben“ (S. 11) angepasst werden an die Notwendigkeit, die „Einwilligung“ gemäß der Definition in Artikel 2 Buchstabe h der Richtlinie einzuholen.

Die Datenschutzgruppe ist der Ansicht, dass in Betracht gezogen werden sollte, die entsprechende Datenschutzterminologie anzugeben und gegebenenfalls den Grad an Interoperabilität der Begriffe zu erläutern.

2.7 Schlussfolgerungen und Empfehlungen

Die Datenschutzgruppe begrüßt die von der Sachverständigengruppe 2 durchgeführte Arbeit und erkennt, dass die zweite Fassung des Musters eine beträchtliche Verbesserung gegenüber der vorangegangenen Fassung darstellt, da die Methode besser dargelegt wird und besser zu handhaben ist. Dennoch gibt es immer noch eine Reihe missverständlicher Elemente und an manchen Stellen ist mehr Klarheit erforderlich. Wird dem auf die beschriebene Weise nachgegangen, wird dies auf entscheidende Weise zum erfolgreichen Einsatz und zur erfolgreichen Nutzung des Musters beitragen.

Die Datenschutzgruppe versteht, dass die von ihr bewertete Fassung möglicherweise noch linguistisch und juristisch überarbeitet wird.

Der Datenschutzgruppe ist der dringende Bedarf an einer Datenschutzfolgenabschätzung im industriellen Sektor bewusst und sie begrüßt eine baldige endgültige Fassung des Musters, dessen Wirksamkeit nach einer bestimmten Zeit der Anwendung gewiss überprüft und verbessert werden muss. Sie empfiehlt deshalb die Organisation einer Testphase mit einigen wirklichen Fällen, über die die Datenschutzgruppe informiert werden sollte. In der Testphase werden es einzelne Datenschutzbehörden möglicherweise in Betracht ziehen, ihre Unterstützung anzubieten. Diese Testphase sollte auch dazu beitragen, dass das Muster den betroffenen Personen im Zusammenhang mit dem Einsatz intelligenter Netze einen verbesserten Datenschutz bietet. Bei der Prüfung des Musters und wie es im Muster vorgesehen ist, wird die Industrie dazu aufgefordert, das Augenmerk auf Schlüsselkonzepte der Datenschutzreform zu richten, wie konzeptionsbedingter und standardmäßiger Datenschutz, Datenminimierung, das Recht vergessen zu werden und Datenportabilität.

Darüber hinaus empfiehlt die Datenschutzgruppe weiterhin, zur prüfen, ob es sinnvoll wäre, eine allgemeingültige Methode für Datenschutzfolgenabschätzungen festzulegen, die für branchenspezifische Aktivitäten von Nutzen wäre.

Brüssel, den 4. Dezember 2013

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM

Anhang: Zusätzliche methodologische Hilfsmittel

In „3.5. Schritt 5 - Bewertung des Datenschutzrisikos“ könnte die nachfolgende Tabelle zur Bewertung der befürchteten Ereignisse verwendet werden:

Verarbeitung und personenbezogene Daten	Maß an Identifikation	Befürchtete Ereignisse	Potenzielle Auswirkungen	Nachteilige Auswirkungen	Schweregrad (Maß an Identifikation + nachteilige Auswirkungen)
[Liste der betroffenen personenbezogenen Daten]	[der geeignetste Grad in der Skala des Maßes an Identifikation, basierend auf personenbezogenen Daten]	[Befürchtetes Ereignis]	[Liste der potenziellen Folgen für betroffene Personen, wenn das befürchtete Ereignis eintritt]	[der geeignetste Grad in der Skala der nachteiligen Auswirkungen, basierend auf potenziellen Auswirkungen]	[Ergänzung]

Werden personenbezogene Daten nicht umfassend bewertet, müssen diese Zeilen wiederholt werden (z. B. für jede Verarbeitung).

Dieselbe Tabelle könnte auch um weitere Spalten ergänzt werden, die den Bedrohungen entsprechen, so dass die gesamten Risiken gezeigt werden können:

Verarbeitung und personenbezogene Daten	Maß an Identifikation	Befürchtete Ereignisse	Potenzielle Auswirkungen	Nachteilige Auswirkungen	Schweregrad (Maß an Identifikation + nachteilige Auswirkungen)	Wichtigste Bedrohungen	Anfälligkeiten	Risikoquellen	Fähigkeiten	Wahrscheinlichkeit (Anfälligkeiten + Fähigkeiten)

Es sollte ein neuer Abschnitt eingefügt werden, um die Einhaltung der Ziele in Bezug auf die Privatsphäre nachzuweisen. Dieser Abschnitt könnte sich zwischen 2.6.2 und 2.6.3 befinden und „2.6.3 Einhaltung der Ziele in Bezug auf die Privatsphäre“ genannt werden. Da diese Ziele in Bezug auf die Privatsphäre vorgeschrieben und nicht verhandelbar sind, sollte festgestellt werden, dass für jedes

Ziel in Bezug auf die Privatsphäre anzugeben ist, wie es umgesetzt wird oder zu begründen ist, warum es nicht umgestzt wurde[9].

Für diesen Zweck könnte die nachfolgende Tabelle verwendet werden:

Ziele in Bezug auf die Privatsphäre	Erklärungen	Beschreibung / Begründung
Wahrung der Qualität personenbezogener Daten	Datenvermeidung und Datenminimierung, Festlegung und Eingrenzung des Zwecks, Datenqualität und -transparenz sind die vorrangigen Ziele, die sicherzustellen sind.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Rechtmäßigkeit der Verarbeitung personenbezogener Daten	Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten muss sichergestellt werden, indem die Datenverarbeitung wahlweise auf ausdrücklicher Einwilligung, einem Vertrag, einer rechtlichen Verpflichtung usw. basiert.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Rechtmäßigkeit der Verarbeitung sensibler personenbezogener Daten	Die Rechtmäßigkeit der Verarbeitung sensibler personenbezogener Daten muss sichergestellt werden, indem die Datenverarbeitung wahlweise auf ausdrücklicher Einwilligung, einer speziellen Rechtsgrundlage usw. basiert.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Einhaltung des Rechts der betroffenen Person, unterrichtet zu werden	Es muss sichergestellt werden, dass die betroffene Person rechtzeitig über die Erhebung ihrer Daten unterrichtet wird.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Einhaltung des Rechts der betroffenen Person auf Auskunft, Berichtigung und Löschung der Daten	Es muss sichergestellt werden, dass dem Wunsch der betroffenen Person auf Auskunft, Berichtigung, Löschung oder Sperrung ihrer Daten zeitnah nachgekommen wird. Die Umsetzung des Rechts, vergessen zu werden und auf Datenportabilität sollte gefördert werden.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Einhaltung des Rechts der betroffenen Person, Widerspruch einzulegen	Es muss sichergestellt werden, dass die Daten der betroffenen Person nicht länger verarbeitet werden, wenn diese Widerspruch einlegt. Insbesondere im Fall der Profilerstellung muss die Transparenz der automatisierten Entscheidungen gegenüber dem Einzelnen sichergestellt werden.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Schutz der Vertraulichkeit und Sicherheit der Verarbeitung	Die Verhinderung des unberechtigten Zugriffs, die Aufzeichnung der Datenverarbeitung, Netzwerk- und Transportsicherheit und die Verhinderung des zufälligen Datenverlusts sind die vorrangigen Ziele, die sicherzustellen sind. Es sollten Verfahren für die Meldung von Sicherheitsverletzungen gefördert werden.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]

[9] Dies ist vergleichbar mit der „Anwendbarkeitserklärung“ aus ISO/IEC 27001.

Ziele in Bezug auf die Privatsphäre	Erklärungen	Beschreibung / Begründung
Einhaltung der Meldepflicht	Die Meldung der Datenverarbeitung, die vorherige Überprüfung der Einhaltung und die Dokumentation sind die vorrangigen Ziele, die sicherzustellen sind. Für dieses Ziel sollte die Datenschutzfolgenabschätzung als entscheidendes Mittel angesehen werden.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Einhaltung der Pflichten im Zusammenhang mit der Vorratsdatenspeicherung	Die Vorratsdatenspeicherung sollte auf den Mindestzeitraum begrenzt werden, der mit dem Zweck der Speicherung oder mit anderen rechtlichen Anforderungen vereinbar ist.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Konzeptionsbedingte Privatsphäre	Unter Berücksichtigung des Stands der Technik und der Kosten der Umsetzung, werden die technischen und organisatorischen Maßnahmen und die Verfahren sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst, so konzipiert, dass sie die Rechte der betroffenen Person auf Privatsphäre und Datenschutz vollumfänglich einhalten.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]
Standardmäßige Privatsphäre	Es sind Mechanismen umzusetzen, die sicherstellen, dass standardmäßig nur die personenbezogenen Daten verarbeitet werden, die für den jeweiligen spezifischen Zweck der Verarbeitung erforderlich sind und insbesondere, dass nicht eine größere Datenmenge erhoben und diese nicht für einen längeren Zeitraum gespeichert wird, als für diese Zwecke erforderlich ist.	[Beschreibung, wie das Ziel in Bezug auf die Privatsphäre umgesetzt wurde ODER Begründung, warum es nicht umgesetzt wurde]

Selbstverständlich kann jeder der vorstehenden Einträge mehrfach erfolgen, um gegebenenfalls jedes Ziel in Bezug auf die Privatsphäre weiter aufzuschlüsseln. „Datenqualität“ beispielsweise umfasst viele andere Grundsätze wie Datenminimierung und -vermeidung, Notwendigkeit und Verhältnismäßigkeit in Bezug auf die Zwecke usw. Darüber hinaus verdienen verschiedene Kontrollen, die verwendet werden, um dasselbe Ziel in Bezug auf die Privatsphäre zu erreichen, möglicherweise Einträge an unterschiedlichen Stellen, damit sie sich abheben.

Schlussendlich werden Datenschutzrisiken auf diese Weise verwaltet (bewertet und behandelt) und auf diese Weise wird beschrieben (und kann kontrolliert werden), was unternommen wird, um die Ziele in Bezug auf die Privatsphäre einzuhalten.

Ein gemischter Ansatz ist nach wie vor möglich, indem auch die Risiken untersucht werden, einige der Ziele in Bezug auf die Privatsphäre zu verfehlen (nicht nur im Bereich der Sicherheit, sondern beispielsweise auch in Bezug auf die Zweckbegrenzung, die Notwendigkeit und Verhältnismäßigkeit, die Vorratsdatenspeicherung, die Gewährung der Rechte der betroffenen Person usw.).