Sebastian Meissner

EuroPriSe 2.0: Neues vom europäischen Datenschutzgütesiegel

Das Datenschutzgütesiegel EuroPriSe wird an IT-Produkte und IT-basierte Dienstleistungen verliehen, die den Vorgaben des europäischen Datenschutzrechts entsprechen. Nach der durch die Europäische Union geförderten Projektphase wurden EuroPriSe-Zertifizierungen vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) angeboten. Seit Januar 2014 wird das European Privacy Seal von der EuroPriSe GmbH fortgeführt. Der Beitrag vermittelt grundlegende Informationen zu EuroPriSe und stellt die aktuellen Entwicklungen in einem Überblick dar.

1 Einleitung

Der 1. Januar 2014 ist für das europäische Datenschutzgütesiegel EuroPriSe ein wichtiges Datum: Zum Jahreswechsel ist das European Privacy Seal vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) auf die EuroPriSe GmbH übergegangen. Die Fortführung in privater Trägerschaft bietet dem Siegel neue Wachstums- und Entwicklungschancen. Gleichzeitig wird EuroPriSe die bewährten Zertifizierungskriterien, das qualitätsgesicherte zweistufige Verfahren und die Orientierung an höchsten Datenschutzstandards, wie sie von der sogenannten Artikel 29-Datenschutzgruppe[1] in Stellungnahmen und Arbeitspapieren ausgearbeitet werden, beibehalten. Durch die Mitwirkung in einem Beirat („Advisory Board") wird das ULD an der künftigen Entwicklung und inhaltlichen Ausgestaltung von EuroPriSe beteiligt sein. Darüber hinaus wird es auch weiterhin die Möglichkeit der Durchführung eines sogenannten Kombiverfahrens geben, nach dessen erfolgreichem Abschluss sowohl das EuroPriSe-Zertifikat als auch das Datenschutzgütesiegel Schleswig-Holstein verliehen werden. Geplant ist, das Portfolio von EuroPriSe künftig um die Möglichkeit weiterer Zertifizierungen (z. B. von Websites) zu ergänzen.

Nachfolgend wird zunächst die bisherige Entwicklung von EuroPriSe sowie die inhaltliche Ausgestaltung des Zertifizierungsschemas in einem Überblick vorgestellt. Im Anschluss hieran wird die Fortführung des Zertifizierungsprogramms durch die EuroPriSe GmbH einer genaueren Betrachtung unterzogen. Der Beitrag endet mit einem kurzen Ausblick.

1 Die Gruppe ist das unabhängige Beratungsgremium der EU in allen Fragen des Datenschutzes. Sie setzt sich aus Vertretern der nationalen Datenschutzaufsichtsbehörden, des Europäischen Datenschutzbeauftragten und der EU-Kommission zusammen.

Ass. iur. Sebastian Meissner

Head of Certification Authority bei der EuroPriSe GmbH; zuvor stellvertretender Referatsleiter des EuroPriSe-Referats beim ULD

E-Mail: meissner@european-privacy-seal.eu

2 EuroPriSe im Überblick

2.1 Start als EU-gefördertes Projekt

In seiner Anfangsphase (Juni 2007 – Februar 2009) wurde das europäische Datenschutzgütesiegel EuroPriSe von der Europäischen Union im Rahmen des eTEN-Programms gefördert.[2] Zu dem vom ULD geleiteten Konsortium gehörten neben privatwirtschaftlichen Unternehmen und öffentlichen Forschungseinrichtungen zwei weitere Datenschutzaufsichtsbehörden: Die französische CNIL und die Madrider APDCM. Zudem wird EuroPriSe seit dieser Frühphase vom Europäischen Datenschutzbeauftragten Peter Hustinx unterstützt.[3]

Während der Projektphase wurde das Konzept für ein europaweit angebotenes Datenschutzgütesiegel erarbeitet und im Rahmen von Pilotverfahren erprobt: Zunächst wurden Gutachter für das neue Zertifizierungsprogramm akkreditiert, anschließend mehrere Zertifizierungsverfahren erfolgreich abgeschlossen. Profitieren konnte EuroPriSe dabei von den Erfahrungen, die das ULD bereits mit dem Datenschutzgütesiegel Schleswig-Holstein gesammelt hatte.[4]

2.2 EuroPriSe unter ULD-Ägide

Aufgrund des positiven Verlaufs der Projektphase entschloss sich das ULD, das European Privacy Seal ab März 2009 in Eigenre-

2 Hierzu vgl. *Bock*, DuD 2007, S. 410 und *Meissner*, ADV-Mitteilungen, Ausgabe 1/2009, S. 7 ff.

3 Dieser hat seine Unterstützung insbesondere dadurch zum Ausdruck gebracht, dass er im Juli 2008 das erste Europäische Datenschutzgütesiegel an den Betreiber der Metasuchmaschine Ixquick überreicht hat. Hierzu vgl. den Jahresbericht 2008 des EDSB, S. 85. Dieser kann unter https://secure.edps.europa.eu/EDPSWEB/edps/lang/de/EDPS/Publications/AR abgerufen werden (letzter Abruf 25.1.2014).

4 Informationen hierzu können unter https://www.datenschutzzentrum.de/guetesiegel/ abgerufen werden (letzter Abruf 25.1.2014).

gie fortzuführen.[5] In dieser Zeit erhöhten sich Sichtbarkeit und Bekanntheitsgrad von EuroPriSe beträchtlich. Dies lässt sich etwa daran ablesen, dass dem European Privacy Seal sowohl in einem Informationsbericht des französischen Senats[6] als auch in einem vom EU-Parlament[7] verabschiedeten Bericht Vorbildcharakter attestiert worden ist. Auch die Kooperation mit den nationalen Datenschutzaufsichtsbehörden und der Artikel 29-Datenschutzgruppe wurde kontinuierlich ausgebaut, etwa durch Workshops mit einzelnen Aufsichtsbehörden, in denen diese umfassend über das Zertifizierungsprogramm informiert wurden.

Bis Ende 2013 konnten zwei Dutzend Erst- und sieben Rezertifizierungen erfolgreich abgeschlossen werden.[8] Insgesamt wurden mehr als 150 Gutachter aus 15 Mitgliedstaaten der Europäischen Union sowie aus Argentinien, der Schweiz, Taiwan und den Vereinigten Staaten von Amerika akkreditiert. Die Erfahrungen aus den Pilotzertifizierungen wurden dazu genutzt, das Zertifizierungsverfahren weiter zu verbessern und um zusätzliche Elemente zur Qualitätssicherung zu ergänzen: Insoweit ist insbesondere die Einführung des für IT-basierte Dienste obligatorischen Monitorings[9] zu nennen. Auch wurden Mechanismen implementiert, durch die sichergestellt werden soll, dass in vergleichbaren Verfahren stets auch ein ähnliches Maß an Prüftiefe angelegt wird.[10] Dies betrifft insbesondere die Tätigkeit der technischen Gutachter. Hat die Zertifizierungsstelle einem Gutachter in einem Verfahren aufgegeben, IT-Systeme vor Ort in einem bestimmten Umfang zu begutachten, so muss der gleiche Maßstab natürlich auch in einem vergleichbaren Verfahren angelegt werden.

Neben dem Zertifizierungsverfahren werden nachfolgend auch die Zertifizierungskriterien, die Gütesiegelaussage sowie der Anwendungsbereich des europäischen Datenschutzgütesiegels EuroPriSe kurz vorgestellt. Zudem erhält der Leser Informationen dazu, unter welchen Voraussetzungen ein rechtlicher oder technischer Datenschutzexperte als EuroPriSe-Gutachter akkreditiert werden kann.

2.3 Anwendungsbereich

Gegenwärtig können IT-Produkte und IT-basierte Dienstleistungen nach EuroPriSe zertifiziert werden.[11] Dabei reicht die Palette der in Betracht kommenden Dienste vom shreddergestützten Entsorgungsdienst für Akten und Datenträger, über den Digitalisierungsdienst für Fotos und Dias, bis hin zu web-basierten Diensten, wie Online-Shops, Internet-Suchmaschinen, Diensten zur verschlüsselten Kommunikation im Internet, sozialen Netzwerken oder webgestützten Hinweisgebersystemen. Für die Frage nach der grundsätzlichen Zertifizierbarkeit spielt es keine Rolle, ob der Anbieter des Dienstes personenbezogene Daten als verantwortliche Stelle („controller") oder als Auftragnehmer („processor") im Rahmen einer Auftragsdatenverarbeitung verarbeitet. In beiden Fällen kann ein Zertifizierungsverfahren angestrebt werden.

Der Begriff des IT-Produkts umfasst sowohl Hardware als auch Software: Zertifiziert werden können also beispielsweise eine Hochsicherheitsfestplatte, eine Hardware-Firewall, ein Softwaremodul zur Verschleierung von Videodaten oder eine Software zur Bereitstellung von Daten für Entwicklungs- oder Testzwecke. Weist eine Software servicespezifische Funktionalitäten auf, so ist sie allerdings als IT-basierter Dienst zu qualifizieren. Dies ist insbesondere der Fall, wenn die Software als Dienstleistung via Internet zur Verfügung gestellt wird (Stichwort „Software as a Service").

2.4 Gütesiegelaussage

Die Differenzierung zwischen Produkten und Diensten ist von erheblicher praktischer Bedeutung. Dies zeigt sich schon bei der mit der Verleihung eines EuroPriSe-Zertifikats zum Ausdruck gebrachten Gütesiegelaussage[12]: Einem IT-Produkt wird lediglich attestiert, dass dieses es der einsetzenden Stelle leicht macht, es in Vereinbarkeit mit EU-Datenschutzrecht zu verwenden. Einem IT-basierten Dienst kann hingegen bescheinigt werden, dass er alle relevanten datenschutzrechtlichen Vorgaben einhält. Hintergrund hierfür ist, dass bei einem IT-Produkt die es einsetzende Stelle entscheidet, ob alle rechtlichen Vorgaben eingehalten werden. Selbst ein noch so datenschutzfreundlich konzipiertes und konfiguriertes Produkt kann in einer Art und Weise zum Einsatz kommen, die gegen geltendes Datenschutzrecht verstößt. Geht es hingegen um einen IT-basierten Dienst, so kann im Rahmen einer EuroPriSe-Zertifizierung die konkrete Implementierung dieses Dienstes auf ihre Datenschutzkonformität hin überprüft werden.

Im Fokus einer EuroPriSe-Zertifizierung steht das geltende EU-Datenschutzrecht: Prüfungsmaßstab sind gegenwärtig also in erster Linie die Bestimmungen der allgemeinen Datenschutzrichtlinie 95/46/EG.[13] Anbieter von TK-Diensten müssen zudem auch die sektorspezifischen Vorgaben der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG[14] (sogenannte „ePrivacy-Richtlinie") beachten. Inwieweit darüber hinaus auch – die Richtlinien implementierendes – nationales Datenschutz-

5 Vgl. hierzu die einschlägige Pressemitteilung des ULD, die abgerufen werden kann unter https://www.datenschutzzentrum.de/presse/20081016-europrise-betriebsphase.htm (letzter Abruf 25.1.2014).

6 Eine inoffizielle Übersetzung der Passagen zu EuroPriSe ins Deutsche findet sich unter: https://www.datenschutzzentrum.de/europrise/20090529-franzoesischer-senat-europrise.html (letzter Abruf 25.1.2014).

7 Vgl. die entsprechende Pressemitteilung unter http://www.europarl.europa.eu/news/de/news-room/content/20101215IPR10208/html/Protecting-consumers-from-intrusive-new-advertising-on-the-internet (letzter Abruf 25.1.2014).

8 Eine Liste der zertifizierten IT-Produkte und IT-basierten Dienste ist abrufbar unter https://www.european-privacy-seal.eu/ws/EPS-en/Awarded-seals (letzter Abruf 25.1.2014).

9 Ausführungen hierzu erfolgen unter 2.6.

10 Vor Beginn der Evaluierung sind die von den Gutachtern geplanten Evaluierungsmethoden der Zertifizierungsstelle mitzuteilen. Diese überprüft, ob die benannten Maßnahmen die erforderliche Prüftiefe aufweisen und stellt sicher, dass es insoweit bei vergleichbaren Zertifizierungsverfahren nicht zu Abweichungen kommt.

11 Hierzu vgl. auch *Meissner*, Datenschutzgütesiegel als vertrauensbildende Maßnahme am Beispiel des europäischen EuroPriSe-Zeichens, in: Bogendorfer (Hrsg), Datenschutzgespräche 2011 – Datenschutz im Unternehmen, Jan Sramek Verlag, 2011, Kapitel D.I, S. 99 f.

12 Ausführliche Ausführungen zur Gütesiegelaussage finden sich auch bei *Meissner* (o. Fn. 11), Kapitel D.II, S. 100 ff.

13 Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, geändert durch Verordnung 1882/2003/EG. Der (konsolidierte) Richtlinientext kann abgerufen werden unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:DE:PDF (letzter Abruf 25.1.2014).

14 Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), zuletzt geändert durch Richtlinie 2009/136/EG. Der (konsolidierte) Richtlinientext ist abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:DE:PDF (letzter Abruf 25.1.2014).

recht als solches zu berücksichtigen ist, hängt wiederum davon ab, ob ein IT-Produkt oder ein IT-basierter Dienst zertifiziert werden soll.[15] Unabhängig hiervon bescheinigt das EuroPriSe-Zertifikat aber stets nur die Vereinbarkeit eines Zertifizierungsgegenstands mit EU-Datenschutzrecht im oben beschriebenen Sinne.

2.5 Zertifizierungskriterien

Die Zertifizierungskriterien sind aus den Bestimmungen der beiden Datenschutzrichtlinien 95/46/EG und 2002/58/EG abgeleitet worden. Ein Problem stellte insoweit der Umstand dar, dass beide Richtlinien nur abstrakt-generelle Vorgaben für die zu implementierenden technischen und organisatorischen Maßnahmen (TOM) enthalten.[16] Es war nämlich allein anhand dieser Vorgaben nicht möglich, aussagekräftige Kriterien – insbesondere für die technische Überprüfung eines Produkts oder Dienstes – abzuleiten. Aus diesem Grunde wurde auf Bestimmungen verschiedener nationaler Rechtsordnungen zurückgegriffen, in denen sich teils umfassende Regelungen zu den zu ergreifenden TOM finden.[17]

Der Kriterienkatalog besteht aus vier Komplexen[18]: Der erste Komplex befasst sich mit grundsätzlichen Fragen, die sich kurz mit „Wer verarbeitet welche personenbezogenen Daten zu welchen Zwecken?“ und „Erfolgt die Verarbeitung in transparenter und datensparsamer Art und Weise?“ zusammenfassen lassen. Der zweite Komplex betrifft rechtliche Fragestellungen wie insbesondere die nach dem Vorhandensein einer Rechtsgrundlage für jede Verarbeitung personenbezogener Daten. Im dritten Komplex ist die Angemessenheit der implementierten technischen und organisatorischen Maßnahmen zu prüfen. Der vierte Komplex schließlich hat die Betroffenenrechte auf Auskunft, Berichtigung, Löschung etc. zum Gegenstand.

Sowohl für die Anwendbarkeit einiger Kriterien (insbesondere aus dem eben erwähnten dritten Komplex) als auch für die konkrete Anwendung der anwendbaren Kriterien – insbesondere für Art und Ausmaß der technischen Prüfung – ist es wieder von Bedeutung, ob der Zertifizierungsgegenstand als IT-Produkt oder IT-basierter Dienst zu qualifizieren ist. Ausführliche Erläuterungen hierzu sind bereits an anderer Stelle gemacht worden.[19] Die jeweils aktuelle Fassung des Kriterienkatalogs kann auf der EuroPriSe-Website abgerufen werden.[20]

2.6 Zertifizierungsverfahren

Der Ablauf eines EuroPriSe-Zertifizierungsverfahrens lässt sich wie folgt zusammenfassen[21]: In einem ersten Schritt entscheidet sich der künftige Antragsteller (Siegelinteressent) für einen konkreten Zertifizierungsgegenstand (Target of Evaluation – ToE). Hierbei kann es sich um ein IT-Produkt oder einen IT-basierten Dienst handeln. Im Anschluss hieran beauftragt der Hersteller ein ihm als geeignet erscheinendes Team aus einem rechtlichen und einem technischen Gutachter mit der Evaluierung nach EuroPriSe. Bei der Auswahl der Gutachter kann auf die im öffentlichen Register der akkreditierten Gutachter verfügbaren Informationen zurückgegriffen werden.[22] Dem Antragsteller ist zu empfehlen, möglichst schon in diesem frühen Stadium des Verfahrens einen gemeinsamen Gesprächstermin mit den Gutachtern und der Zertifizierungsstelle zu vereinbaren. In einem solchen Erstgespräch können dann grundlegende Fragen zum Verfahren sowie zum Zuschnitt des ToE besprochen werden.

Formal angestoßen wird das Zertifizierungsverfahren mit der Einreichung eines Antragsformulars („Application for Certification“) bei der Zertifizierungsstelle. Diese bestimmt auf der Grundlage der ihr übermittelten Informationen die für das Verfahren anzusetzenden Gebühren. Im nächsten Schritt kommt es zum Vertragsschluss zwischen dem Antragsteller und der Zertifizierungsstelle. Bevor die Gutachter mit der technischen und rechtlichen Evaluierung des Zertifizierungsgegenstandes beginnen, ist der Zertifizierungsstelle mitzuteilen, welche Evaluationsmethoden (z. B. Dokumentencheck, Vorortprüfung) die Gutachter zur Anwendung bringen wollen.[23] Die Ergebnisse der sodann durchgeführten Evaluierung halten die Gutachter in einem Prüfbericht fest, der der Zertifizierungsstelle zugesandt wird.

Diese prüft das Gutachten auf Vollständigkeit, Nachvollziehbarkeit und Schlüssigkeit und stellt eine einheitliche Anwendung der Kriterien über verschiedene Verfahren hinweg sicher. Identifiziert die Zertifizierungsstelle im Rahmen der Validierung Fragen oder Problemstellungen, so werden diese mit den Gutachtern diskutiert und einer Klärung zugeführt. Im Anschluss hieran erstellen die Gutachter ein Kurzgutachten, das die wesentlichen Ergebnisse der Evaluierung enthält und nach Freigabe durch den Antragsteller auf der EuroPriSe-Website veröffentlicht wird.[24]

Nach Veröffentlichung des Kurzgutachtens kann das EuroPriSe-Zertifikat verliehen werden. Folgende Abildung gibt das Verfahren nochmals vereinfacht wieder:

Abbildung 1 | Verfahren

15 Vgl. *Meissner* (o. Fn. 11), Kapitel D.II.2, S. 101 ff.

16 Siehe Art. 17 RL 95/46/EG bzw. Art. 4 RL 2002/58/EG.

17 Ausführliche Informationen hierzu sowie allgemein zur Entwicklung der Kriterien finden sich bei *Meissner*, DuD 2008, S. 525 (S. 527 ff.).

18 Vgl. *Meissner*, DuD 2008, S. 525 (S. 529 ff.).

19 Vgl. *Meissner* (o. Fn. 11), Kapitel F.I.1.b), S. 112 f.

20 Der Kriterienkatalog ist abrufbar unter https://www.european-privacy-seal.eu/ws/EPS-en/Criteria (letzter Abruf 25.1.2014).

21 Vgl. hierzu auch *Meissner* (o. Fn. 11), Kapitel F.I.2, S. 115 ff.

22 Das Gutachterregister ist abrufbar unter https://www.european-privacy-seal.eu/ws/EPS-en/Register-of-experts (letzter Abruf 25.1.2014).

23 Hierzu vgl. schon o. Fn. 10.

24 Links zu den Kurzgutachten finden sich in den von der Zertifizierungsstelle angefertigten Übersichtstabellen mit grundlegenden Informationen zu den einzelnen Verfahren (vgl. z. B. unter https://www.european-privacy-seal.eu/ws/EPS-en/Business-Keeper, letzter Abruf 25.1.2014).

Das Zertifikat ist für einen Zeitraum von zwei Jahren gültig. Während dieses Zeitraums ist der Hersteller dazu verpflichtet, der Zertifizierungsstelle datenschutzrechtlich relevante Änderungen am ToE mitzuteilen. Bei IT-basierten Diensten muss im Rahmen eines formalisierten Verfahrens („Monitoring") von den Gutachtern aktiv geprüft werden, ob es zu relevanten Änderungen gekommen ist.[25] Die Ergebnisse dieser Überprüfungen sind der Zertifizierungsstelle im Monat acht und erneut im Monat 16 nach einer erfolgten Zertifizierung mitzuteilen. Bei gravierenden Änderungen kann eine vorzeitige Rezertifizierung erforderlich werden. Anderenfalls bleibt es bei der Gültigkeitsdauer von zwei Jahren. Folgende Abbildung zeigt das Zertifikat und erläutert die in diesem enthaltenen Angaben:

Abbildung 2 | Siegel mit Erläuterungen

Eine Verlängerung der Gültigkeit kann im Wege der Rezertifizierung herbeigeführt werden. Im Rahmen einer solchen Rezertifizierung wird überprüft, ob sich der Zertifizierungsgegenstand, der Stand der Technik oder die rechtlichen Rahmenbedingungen geändert haben. Erfüllt das ToE nach wie vor alle anwendbaren Zertifizierungskriterien, kann das Rezertifizierungsverfahren erfolgreich abgeschlossen werden. Hierdurch verlängert sich die Gültigkeit des Zertifikats um zwei Jahre.

2.7 Akkreditierte Gutachter

Wie bereits dargestellt, wird die Evaluierung des Zertifizierungsgegenstands bei EuroPriSe durch von der Zertifizierungsstelle akkreditierte Gutachter durchgeführt. Diese werden entweder für den Bereich Recht oder für den Bereich Technik akkreditiert, in seltenen Fällen ist auch eine Doppelakkreditierung möglich. Akkreditierte Gutachter müssen über fundierte rechtliche bzw. technische Kenntnisse im Bereich des Datenschutzes verfügen und diese durch eine mehrjährige einschlägige Berufserfahrung unter Beweis gestellt haben. Als Gutachter zugelassen wird nur, wer neben der fachlichen Expertise und Berufserfahrung auch die erforderliche Zuverlässigkeit aufweist. Diese liegt beispielsweise dann nicht vor, wenn über das Vermögen einer Person ein Insolvenzverfahren eröffnet worden ist. Voraussetzung für eine Akkreditierung ist schließlich die Teilnahme an einem speziellen Akkreditierungsworkshop für EuroPriSe-Gutachter und die erfolgreiche Anfertigung eines Trainingsgutachtens zu einem während des Workshops vorgestellten fiktiven Produkt oder Dienst.

Die Erstakkreditierung eines Gutachters ist für einen Zeitraum von drei Jahren gültig. Die Gültigkeit kann um jeweils drei Jahre verlängert werden, wenn ein Gutachter an einem Fortbildungsworkshop („Expert Enhancement Workshop") teilnimmt oder wenn er erfolgreich die Evaluierung eines „echten" Produkts oder Dienstes nach EuroPriSe abschließt.[26] Eine Verlängerung erfolgt dann zu dem Zeitpunkt, zu dem das EuroPriSe-Zertifikat an den jeweiligen Antragsteller verliehen wird. Nicht ausreichend ist der Abschluss einer Rezertifizierung, da diese üblicherweise mit einem erheblich geringeren Aufwand verbunden ist als eine Erstzertifizierung.

3 EuroPriSe 2.0: Was bleibt, was ändert sich?

3.1 Kriterien und Verfahren haben Bestand

Es wird keine Änderungen am Zertifizierungsverfahren und an den Zertifizierungskriterien bei EuroPriSe geben. Sowohl das bewährte qualitätsgesicherte Verfahren als auch der vielfach erprobte Kriterienkatalog kommen weiterhin zur Anwendung. Die jeweils aktuelle Fassung des Katalogs[27] sowie Informationen zum Ablauf des Verfahrens werden nach wie vor auf der EuroPriSe-Website zum Abruf bereitgehalten und sind damit für jedermann einsehbar und transparent. Gleiches gilt für die Ergebnisse einer erfolgreichen Evaluierung nach EuroPriSe, die in Gestalt von Kurzgutachten und Übersichtstabellen auf der EuroPriSe-Website veröffentlicht werden.[28] Dies erlaubt es interessierten Personen nachzuvollziehen, wie die Zertifizierungskriterien im konkreten Einzelfall angewendet worden sind (Stichwort: „Prüfbarkeit").

Bei der Anwendung der EuroPriSe-Kriterien orientieren sich die akkreditierten Gutachter und die Zertifizierungsstelle auch weiterhin an dem hohen Datenschutzstandard, wie er von der Artikel 29-Datenschutzgruppe in Stellungnahmen und Arbeitspapieren definiert wird.[29] Die Zusammenarbeit mit der Gruppe wird fortgeführt und soll in Zukunft noch intensiviert werden. Eine wichtige Rolle wird in diesem Zusammenhang das u. a. mit Vertretern von Datenschutzaufsichtsbehörden besetzte unabhängige Expertengremium („Advisory Board") spielen, auf das in der Folge näher eingegangen wird.

3.2 ULD wird Mitglied im Advisory Board

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein bleibt EuroPriSe eng verbunden: Zum einen wird das ULD über das Advisory Board die weitere Entwicklung des European Privacy Seal mit beeinflussen, zum anderen ist es auch weiterhin möglich, das Gütesiegel Schleswig-Holstein und das EuroPriSe-Zertifikat in einem kombinierten Verfahren zu erwerben.

Aufgabe des unabhängigen Expertengremiums wird es sein, die Weiterentwicklung von EuroPriSe beratend zu begleiten. Dies betrifft beispielsweise die Vornahme von Änderungen am Krite-

25 Zum Monitoring vgl. auch *Meissner* (o. Fn.11), Kapitel F.I.2.c), S. 118 f.

26 Dabei ist der jeweilige Verlängerungstatbestand zu verwirklichen, bevor der Gültigkeitszeitraum der Akkreditierung abläuft.

27 Hierzu siehe schon o. Fn. 20.

28 Vgl. o. Fn. 24.

29 Diese können abgerufen werden unter http://ec.europa.eu/justice/data-protection/article-29/documentation (letzter Abruf 25.1.2014).

rienkatalog, wie sie insbesondere bei Änderungen der rechtlichen Rahmenbedingungen erforderlich werden. Man denke insoweit nur an die Auswirkungen, die das Inkrafttreten einer künftigen Datenschutzgrundverordnung auf den EuroPriSe-Kriterienkatalog haben würde. Das Expertengremium wird auch konsultiert werden, bevor neue Zertifizierungsprodukte (z. B. die Zertifizierung von Webseiten oder von Schulungsmaterialien) angeboten werden.[30] Auch in diesem Zusammenhang wird es eine wichtige Aufgabe des Gremiums sein, künftige Zertifizierungsschemata und spezielle Kriterienkataloge einer eingehenden Vorabprüfung zu unterziehen. EuroPriSe wird die Ergebnisse einer solchen Prüfung und die von dem Advisory Board ausgesprochenen Empfehlungen bei der Weiterentwicklung des Siegels berücksichtigen.

Das Advisory Board wird aus mehreren ausgewiesenen Datenschutzexperten bestehen. Aufgrund des europäischen Ansatzes von EuroPriSe werden diese Experten aus verschiedenen Mitgliedstaaten der Europäischen Union stammen. Neben Vertretern von Aufsichtsbehörden (wie dem ULD) und anderen Organisationen wird ein Mitglied des Advisory Boards aus den Reihen der akkreditierten EuroPriSe-Gutachter stammen. Diese Person wird von den Gutachtern im Rahmen einer Wahl bestimmt und für einen Zeitraum von drei Jahren in das Gremium entsandt. Nach Ablauf dieses Zeitraums wird eine erneute Wahl durchgeführt, wobei eine Wiederwahl des bisher im Advisory Board vertretenen Gutachters möglich ist. Dadurch, dass auch Vertreter von Datenschutzaufsichtsbehörden in dem Gremium vertreten sein werden, wird dieses auch zu einer Intensivierung des Kontakts zur Artikel 29-Datenschutzgruppe beitragen.

3.3 Kombiverfahren auch weiterhin möglich

Will ein Hersteller national und international auftreten, so kann es für ihn sinnvoll sein, sowohl eine Zertifizierung nach EuroPriSe als auch die Auszeichnung mit dem Datenschutzgütesiegel Schleswig-Holstein anzustreben. Schon bislang war es möglich, in einem solchen Fall beide Verfahren zu verbinden und ein sogenanntes Kombiverfahren durchzuführen. Ein solches Verfahren bietet dem Antragsteller Kostenvorteile gegenüber der Durchführung zweier getrennter Verfahren.

Beim Kombiverfahren wird stets eines der beiden Zertifizierungsprogramme (Datenschutzgütesiegel Schleswig-Holstein oder EuroPriSe) die führende Rolle übernehmen. Die Zertifizierungsstelle des jeweils anderen Programms wird dann die Vorarbeiten des führenden Programms nutzen, wodurch Synergieeffekte erzielt werden. Interessierte Antragsteller erteilen vor Beginn des Verfahrens ihr Einverständnis dazu, dass für das Kombiverfahren relevante Informationen zwischen dem ULD und der EuroPriSe GmbH ausgetauscht werden dürfen.

3.4 Übernahme von Gutachtern und Zertifizierungsverfahren

Zertifizierungsverfahren, die bereits vor dem 1.1.2014 durch das ULD begonnen wurden, werden von EuroPriSe unter der Voraussetzung fortgeführt, dass der Antragsteller sich hiermit und mit der Übermittlung aller relevanten Informationen vom ULD an die EuroPriSe GmbH einverstanden erklärt. Anzumerken ist, dass die Fortführung der Verfahren durch EuroPriSe zu keinen zusätzlichen Kosten für den Antragsteller führt. Vielmehr verbleibt es bei den mit dem ULD bereits vereinbarten Zertifizierungsgebühren.

EuroPriSe akzeptiert die Akkreditierungen von in der Vergangenheit durch das ULD zugelassenen Gutachtern und listet diese im Gutachterverzeichnis auf der EuroPriSe-Website auf. Voraussetzung hierfür ist, dass die Gutachter sich hiermit und mit der Übermittlung aller relevanten Informationen an EuroPriSe einverstanden erklären und ihre Akkreditierung zum Zeitpunkt des Übergangs noch gültig ist bzw. zeitnah reaktiviert wird.

Eine bereits unter ULD-Ägide angedachte Neuerung besteht in der Einführung eines jährlich anfallenden Akkreditierungsbeitrags in Höhe von 390 Euro, der von allen akkreditierten Gutachtern zu entrichten ist. Durch diesen Beitrag wird insbesondere die kostenlose Teilnahme an einem Fortbildungsworkshop für EuroPriSe-Gutachter während eines Akkreditierungszyklus (Dauer: drei Jahre) abgedeckt. Darüber hinaus wird der Beitrag zur Deckung der Unkosten für folgende Tätigkeiten von EuroPriSe erhoben:

- Versand eines qualitativ und quantitativ verbesserten Newsletters mit relevanten Informationen für EuroPriSe-Gutachter;
- Bereitstellung von Tools und Arbeitsplattformen;[31]
- Regelmäßiges Einpflegen von Updates zu Rechtsprechung, Stellungnahmen der Art. 29-Gruppe etc. in den EuroPriSe-Kommentar für Gutachter;
- Verwaltung und Aktualisierung des Gutachterverzeichnisses auf der EuroPriSe-Website;
- Organisation und Durchführung der Wahl des Gutachtervertreters für das neu geschaffene Advisory Board;
- Zurverfügungstellung von Werbemitteln (insbesondere von Logos) für EuroPriSe-Gutachter.

3.5 Arbeitserleichterung durch neue Arbeitsmittel und Tools

EuroPriSe stehen seit 1.1.2014 neue Arbeitsmittel und Tools zur Verfügung, die die Arbeit von Antragstellern, Gutachtern und Zertifizierungsstelle erleichtern sollen. Zu nennen ist insoweit „Secure File Exchange“, eine Plattform für den sicheren Datenaustausch. Hierüber können während eines Zertifizierungsverfahrens vertrauliche Dokumente wie Prüfgutachten, Auditberichte oder andere zertifizierungsrelevante Dokumente (z. B. Auftragsdatenverarbeitungsverträge oder IT-Sicherheitskonzepte) projektbezogen ausgetauscht werden. Die Verfahrensbeteiligten erhalten hierdurch eine zusätzliche[32] Möglichkeit für den sicheren Dokumentenaustausch, deren Vorteil in ihrer einfachen Handhabbarkeit besteht.

Webbasierte Trainings für Antragsteller informieren darüber wie ein Zertifizierungsverfahren nach EuroPriSe abläuft und wie man sich hierauf vorbereiten können. Akkreditierten Gutachtern, die noch keine praktische Erfahrung mit der Durchführung von EuroPriSe-Verfahren gesammelt haben, werden durch ein solches Training grundlegende Informationen sowie Best Practice-Empfehlungen zur Gutachtertätigkeit im Rahmen eines Verfahrens vermittelt.

30 Nähere Ausführungen zur geplanten Einführung neuer Zertifizierungsprodukte erfolgen unter 3.7.

31 Nähere Informationen hierzu finden sich in Kapitel 3.5.

32 Weitere Optionen bestehen in der Versendung PGP-verschlüsselter E-Mails oder passwortgesicherter ZIP-Archive / PDF-Dokumente.

Umfragen und Wahlen für das Advisory Board werden mit softwaregestützten Tools durchgeführt.

3.6 Ausweitung der internationalen Präsenz

EuroPriSe kommt zu den Siegelinteressenten und Datenschutzexperten. Auch wenn EuroPriSe von Anfang an als europa- bzw. sogar weltweit angebotenes Zertifizierungsprogramm konzipiert gewesen ist, waren die Möglichkeiten, international präsent zu sein, während der durch das ULD als Landesdatenschutzbehörde angebotenen Betriebsphase naturgemäß stark limitiert. Dadurch, dass die Gründungsgesellschafterin der EuroPriSe GmbH, die 2B Advice-Gruppe, über Standorte in mehreren Ländern Europas und in den USA verfügt, ergeben sich hier neue Möglichkeiten und Chancen (beispielsweise bei der Akquirierung von Zertifizierungsverfahren) für EuroPriSe.

Von der internationaleren Ausrichtung profitieren auch die angehenden sowie die bereits akkreditierten EuroPriSe-Experten: Akkreditierungs- und Fortbildungsworkshops werden künftig nicht nur am Sitz von EuroPriSe in Bonn, sondern auch an weiteren Standorten in unterschiedlichen Mitgliedstaaten der Europäischen Union sowie (potentiell) auch außerhalb von Europa – z. B. in den Vereinigten Staaten – durchgeführt werden. Für das Jahr 2014 sind bereits Akkreditierungs- und Fortbildungsworkshops für Gutachter in Wien und London geplant.[33] Die Akkreditierungs- und Fortbildungsworkshops werden künftig zusammengelegt, damit die neuen Experten gleich von dem Fortbildungsworkshop profitieren können und ein Austausch zwischen neuen und erfahrenen Gutachtern ermöglicht wird.

3.7 Einführung neuer Zertifizierungsprodukte

Zu Beginn der EuroPriSe-Projektphase wurde bewusst die Entscheidung getroffen, den Anwendungsbereich des Zertifizierungsprogramms zunächst auf die Zertifizierung von IT-Produkten und IT-basierten Diensten zu beschränken – dies allerdings mit der Option darauf, das Spektrum der angebotenen Zertifizierungsleistungen bei Bedarf später entsprechend zu erweitern. Von dieser Option wurde während der sich an die Projektphase anschließenden Betriebsphase von EuroPriSe beim ULD kein Gebrauch gemacht, obwohl mehrfach konkret über eine solche Ausweitung nachgedacht wurde. Ein wichtiger Grund dafür, auf die Erweiterung der EuroPriSe-Produktpalette zu verzichten, war der Umstand, dass für die Konzeption und Implementierung eines neuen Zertifizierungsprodukts nicht unerhebliche personelle Ressourcen benötigt werden.

EuroPriSe plant nun, die bestehende Produktpalette um weitere Arten von Zertifizierungsgegenständen zu ergänzen, um an einer Zertifizierung interessierten Organisationen zusätzliche Optionen zur Verfügung zu stellen. So wäre es gut denkbar, die mit der Zertifizierung von Produkten und Diensten gemachten Erfahrungen auf die Zertifizierung von Verfahren, Konzepten, Personen, Schulungen, Datenverarbeitungen im Auftrag oder Webseiten zu übertragen. Die vergangenen Jahre haben gezeigt, dass gerade bei kleineren und mittleren Unternehmen (KMU) der Bedarf besteht, zunächst mit einer Art „Einstiegs- oder Basiszertifizierung" mit einem überschaubaren Zertifizierungsgegenstand und weitgehend standardisierten Prüfungen durch die Gutachter Erfahrungen zu sammeln, bevor die oft mit erheblichen personellen und finanziellen Aufwänden verbundene Zertifizierung eines IT-Produkts oder IT-basierten Dienstes angegangen wird. Vor diesem Hintergrund wird demnächst ein Konzept zur Zertifzierung von Websites durch EuroPriSe erstellt und dem unter 3.2 vorgestellten Advisory Board vorgelegt werden.

Klar kommuniziert werden muss bei einer Erweiterung der Produktpalette, was mit der jeweiligen Zertifizierung bescheinigt wird und wie umfangreich die durch die Gutachter durchzuführenden rechtlichen und technischen Prüfungen jeweils sind. Vermieden werden müsste etwa, dass ein Unternehmen, das eine Basiszertifizierung – wie bspw. die Überprüfung einer Webseite auf Grundlage stark standardisierter Prüfmethoden und mit Hilfe von Standard-Prüftools – abgeschlossen hat, erfolgreich den Eindruck erwecken kann, dass dieser Zertifizierung die gleiche „Wertigkeit" zukommt wie der Zertifizierung eines komplexen IT-basierten Dienstes. Auch für alle neuen Zertifizierungsangebote werden die Zweistufigkeit des Verfahrens und die Einbindung der akkreditierten Gutachter erhalten bleiben. Eine Prüfung erfolgt zunächst durch technische und rechtliche Experten, bevor die Zertifizierungsstelle die schriftlich fixierten Ergebnisse der Prüfung validiert und ggf. selbst stichprobenartige Checks vornimmt.

4 Ausblick

Die Fortführung durch die EuroPriSe GmbH bietet für EuroPriSe neue Chancen und Möglichkeiten. Durch eine internationalere Ausrichtung und eine beispielsweise um die Zertifizierung von Webseiten ergänzte Produktpalette wird es möglich, die Sichtbarkeit von EuroPriSe erheblich zu steigern und diesem inhaltlich bereits sehr ausgereiften Zertifizierungsprogramm deutlich bessere Wachstumsmöglichkeiten zu geben, als dies bisher der Fall gewesen ist.

Gleichzeitig haben das bewährte Zertifizierungsverfahren und der Kriterienkatalog weiterhin Bestand und dienen als Vorbild für eventuelle Weiterentwicklungen. Die Qualität solcher Weiterentwicklungen wird nicht zuletzt durch die beratende Funktion des mit ausgewiesenen Datenschutzexperten besetzten Advisory Board sichergestellt werden.

33 Informationen hierzu sind abrufbar unter https://www.european-privacy-seal.eu/ws/EPS-en/Expert-workshops (letzter Abruf 25.1.2014).