Der „Einheitliche Ansprechpartner“ nach der Dienstleistungsrichtlinie

Aspekte des Datenschutzes und der Datensicherheit

Arbeitskreise "Technik" und "Verwaltungsmodernisierung"
der Landes- und des Bundes-Datenschutzbeauftragten

AK "Technik"
(Leitung: Gabriel Schulz, Mecklenburg Vorpommern, datenschutz@mvnet.de)

AK „Verwaltungsmodernisierung"
(Leitung: Andreas Schneider, Andreas.Schneider@slt.sachsen.de).

1. Einleitung

Nach Art. 8 Abs. 1 der Richtlinie über Dienstleistungen im Binnenmarkt 2006/123/EG vom 12. Dezember 2006 - Dienstleistungsrichtlinie, nachfolgend abgekürzt mit DL-RL - stellen die Mitgliedstaaten sicher, dass alle Verfahren und Formalitäten , die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner (EA) oder bei der betreffenden zuständigen Behörde abgewickelt werden können.

Dieser EA soll nach der Richtlinie als Mittler zwischen den Dienstleistungserbringern und den zuständigen Behörden agieren. Anderenfalls kann der EA auch selbst zuständige Behörde sein, soweit ihm die Ausstellung der für die Aufnahme der Dienstleistungstätigkeit erforderlichen Dokumente obliegt. Da weiterhin die Möglichkeit besteht, sich direkt an die zuständige Behörde zu wenden oder ggf. den Weg im Verfahren zu wechseln, kann auch eine Abstimmung zwischen EA und dieser Stelle erforderlich werden. In allen Fällen sind Überlegungen zum Datenschutz und zur Datensicherheit anzustellen. Vorab müssen jedoch die Aufgaben des EA sowie die verschiedenen Abwicklungsarten beleuchtet werden, da diese die Basis für weitere Untersuchungen darstellen.

Nach Art. 43 der DL-RL sind bei deren Umsetzung und Anwendung, und insbesondere der Bestimmungen über Kontrollen, die Vorschriften zum Schutz personenbezogener Daten (Richtlinie 95/46/EG und Richtlinie 2002/58/EG) einzuhalten. Mit der Umsetzung der DL-RL ist verbunden, dass nicht nur die für eine Erlaubnis, Genehmigung oder Entgegennahme einer Anzeige oder Registrierung für die Aufnahme einer Dienstleistungstätigkeit zuständige Behörde, sondern auch der EA personenbezogene Daten erhebt, standardisiert zugänglich und verarbeitbar macht, und zwar im elektronischen Verfahren. Regelungen zur Verarbeitung personenbezogener Daten finden sich den Datenschutzgesetzen des Bundes und der Länder sowie in einzelnen Spezialgesetzen. Für Verfahren, die

- ein EA selber zur Aufgabenerfüllung nutzt,
- für die Zusammenarbeit zwischen einem EA und den Behörden,
- zwischen den Behörden innerhalb eines Bundeslandes sowie
- für die technisch neu auszugestaltenden Fachverfahren innerhalb der einzelnen Behörden dienen,

sind insbesondere die Landesdatenschutzgesetze der jeweiligen Bundesländer einschlägig.

Die Datenschutzgesetze der Länder sowie das Bundesdatenschutzgesetz stimmen in ihren Regelungsprinzipien weitgehend überein. So bedarf jede Datenverarbeitung einer Rechtsgrundlage (z.B. Einwilligung des Betroffenen, Gesetz, Vertrag oder betriebliche Vereinbarung). Eine Einwilligung ist nur dann wirksam, wenn der Betroffene vorher ausreichend informiert wurde und die Einwilligung freiwillig erfolgte. Personenbezogene Daten dürfen ferner nur für den explizit anzugebenden Zweck erhoben und verwendet werden. Weiterhin ist die Datenverarbeitung auf den für den Erhebungszweck notwendigen Umfang zu begrenzen, insbesondere im Hinblick auf die Art und Menge der verarbeiteten Daten. Die Erhebung und Verarbeitung von Daten muss gegenüber den Betroffenen transparent sein, damit dieser seine Auskunfts-, Berichtigungs-, Sperrungs- und Löschungsrechte ausüben kann. Datenschutz kann nur dann gewährleistet werden, wenn personenbezogene Daten

sicher, das heißt zumindest vertraulich und integer von einer zuständigen Stelle, verarbeitet werden. Dem besonderen Schutzbedarf streng persönlicher Daten ist Rechnung zu tragen. Sind – wie hier – Datentransporte erforderlich, gilt das auch für den Übertragungsweg. Und nicht zuletzt muss eine Daten verarbeitende Stelle ihre Datenverarbeitung so anlegen, dass diese für die zuständigen Aufsichtsbehörden fortlaufend kontrollierbar ist.

2. Die Aufgaben des Einheitlichen Ansprechpartners im Überblick

Nach den Bestimmungen der DL-RL treffen den EA folgende Pflichten:

a) Abwicklung von Formalitäten und Verfahren über den EA (Art. 6 Abs. 1).
Die Unterscheidung zwischen *„Formalitäten" und „Verfahren"* dürfte sich auf Formerfordernisse wie z.B. Schriftform- oder Beglaubigungserfordernisse einerseits und fach- und verwaltungsverfahrensbezogene Regelungen andererseits beziehen. „Erklärungen und Anmeldungen" sind daher eher als Formalitäten, „Beantragungen von Genehmigungen oder Beantragungen von Registereintragungen" eher als Verfahren anzusehen. Zu beachten ist, dass nicht nur die „Aufnahme", sondern auch die „Ausübung" der Dienstleistungstätigkeit über den EA abgewickelt werden soll, vgl. Art. 8 Abs. 1. Hierbei können personenbezogene Daten, ggf. auch mit hohem Schutzbedarf wie z.B. Gesundheitszeugnisse, anfallen.

b) Bereitstellung von Informationen, ggf. durch Abruf (Art. 7 Abs. 1).
Umfasst sind etwa Angaben über die zuständigen Behörden oder Informationen zu Mitteln und Bedingungen für den Zugang zu öffentlichen Registern und Datenbanken. Da die Mitgliedstaaten nach Art. 7 Abs. 3 u.a. sicherstellen müssen, dass „Informationen und Unterstützung aus der Ferne und elektronisch leicht zugänglich sind", spricht hier Einiges für die Einrichtung eines automatisierten Abrufverfahrens, bei dem seitens des Antragstellers nur wenige personenbezogene Daten anfallen werden.

c) Zügige Beantwortung von Auskunfts- und Unterstützungsersuchen sowie unverzügliche Benachrichtigung des Antragstellers, wenn dessen Ersuchen fehlerhaft oder unbegründet ist (Art. 7 Abs. 4).
Dies umfasst die Bearbeitung von Unterstützungsersuchen, wobei offenbar eine Einzelfallprüfung durch den EA stattfinden soll, jedoch kein automatisierter Datenabruf. Da nach Art. 7 Abs. 3 auch eine „Unterstützung" auf elektronischem Wege realisiert werden soll, kommt eine Umsetzung im Wege einer Online-Auskunft in Betracht, d.h. der Antragsteller wird nach Prüfung seines Ersuchens bspw. per E-Mail informiert. Die Prüfung, inwieweit das Ersuchen des Antragstellers fehlerhaft oder unbegründet ist, wirft die Frage auf, ob die Aufgabenerfüllung durch den EA eine inhaltliche Kenntnisnahme impliziert und inwiefern dabei eine Verarbeitung personenbezogener Daten erfolgt. Für die Feststellung, ob ein Auskunfts- oder Unterstützungsersuchen „fehlerhaft" ist, dürfte eine inhaltliche Kenntnisnahme nicht erforderlich werden, soweit nur formelle Mängel des Ersuchens geprüft werden[1]. Da Art. 7 Abs. 4 die Regelung des Art. 7 Abs. 2 in Bezug nimmt, obliegen die Auskunftserteilung und Unterstützungsleistung nicht allein den zuständigen Behörden, sondern auch den EA im Sinne einer Beratung zu den Anforderungen, die

[1] *Zu einer Vollständigkeitskontrolle gehört auch die Überprüfung, ob vorgelegte Unterlagen tatsächlich beinhalten, was sie ihrer Bezeichnung nach beinhalten sollten. Hier ließe sich bis zu einem gewissen Grade durch automatisierte Verfahren etwas ausrichten, die feststellen, ob Schlüsselworte vorkommen oder eine Grafik auch eine Grafik ist.*

für die Aufnahme einer Dienstleistungstätigkeit bestehen. Der EA wird im Hinblick auf einzelne Anfragen Vorgänge anlegen und auch personenbezogene Daten (d.h. die Anfragen der Dienstleistungserbringer) speichern, insbesondere dann, wenn Rückfragen bei den zuständigen Behörden notwendig werden, um der eigenen Beratungspflicht nachkommen zu können. Demnach erfolgt wahrscheinlich eine Verarbeitung personenbezogener Daten. Es kommt nicht zu einer bloßen Durchleitung von Informationen an die Behörden, sondern der EA wird selbst als Prüfinstanz tätig**.**

d) Bereitschaft, die Informationen in Art. 7 auch in der Landessprache des Antragstellers bereitzustellen (Art. 7 Abs. 5)
Zumindest sollten die Kommission und die Mitgliedstaaten begleitende Maßnahmen ergreifen, um die Bereitschaft des EA zu fördern, die in Art. 7 genannten Informationen auch in anderen Gemeinschaftssprachen bereitzustellen. Personenbezogene Daten sind hierbei nicht betroffen.

e) Entgegennahme und Verarbeitung von Daten der Dienstleistungserbringer, soweit sich Änderungen (etwa zu den Voraussetzungen der Genehmigung) ergeben (Art. 11 Abs. 3).
Auch hier erfolgt eine Verarbeitung personenbezogener Daten. Der EA nimmt nicht lediglich eine Botenfunktion wahr, sondern er wird aller Voraussicht nach die übermittelten personenbezogenen Daten speichern und folglich verarbeiten.

3. Zwei Abwicklungsarten

Die Dienstleistungsrichtlinie will zwei Möglichkeiten einer elektronischen Abwicklung von „Verfahren und Formalitäten“ bieten (Art. 8 Abs. 1):

- die Abwicklung über den EA und
- bei der betreffenden zuständigen Behörde.

Die beiden Verfahrenszuständigkeiten wurden in der Dienstleistungsrichtlinie nicht klar voneinander getrennt, sondern es finden sich - verstreut über die Art. 6 ff. - Regelungen, die teilweise nur *für eine Abwicklungsart* passen, teilweise jedoch auch *für beide Abwicklungsarten* Geltung beanspruchen. Im Ergebnis wird von der Dienstleistungsrichtlinie eine parallele Ingangsetzung beider Abwicklungsarten in Kauf genommen:

a) Wendet sich der Antragsteller direkt an die zuständigen Behörden, so bleibt ihm parallel die Möglichkeit, über den EA Informationen nach Art. 7 Abs. 1 einzuholen.

b) Im Hinblick auf Art. 7 Abs. 2 werden zwar die zuständigen Behörden verpflichtet, allerdings bleibt eine Auskunft der Behörden auch dann sinnvoll, wenn der Antragsteller eine Abwicklung über den EA wünscht. Daher ist Art. 7 Abs. 2 über Art. 7 Abs. 4 anwendbar.

c) Die in Art. 7 Abs. 4 geregelte Beantwortungs- und Prüfungspflicht trifft die Behörden und den EA gleichermaßen und besteht in beiden Abwicklungsvarianten. Allerdings verschwimmen hier zunehmend die Grenzen zwischen den beiden Abwicklungsvarianten: Die Wahrnehmung der Pflichten in Art. 7 Abs. 4 kann für den EA eigentlich nur dann Bedeutung haben, wenn der Antrag auch bei ihm - zur

Weiterleitung an die Behörde - eingereicht wurde, eine Abwicklung also über den EA erfolgen soll. Bei der Abwicklung über den EA besteht allerdings eine parallele Beantwortungs- und Prüfungspflicht für die Behörde, sodass der Antragsteller sich zusätzlich an diese wenden kann. Auch im umgekehrten Fall, d.h. wenn der Antragsteller die Abwicklung über die Behörden begehrt, bleibt ihm die Möglichkeit, eine Beantwortung und Prüfung durch den EA zu verlangen. Dies könnte in der Praxis zu Doppelarbeit, zu unterschiedlichen Fristsetzungen und ggf. zu unterschiedlichen Ergebnissen führen.

d) Art. 11 Abs. 3 sieht zwingend vor, dass der EA über Änderungen beim Dienstleister zu informieren ist. Allerdings dürfte diese Bestimmung für den Fall keine Bedeutung haben, wenn die Abwicklung direkt bei der Behörde vorgenommen wurde. „Sinnvoll“ bleibt Art. 11 Abs. 3 bei einer Abwicklung über die Behörden wohl insoweit, als der EA parallel in Anspruch genommen wird oder dieser im Rahmen der Ausübung der Dienstleistungstätigkeit (nicht im Rahmen des Aufnahmeverfahrens) vom Dienstleistungserbringer kontaktiert wird.

4. Perspektiven einer datensicherheitstechnischen Umsetzung

In den verschiedenen Interpretationen der DL-RL ist davon die Rede, dass der EA auf eine ordnungsgemäße und zügige Bearbeitung hinzuwirken und dafür den Verfahrensgegenstand zu kennen hat. Die bislang vorgestellten Konzepte und Modelle zum EA sehen den EA deshalb, wie schon angesprochen, in einer zentral stehenden Vermittlungsposition zwischen dem Antragsteller („Dienstleister“) und den zu beteiligenden Verwaltungen. Technisch erfolgt die Kenntnisnahme des EA darüber, dass ein Antrag erstellt wurde, dabei typischerweise so, dass der Antragsteller per Webbrowser Kontakt zum Web-Portal des EA aufnimmt und zwecks Authentifizierbarkeit ein Login mit Passwort beantragt und in der Regel zugeteilt bekommt, um den verbindlichen Beantragungsprozess in Gang setzen zu können. Typischerweise kann der Antragsteller nach einer erfolgten Authentisierung dann aus einer Liste das ihn interessierende Gewerbe auswählen. Ist das Gewerbe ausgewählt und bestätigt worden, dass ein Antragsverfahren gestartet werden soll, startet beim EA ein Verfahren bzw. ein Workflow, der allen Beteiligten (dem Antragsteller, dem EA selber, den unmittelbar beteiligten Verwaltungen, möglicherweise aber auch andere EA und Verwaltungen) bestimmte Rollen, Aufgaben und Fristen zuordnet und diese zueinander in ein ablauffähiges, für den EA kontrollierbares Verhältnis setzt.

Unter diesen Umständen ist eine Voraussetzung für eine datenschutzgerechte Umsetzung des EA, dass dessen Aufgaben festgelegt sind und geklärt ist, wo der EA organisatorisch angesiedelt ist. Erst dann können die Verantwortlichkeiten im Einzelnen, die erforderlichen Datentransporte, die technische Infrastruktur, der Schutzbedarf weitergereichter Daten und damit die notwendigen datenschutztechnischen Maßnahmen und Anforderungen formuliert und beurteilt werden.

Wird eine zuständige Behörde selbst als EA tätig, so verarbeitet der EA die personenbezogenen Daten für sich selbst (§ 3 Abs. 7 BDSG bzw. entsprechende landesgesetzliche Regelung), sodass ihr bzw. ihm die Rolle der Daten verarbeitenden Stelle zukommt. In der „Vermittlungsfunktion“ hingegen gestaltet sich die Beurteilung schwieriger. Für die Beantwortung der Frage, ob der EA dann Daten verarbeitende Stelle oder Auftragsdatenverarbeiter der zuständigen Behörden ist,

dürften die in Art. 7 Abs. 4 und Art. 11 Abs. 3 enthaltenen Regelungen maßgebend sein. In diesen Fällen kommt es auf Seiten des EA ggf. zu einer Speicherung personenbezogener Daten der Dienstleistungserbringer. Allerdings entscheidet der EA nicht über die „Mittel“ der Datenverarbeitung (Art. 2 d) der Richtlinie 95/46/EG). Auch eine Entscheidung über die „Zwecke“ der Datenverarbeitung ist fraglich, da die Speicherung eigentlich nur aus dem Grund erfolgt, die Zusammenarbeit mit den zuständigen Behörden zu optimieren. Eine Abwicklung soll, soweit der EA nicht zuständige Behörde ist, stets „über“ und nicht „durch“ den EA stattfinden. Eine Datenverarbeitung für eigene Zwecke entspricht in diesem Zusammenhang nicht der Vermittlungsposition des EA. Folgt man dieser Sichtweise, so würde der EA keine Daten verarbeitende Stelle sein.

Vor der Betriebsaufnahme eines EA muss der Betreiber dem Landesdatenschutzbeauftragten eine IT- und Sicherheitsdokumentation vorlegen sowie vielfach eine Vorabkontrolle durchlaufen. Die Ausgestaltung dieser Dokumentationen in Bezug auf mögliche Datenschutz-Risiken und Maßnahmen zu deren Verhinderung hängt davon ab, wie seitens des Gesetzgebers bzw. der Bundes- und Landesverwaltungsverfahrensgesetze die Aufgaben des EA zugeschnitten sind. Bezüglich des Aufgabenumfangs und der Zuständigkeit des EA stellt die DL-RL fest, dass die „Schaffung einheitlicher Ansprechpartner (…) nicht die Verteilung von Zuständigkeiten und Befugnissen zwischen Behörden innerhalb der nationalen Systeme“ berühre (vgl. Art. 6 Abs. 2 DL-RL). Diese Bestimmung ist dahingehend auszulegen, dass den zuständigen Behörden durch die Schaffung von EA keine bestehenden Zuständigkeiten genommen werden. Darüber hinausgehend kommt es auf der Ebene der Umsetzung darauf an, ob der EA mit eigenen Verantwortlichkeiten ausgestattet werden soll bzw. muss und somit zur Daten verarbeitenden Stelle wird. Einfach zugespitzt stellt sich die Frage, in welchem Maße es somit erforderlich werden könnte, dass ein EA Kenntnis von den inhaltlichen Daten nehmen muss, um seine zugedachten Funktionen der elektronisch zugänglichen, zentralen Anlaufstelle und des Verfahrensvermittlers erfüllen zu können. Im Rahmen der Umsetzung wäre in diesem Sinne beispielsweise zu prüfen, wie Stellung und Befugnisse des EA im Hinblick auf den Vorwarnmechanismus und die Informationen über die Zuverlässigkeit von Dienstleistungserbringern (Art. 32 und Art. 33 DL-RL) auszugestalten sind.

Generell gilt: Wenn der EA auf Inhalte zugreift - und somit grundsätzlich davon auszugehen ist, dass personenbezogene Daten mit höchstem Schutzbedarf zur Kenntnis gebracht werden - dann muss Datensicherheit und Datenschutz auf angemessenem Niveau technisch und organisatorisch gewährleistet sein. Die Sicherstellung von Authentizität und Integrität der Nachricht / des Dokuments durch Signaturen und der Vertraulichkeit durch Verschlüsselung sind Mechanismen, die zu einer tatsächlich umzusetzenden Ende-zu-Ende-Sicherheit beitragen können.[2] Eine qualifizierte Signaturerstellung erfordert den Einsatz einer sicheren Signaturerstellungseinheit, die – wie alle Mittel zur Erzeugung der Signatur - eindeutig unter der alleinigen Kontrolle des Nutzers steht (§2 Nr. 2 und 3 SigG), damit Authentizität und Verbindlichkeit der Nachricht bzw. des Dokuments nachgewiesen werden können. Es kommt hinzu, dass im europäischen Rahmen

[2] In WebServices und Portalen werden überwiegend oder sogar ausschließlich XML-Dokumente eingesetzt. Es gibt zwar je einen Standard für XML-Signaturen und –Verschlüsselung. Für eine Ausschreibung, und damit für den konkreten Einsatz dieser Techniken in der Verwaltung, sollten mindestens drei Anbieter von solchen Produkten mit einer Prüfung und Bestätigung oder einer Herstellererklärung nach SigG vorhanden sein. Für XML-Signaturen ist unklar, ob diese Voraussetzung derzeit oder absehbar gegeben ist. Hier besteht dringender Klärungs- bzw. Handlungsbedarf.

Interoperabilität von Zertifikaten bislang allenfalls für qualifizierte Signaturen gegeben ist. Dementsprechend sind gemäß § 23 SigG derzeit nur qualifizierte elektronische Signaturen und solche mit Anbieter-Akkreditierung aus dem EU-Ausland deutschen Signaturen gleichgestellt. Insofern kommt die Verwendung fortgeschrittener Signaturen nicht nur aus rechtlicher sondern auch aus technisch-funktionaler Sicht nicht infrage. Darüber hinaus ist eine Langzeitarchivierung von Dokumenten mit einer ausländischen Signatur sicherzustellen; die Projekte ARCHISIG und ARCHISAFE beschränken sich bisher auf deutsche Signaturen.

Viele andere Funktionen, die zu erbringen man in einigen Vorstellungen zum EA bislang ebenfalls dem EA zudenkt, ohne dass sich diese als Verpflichtung aus der DL-RL ableiten ließen, können sehr viel besser direkt auf dem PC des Antragstellers erbracht werden. Neben der angesprochenen unerlässlichen Ende-zu-Ende-Sicherheit in Bezug auf Authentizität, Vertraulichkeit und Integrität der Kommunikationsverbindungen, sollte auch die direkte Kommunikation zwischen dem Antragsteller und den Behörden, ohne Beteiligung des EA, unterstützt und die Nutzung eines Identitätsmanagers im Zusammenspiel mit einem Dokumentensafes auf dem Rechner des Antragstellers ermöglicht werden. Dies setzt voraus, dass der Antragsteller über eine hinreichend leistungsfähige und absicherungsfähige PC-Ausstattung verfügt.[3]

Wenn der EA mit seinen Aktivitäten inhaltlich selber keine die Beantragungsinhalte betreffende Entscheidungen zu treffen hat, sind zum Nachweis der Rechtmäßigkeit der getroffenen Entscheidungen an die Aktenführung keine hohen Ansprüche zu stellen. Hohe Anforderungen sind aber grundsätzlich an die Protokollierung der Abläufe, die der EA steuert und kontrolliert, zu stellen. Die zentrale Vermittlungsposition des EA wird absehbar dazu führen, dass dieser generell bei Konfliktfällen zwischen dem Antragsteller und den Verwaltungen vermittelnd involviert sein wird. So können Fragestellungen bezüglich der Fairness bei der Behandlung von Anträgen durch den EA oder zum Nachweis des spezifikationsgemäßen Funktionierens entstehen, wenn technische Fehlfunktionen in der gesamten Beantragungskette aufgetreten sind und der Fehler gesucht, die Ursache analysiert und festgestellt und die Verantwortung dafür zugeordnet werden muss. Zur Vermeidung bzw. rechtlichen Klärung solcher Konflikte müssen technische Vorkehrungen getroffen werden, um die einzelnen Aktionen und Abläufe sicher nachweisen zu können. Insofern empfiehlt es sich, hierfür auf eine dritte, unabhängige Stelle mit einer Notariatsfunktion oder zumindest einer zentralen Protokollierfunktion für alle Beteiligten zurückgreifen zu können.

Mit der im Rahmen der SOA-Architekturkonzeption anstehenden Umstellung der netzgestützten Kommunikationstechnik auf WebServices wird strategisch eine weitgehende Vollautomatisierung der Organisationsgrenzen übergreifenden Workflows angestrebt. Insofern sind grundsätzlich Zuordnungen bzgl. der Verantwortungsübernahmen durch die jeweiligen Daten verarbeitenden Stellen aufwändiger als bislang zu regeln. Denkbar wäre, eine Verantwortung jeweils für die

[3] Als technisch-operative Infrastruktur für die sichere Direktkommunikation zwischen dem Antragsteller und der Verwaltung, also ohne Vermittlung der Kommunikation durch den EAP, zeichnet sich die Nutzung von OSCI ab (vgl. http://www.osci.de/). In einem Video wird das Szenario eines Gründungsprozesses mit Hilfe eines EA sowie einem Client, der auf OSCI aufsetzt, plastisch durchgespielt, vgl. http://showroom.bos-bremen.de/web/szenario.html?videoid=126728. Dieses Szenario ließe sich dadurch konsequent vervollständigen, wenn wesentliche oder auch alle Bestandteile der Workflow-Anweisungen eines Beantragungsprozesses nicht auf dem EA sondern auf dem PC des Antragstellers abliefen. Der EA übernähme „nur“ die Überwachung der Aktivitäten und Prozesse (vgl. Rost, Martin, 2008: Das etwas andere Modell vom EA; in: Verwaltung & Management – Zeitschrift für allgemeine Verwaltung, 14. Jahrgang, Heft 4/2008, im Erscheinen).

Datenhaltung und für den Verfahrensablauf zu unterscheiden. Letzteres empfiehlt sich deshalb, weil für viele Betreiber und Verfahrensverantwortliche gar keine Möglichkeit besteht, Einfluss auf die Verfahren und deren Prozessgestaltung zu nehmen.

Die Funktionen von WebServices werden über Policies gesteuert. Zur Bereitstellung solcher Policies muss ein Policy-Server als eine Instanz vorgehalten werden, von der Server aktuelle und verbindliche (Sicherheits-)Regelwerke (z.B. „WS-Policy“, „WS-Security-Policy“) beziehen können. Es muss desweiteren eine Organisation damit beauftragt werden, derartige Policies den rechtlichen Anforderungen entsprechend verantwortlich zu erstellen und auf dem Policy-Server zur Verfügung zu stellen.[4] In diesem Zusammenhang empfiehlt es sich, Mechanismen des Qualitätsmanagements einzuführen. Der Sinn des Qualitätsmanagement besteht darin, Auftraggeber und Aufsichtsbehörden in die Lage zu versetzen überprüfen zu können, ob die technischen Betreiber der Systeme die rechtlich geforderten, vertraglich zugesagten und technisch spezifizierten Eigenschaften der Systeme tatsächlich einhalten. Die Systeme müssen dafür eigens vorgesehene Prüfmöglichkeiten anbieten, an denen der aktuelle Zustand von Verfahren bzw. Prozessen festgestellt werden kann. Anderenfalls können die Kontroll-Aufgaben (nicht nur) der Datenschutzbeauftragten in den einzelnen Verwaltungen sowie beim EA unter den neuen Bedingungen einer hochgetriebenen Automation der Verfahren einerseits sowie einer heterogenen, nicht-hierarchisch organisierten europaweiten Gesamtstruktur andererseits nicht erfüllt werden. Nicht korrekt betriebene Systeme verursachen unnötige Kosten und können vor allem zu einer Beeinträchtigung der Sicherheit einzelner Komponenten oder des gesamten Systems führen.

Die durch die Installation eines EA ausgelöste Standardisierung, Technisierung bzw. Automatisierung der Verwaltungstätigkeiten führt dazu, dass nicht nur die vom EA betreuten Aktivitäten, sondern auch die Aktivitäten in den Verwaltungsorganisationen sehr viel stärker und hochauflösender als bislang automatisiert beobachtet werden. Diese verbesserte Vermessung von Prozessen bedeutet einerseits, dass auch besser als bislang die Rechtmäßigkeit des Verwaltungshandelns nachweisbar werden kann. Das bedeutet andererseits aber auch, dass das Risiko hinsichtlich automatisierter Leistungs- und Verhaltenskontrollen drastisch zunehmen wird. Hier ist der Gesetzgeber aufgerufen, dringend die Rechtsgrundlagen des Mitarbeiter-Datenschutzes zu verbessern.

[4] Der Bezug dieser Policies muss seinerseits wiederum abgesichert, das heißt durch gegenseitige Authentisierung der beteiligten Instanzen und durch Sicherstellung der Integrität der transferierten Daten geschehen. Erste Schritte in diese Richtung werden im Rahmen des S.A.F.E-Projekts („Secure Access to Federated eGovernment/eJustice“) zur Realisierung des EGVP („Einheitliches Gerichts- und Verwaltungspostfach“) eingeschlagen.