Datenschutzgerechtes Workflow Management bei Mehrfachanträgen in ämterübergreifenden Verwaltungsprozessen

Stefan Audersch[1], Philip Laue[2]

[1] Abt. eGovernment & Multimedia
Information Management
Zentrum für Graphische
Datenverarbeitung e. V., Rostock
Joachim-Jungius-Str. 11
18059 Rostock
stefan.audersch@rostock.zgdv.de

[2] Projektgruppe verfassungs-
verträgliche Technikgestaltung
- provet -
Wilhelmshöher Allee 64-66
34119 Kassel
p.laue@uni-kassel.de

Abstract: Eine Möglichkeit effizientere und bürgerfreundlichere Verwaltungsanwendungen zu realisieren, besteht darin, einzelne auf einem identischen Lebenssachverhalt beruhende Genehmigungsverfahren in einem ämterübergreifenden Workflow zu bündeln. Der Beitrag stellt dazu ein Workflow-System vor, bei dem trotz eines ämterübergreifenden Datenumgangs durch ein auf Zugriffsrechte und Verschlüsselung basierendes Technikkonzept die Einhaltung des datenschutzrechtlichen Zweckbindungsgrundsatzes gewährleistet wird.

1 Einleitung

Ein typischer Kontakt zwischen Bürgern und Unternehmen mit der öffentlichen Verwaltung besteht in der Beantragung von Genehmigungen. Vielfach bedarf dabei der Betroffene trotz eines identischen Lebenssachverhalts gleichzeitig unterschiedlicher Bescheide verschiedener Fachbehörden. Obwohl eine Vielzahl von Einzeldaten, wie beispielsweise Name, Adresse oder Geburtsdatum für alle Verfahren identisch sind, ist der Antragssteller gezwungen, diese Angaben jeder Fachbehörde gesondert zu übermitteln. In der Regel sind mit solchen, für den Antragssteller lästigen, Mehrfachangaben auch zeitaufwändige Behördengänge verbunden. Im Rahmen des innerbehördlichen Verwaltungsablaufs werden anschließend zu jedem Antrag Stellungnahmen weiterer Fachbehörden eingeholt. Dabei sind aufgrund des einheitlichen Lebenssachverhalts sowohl die zu beteiligten Behörden als auch die von ihnen abgegeben Stellungnahmen in beiden Verfahren identisch, so dass es zu zeit- und kostenintensiven Doppelanfragen kommt.

Diese Problematik wurde bereits in den vergangenen Jahren von den öffentlichen Verwaltungsträgern erkannt. So wurden im Rahmen verschiedener E-Government-

Initiativen unterschiedliche Lebenslagenkonzepte entwickelt, um den Verwaltungsablauf bürgerfreundlicher, effektiver und kostengünstiger zu gestalten. Der folgende Beitrag stellt im Sinne dieser Bemühungen am Beispiel der Genehmigungsverfahren zur Durchführung einer Großveranstaltung einen weiteren Ansatz vor, wie durch eine optimierte Workflow-Steuerung unterschiedlicher Fachverfahren Effizienz und damit indirekt auch die Bürgerfreundlichkeit der öffentlichen Verwaltung gesteigert werden kann, ohne gleichzeitig datenschutzrechtliche Grundsätze zu unterlaufen. Grundlage für den Beitrag stellen dabei die Arbeiten im Rahmen des VESUV-Projekts[1] dar. Dem dort entwickelten Anwendungsszenario "Event-Management" liegt die Idee zugrunde, in der Hansestadt Rostock[2] ein zentrales Dienstleistungsbüro "Veranstaltungen" einzurichten.

2 Darstellung des „Ist-Zustandes“ am Beispiel der Genehmigung einer Großveranstaltung

Im Folgenden wird anhand des Genehmigungsverfahrens zur Durchführung einer Großveranstaltung die aufgezeigte Problematik der mehrfachen Antragstellung beispielhaft dargestellt.

2.1 Aus rechtlicher Sicht

Um eine Großveranstaltung wie beispielsweise eine Messe oder einen Markt durchführen zu können, sind in der Regel zwei verschiedene Genehmigungen notwendig. Soweit die Veranstaltung auf öffentlichen Flächen stattfinden soll, ist dafür eine Sondernutzungsgenehmigung nach den jeweiligen straßen- und wegerechtlichen Regelungen des Bundes und der Länder notwendig. Aus gewerberechtlicher Sicht bedarf es eines Bescheids über die Festsetzung der Veranstaltung.[3] Für beiden Verfahren sind grundsätzlich verschiedene Fachämter der jeweiligen Kommune sachlich zuständig. Für die Sondernutzungserlaubnis ist dies in der Regel das Ordnungsamt, Straßenverkehrsamt oder Tiefbauamt und für den gewerblichen Festsetzungsbescheid das Gewerbeamt. Der Antragsteller muss daher bei der jeweils zuständigen Behörde sowohl einen Antrag auf Festsetzung als auch auf Sondernutzung stellen. Auch wenn beiden Anträgen der gleiche Sachverhalt – Durchführung einer Großveranstaltung durch den Antragsteller an einem bestimmten Ort – zu Grunde liegt, sind beide Genehmigungsverfahren rechtlich voneinander unabhängig. Die Erteilung der Sondernutzungserlaubnis ergeht unabhängig von der gewerberechtlichen Festsetzung der Veranstaltung.

Im Rahmen beider Verfahren werden im Wesentlichen von den gleichen Fachbehörden – wie beispielsweise vom Grünamt oder vom Brandschutz- und Rettungsamt –

[1] Verteilte Software-Agenten für sichere, rechtsverbindliche Aufgabendelegation in mobilen kollaborativen Anwendungen (VESUVI), www.vesuv-projekt.de.
[2] www.rostock.de
[3] §§ 64 ff. GewO.

Stellungnahmen eingeholt. Ebenso sind eine Vielzahl personenbezogener Daten, wie Name, Anschrift oder Geburtsdatum des Veranstalters, für beide Verfahren von Relevanz. Bestimmte Daten sind allerdings nur für eines der beiden Verwaltungsverfahren von Bedeutung. So findet nur im Rahmen des gewerberechtlichen Festsetzungsverfahrens eine Prüfung statt, ob der Antragssteller die zur Durchführung der Veranstaltung notwendige Zuverlässigkeit besitzt.[4] Im Rahmen des ebenfalls durchzuführenden Sondernutzungsverfahrens stellt die Frage der Zuverlässigkeit des Antragsstellers dagegen keine Genehmigungsvoraussetzung dar.

2.2 Aus technischer Sicht

Die Bearbeitung der verschiedenen Verwaltungsprozesse innerhalb der Fachbehörden erfolgt bereits heute vielfach auf der Basis von IuK-Technologien. Nachdem die Anträge vom Antragsteller überwiegend händisch ausgefüllt wurden, werden die Daten vom Sachbearbeiter des jeweils zuständigen Fachamts in das zumeist proprietäre Fachverfahren eingepflegt. Dort werden sie mittels unterschiedlicher Vorgangsbearbeitungssystemen wie beispielsweise fachamtsspezifischer Workflow Management-Systeme oder E-Mail-Routinen weiterverarbeitet. Soweit für die Bearbeitung eine ämterübergreifende Kommunikation notwendig ist, erfolgt diese derzeit auf dem herkömmlichen Postweg, auf der Basis von Telefongesprächen oder mittels Fax und E-Mail.

3 Datenschutzrechtliche Anforderungen an eine optimierte Vorgangsbearbeitung

Werden unterschiedliche Fachverfahren in einem Vorgangsbearbeitungssystem miteinander verbunden, so muss ein damit verbundener Umgang mit personenbezogenen Daten so ausgestaltet sein, dass er nicht in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eingreift. Danach hat der einzelne das Recht, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.[5]

Ausfluss des informationellen Selbstbestimmungsrechts ist ein striktes, an die datenverarbeitende Stelle adressiertes, Zweckbindungsgebot [TE98, Yi04]. Danach darf der durch Einwilligung oder gesetzlichen Erlaubnistatbestand festgelegte konkrete Zweck von der datenverarbeitenden Stelle nicht auf weitere oder andere Datenverwendungen ausgeweitet werden. Jede Überschreitung des zugewiesenen Aufgabenbereichs stellt dann eine Zweckänderung oder Zweckentfremdung und damit einen erneuten Eingriff in das Recht auf informationelle Selbstbestimmung dar [RPG01, Yi04]. Bei der Zweckbindung handelt es sich nicht nur um einen Nebenzweck

[4] S. § 69a Abs. 1 Nr. 2 GewO.
[5] BVerfGE 65, 1, 42f.

datenschutzrechtlicher Regelungen, sondern bildet das zentrale Element des Datenschutzrechts [Bu99, Ku99, Ze03].

Um den Betroffen wirksam vor unzulässigen Zweckänderungen oder Zweckentfremdungen zu schützen, ist sowohl durch Weitergabe- und Verwertungsverbote als auch durch organisatorische Vorkehrungen sicherzustellen, dass die vorgesehene Zweckbindung garantiert wird. In der öffentlichen Verwaltung wird ein solcher Schutz durch eine „informationelle Gewaltenteilung“ realisiert. Danach darf jede Stelle nur die für ihre Aufgabenerfüllung erforderlichen Daten sammeln und nutzen [RPG01]. Dabei bildet der Staat keine Informationseinheit, sondern es ist zwischen den verschiedenen Aufgabenbereichen des Staates zu unterscheiden [He87]. Zur Abgrenzung der einzelnen Aufgabenbereiche wird ein „funktionaler Behördenbegriff“ zugrunde gelegt. Die Organisation der staatlichen Verwaltung muss so gestaltet sein, dass eine Kenntnisnahme der Daten durch unzuständige Fachbehörden ausgeschlossen ist [Tu96, TE98]. Datenverarbeitende Stelle ist damit nicht die Gemeinde als organisatorische Einheit, sondern, bezogen auf den jeweiligen Zweck, das zuständige Fachamt. Die Gemeinde wird damit in einzelne, den jeweiligen Aufgaben entsprechende, in sich geschlossene und voneinander abgeschottete Teile aufgespalten [Si86].

Die dargestellten Grundsätze haben Auswirkungen auf die datenschutzgerechte Ausgestaltung einer optimierten Vorgangsbearbeitung. Soweit dort verschiedene Fachverfahren miteinander gekoppelt werden, sind nach dem „funktionalen Behördenbegriff“ unterschiedliche datenverarbeitende Stellen mit einem jeweils eigenen Aufgabenbereich beteiligt. Zur Erfüllung ihrer Aufgaben bedürfen sie zum Teil unterschiedlicher personenbezogener Daten des Antragsstellers. So dürfen Daten, die Rückschlüsse auf die Zuverlässigkeit des Antragsstellers zulassen, nur im gewerberechtlichen, nicht jedoch im Sondernutzungsverfahren genutzt werden. Entsprechend ist in einem optimierten Workflow zu berücksichtigen, dass

- die Daten beider Verfahren nur von der Stelle verarbeitet und genutzt werden dürfen, in deren Aufgabenbereich der Datenumgang fällt.

- technisch-organisatorische Vorkehrungen getroffen werden, die eine Zweckänderung oder Zweckentfremdung ausschließen.

Ein technisches System zur optimierten Vorgangsbearbeitung bedarf daher zum einen eines wirksamen Zugriffsschutzes, um einen zweckgebundenen Datenumgang sicherzustellen. Zum anderen ist aber auch festzuhalten, dass jede Lösung einer einheitlichen Datenhaltung, die diese datenschutzrechtlichen Anforderungen nicht berücksichtigt, unzulässig ist.

4 Realisierungsansätze

Um den Verfahrensablauf bei Mehfachanträgen im Rahmen ämterübergreifender Verwaltungsprozesse zu optimieren, ist eine Vernetzung der verschiedenen

Fachverfahren unerlässlich. Proprietäre Systementwicklungen für das einzelne Fachamt haben sich aufgrund einer damit verbundenen dezentralen Datenhaltung zwar als datenschutzkonform, zugleich aber auch als zu ineffektiv und kostspielig erwiesen. Dagegen vermag eine gemeinsame Vorgangsbearbeitung innerhalb eines Vorgangsbearbeitungssystems zwar zu einer kostengünstigeren und effizienteren Verwaltungsorganisation beitragen. Sie ist aber ohne weitere Schutzvorkehrungen aufgrund der mit ihr verbundenen gemeinsamen Datenhaltung, mit dem Grundsatz der „informationellen Gewaltenteilung“ nicht zu vereinbaren. Herkömmliche Methoden der Verschlüsselung zur Sicherung des Zugriffsschutzes bei einer gemeinsamen Vorgangsbearbeitung von Mehrfachanträgen stellen zwar gegebenenfalls sicher, dass nur die jeweils berechtigte Stelle Zugriff auf die Daten erlangt. Sie erweisen sich jedoch insbesondere dann als unflexibel, wenn unterschiedliche Nutzer in einem gemeinsamen Datenbestand auf unterschiedliche Daten Zugriff erhalten sollen, wie dies in dem dargestellten Beispiel der Sondernutzungs- und Gewerbeverfahren im Rahmen des Genehmigungsverfahrens zur Durchführung einer Großveranstaltung der Fall ist.

Ziel muss es daher sein, eine flexible ämterübergreifende Vorgangsbearbeitung zu ermöglichen, ohne dabei gegen datenschutzrechtliche Grundsätze zu verstoßen. Im Folgenden wird dazu ein, Realisierungsansatz vorgestellt, der im Rahmen des VESUV-Projekts entwickelt wurde.

4.1 Technische Beschreibung

Ausgangspunkt für das VESUV-Framework bilden Technologien aus den Bereichen Semantic Web, Web Services und Workflow Management. Zur Integration von Fachverfahren und zur Dienstekomposition werden semantische Informationen genutzt und juristische Regelmodelle ontologiebasiert in die Vorgangssteuerung integriert [AFS06]. Zudem erlauben semantische Informationen eine wissensbasierte Assistenzunterstützung für den Sachbearbeiter innerhalb manuell zu bearbeitender Entscheidungsprozesse.

Die VESUV-Systemarchitektur basiert auf der eFormsDirect-Frameworkarchitektur [ACF03, Fr05], welche um zusätzliche Komponenten erweitert wurde. Einen Überblick über die Systemarchitektur liefert die Abbildung 1.

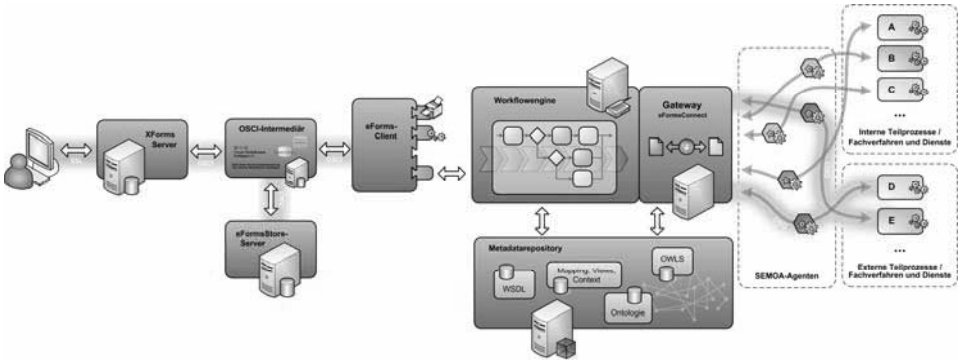

Abbildung 1: VESUV-Systemarchitektur

Bei der Workflowengine handelt es sich um die Open Source Engine ActiveBPEL[6]. Für diese wurden die zwei spezifizierten Workflows (Sondernutzung und Festsetzung) in der Sprache BPEL4WS[7] [AC+03] umgesetzt. Grundlage für die Datenkommunikation im System ist XML. Das Verfahren der mehrfachen Antragstellung bei identischem Lebenssachverhalts wird dabei dahingehend optimiert, dass die Angaben aus den beiden zuvor separaten Anträgen (Antrag auf Sondernutzung und Antrag auf Festsetzung) in einem Dokument erfolgen. Dadurch werden dem Bürger unnötige Doppeleingaben erspart. Das bei der Erstellung des Antrages durch den Antragsteller erzeugte XML-Dokument wird anschließend auf der Basis von OSCI-Technologie[8] an die Behörde übermittelt. Die Bearbeitung des eigentlichen Verwaltungsprozesses erfolgt anschließend in der Workflowengine sowie in den angebundenen Fachverfahren.

Grundlage für die Datenkommunikation im System ist XML. Das bei der Erstellung des Antrages durch den Antragsteller erzeugte XML-Dokument beruht dabei auf einer für das Eventmanagment entwickelten XML-Struktur, die an die Entwicklungen der OSCI-XÖV-Standards angepasst ist. Die OSCI-XÖV-Standards stellen den Teil B der OSCI-Spezifikation dar und beinhalten verschiedene standardisierte Definitionen von Datenstrukturen für verschiedene Anwendungsbereiche im eGovernment. Die Standards XMeld (Meldewesen) und XGewerbe (Gewerbewesen) bilden die Grundlage zur Definition der XML-Dokumente für das Eventmanagement.

Ausgehend von der Feststellung, welche Daten aus den beiden Fachverfahren an welche der unterschiedlichen, am jeweiligen Fachverfahren beteiligten Fachämter zu übermitteln sind, lassen sich die Daten aus dem XML-Dokument in kleinste gemeinsame Teile zusammenfassen. Dabei werden die Daten aus dem XML-Dokument so aufbereitet, dass sowohl diejenigen Daten ermittelt werden, die eine Fachbehörde für beide Fachverfahren benötigt, als auch diejenigen Teile des XML-Dokuments identifiziert werden, die nur für eines der Fachverfahren von Relevanz ist. So wird

[6] www.activebpel.org.
[7] Business Process Execution Language for Web Services.
[8] Online Service Computer Interface (www.osci.de).

beispielsweise das Grünamt für beide Verfahren um eine Stellungnahme gebeten und benötigt dafür identische Angaben. Dagegen sind Angaben zur Zuverlässigkeit des Antragsstellers nur bei der Entscheidung über die gewerberechtliche Festsetzung der Veranstaltung zu berücksichtigen. Die so gebildeten kleinsten gemeinsamen Teile werden zur weiteren Bearbeitung an die jeweiligen Fachämter übermittelt und tragen damit zu einer Optimierung der Ablauforganisation bei.

Der notwendige Zugriffschutz auf die für die jeweiligen Fachämter bestimmten Teile erfolgt durch ein angepasstes Verschlüsselungsverfahren. Die für die Kommunikation innerhalb des Systems verwendeten XML-Dokumente werden dabei für die verschiedenen Empfänger unterschiedlich verschlüsselt und signiert. Grundlage hierfür bieten die Technologien XML-Signature [XS02] und XML-Encryption [XE02]. Im VESUV-Framework lassen sich diese durch spezielle Module bzw. Layer umsetzen und somit in die jeweiligen Teilprozesse integrieren (siehe Abbildung 2).

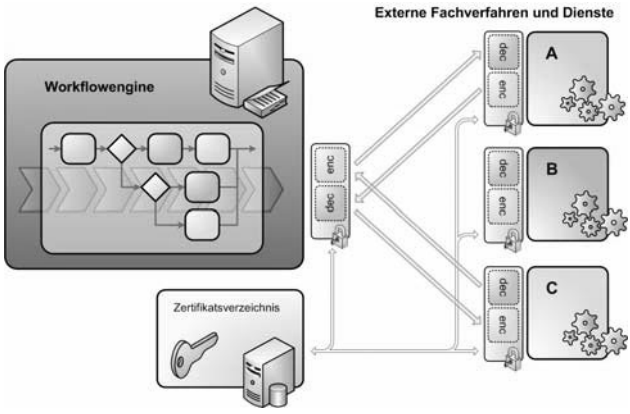

Abbildung 2: Nutzung von Layern für die Verschlüsselung und Zertifizierung

Die Abbildung 3 zeigt den Ansatz für die Verschlüsselung der im System verwendeten Dokumente. Danach werden für die Verschlüsselung bzw. Signatur zunächst die einzelnen Teile einzeln signiert und verschlüsselt. Anschließend wird das Dokument für den Versand an die verschiedenen Empfänger noch einmal komplett übersigniert. Bei der Verschlüsselung kommen dabei sowohl symmetrische als auch asymmetrische Verfahren zum Einsatz. Mit dem symmetrischen Schlüssel werden die einzelnen Teile separat verschlüsselt. Hierbei wird für jedes Teil ein neuer Schlüssel erzeugt. Mit Hilfe der asymmetrischen Schlüssel (Public Key) der einzelnen Empfänger werden diese symmetrischen Schlüssel anschließend für die einzelnen Empfänger nochmals gesondert verschlüsselt. Somit kann beim Empfang eines Dokumentes nur der berechtigte Empfänger mit seinem privaten, asymmetrischen Schlüssel die entsprechenden symmetrischen Schlüssel ermitteln und daraufhin den für ihn notwendigen Inhalt des Dokumentes entschlüsseln.

Abbildung 3: Verschlüsselung der XML-Dokumente

Sind einzelne Dokumententeile für verschiedene Empfänger von Relevanz, so ist es für die Verschlüsselung notwendig zu wissen, welche Elemente für welchen Empfänger bestimmt sind. Ein Lösungsansatz könnte dabei die Nutzung der verschiedenen ontologischen Informationen (Datenstrukturen, Verwaltungsstruktur, Verwaltungsaufgaben) sowie die Nutzung der Workflowbeschreibung darstellen. Speziell die Verknüpfung von Aufgabenverteilung und Beschreibung der Datenstruktur beinhalten bereits indirekt, welche Dokumentteile für welche Empfänger notwendig und zweckgebunden sind.

Ein konkreter Lösungsansatz wird, ebenso wie das entsprechende Schlüsselmanagement, derzeit im Rahmen der Projektarbeit weiter analysiert und fortentwickelt. Dabei wird der Fokus der Forschungsarbeit insbesondere auch auf die Problematik gelegt, wo die Zerlegung der Teilabschnitte, die Schlüsselerzeugung und die (Teil)verschlüsselung erfolgen sollte. Grundsätzlich denkbar wäre hier zum einen eine Client-seitige Zerlegung und Verschlüsselung. Dies würde unter Umständen jedoch weitere spezielle Softwareinstallationen auf Bürger- oder Unternehmensseite zur Kommunikation mit der Verwaltung erforderlich machen, welche stets das Risiko mangelnder Akzeptanz beim Anwender in sich bergen. Zum anderen ist eine Server-basierte Zerlegung und Verschlüsselung denkbar. So könnte beispielsweise die OSCI-Poststelle um eine entsprechende Komponente erweitert werden, die eine entsprechende Aufbereitung des Antrags noch vor der Einspeisung in den gemeinsamen Workflow vornimmt. Dies würde jedoch dazu führen, dass zumindest der Server der Poststelle bei dem der gemeinsame Antrag eingereicht wird, alle Daten zur Kenntnis bekommt.

Berücksichtigung bei der Entwicklung findet die Spezifikation "Web Services Policy 1.2

- Framework (WS-Policy)" des W3C [WS06]. Durch die Definition eines WS-Policy-Dokumentes (welche Teile müssen wie und für welche Empfänger verschlüsselt werden) lässt sich die Verschlüsselung auf dessen Basis innerhalb der Webservice-Architektur automatisieren.

4.2 Rechtliche Beurteilung

Ein datenschutzrechtlicher Schutz vor Zweckänderungen und Zweckentfremdung wurde bislang durch eine räumliche Datenaufteilung gewährleistet, indem die Papierakten in den Räumlichkeiten der jeweils sachlich zuständigen Fachbehörde verwahrt wurden. Im Zuge der technischen Entwicklungen wurden die Daten daneben auch auf den Servern der jeweiligen Fachbehörden vorgehalten. Häufig ging die physische Datenaufteilung mit der Entwicklung proprietärer Fachverfahren einher, die einen Datenaustausch zusätzlich erschwerten. Durch die Architektur des optimierten Workflows wird der datenschutzrechtliche Zweckbindungsgrundsatz nicht durch dezentrale Aufbewahrungs- und Verarbeitungsmechanismen, sondern durch ein auf Zugriffsrechte und Verschlüsselung basierendes Technikkonzept gewährleistet. Indem die Daten, angepasst an das jeweilige Fachverfahren, in Teile zusammengefasst und mit den öffentlichen Schlüsseln derjenigen Fachämter verschlüsselt werden, die im weiteren Verfahren auf die Daten zugreifen müssen, wird sichergestellt, dass das jeweilige Fachamt nur auf die Daten Zugriff erhält, deren Kenntnis zur Erledigung seiner Aufgaben erforderlich ist. Gleichzeitig wird mit diesem auf den jeweiligen Verwendungskontext angepassten Zugriffschutz die Möglichkeit eröffnet, personenbezogene Daten auch in ämterübergreifenden Workflows zu bearbeiten, ohne durch eine dadurch bedingte Datensammlung gegen das Gebot der „informationellen Gewaltenteilung“ zu verstoßen. Die herkömmliche Form des dezentralen Datenumgangs aufgrund proprietärer Fachverfahren lässt sich so in datenschutzkonformer Weise durch effizientere Methoden der ämterübergreifenden Vorgangsbearbeitung ergänzen. Dass Daten, die für beide Verfahren von Relevanz sind, für notwendige Stellungnahmen gemeinsam an weitere Fachämter übermittelt werden und von diesen einsehbar sind, stellt ebenfalls keinen Verstoß gegen den Zweckbindungsgrundsatz dar. Der Datenumgang für mehrere Zwecke und damit eine gemeinsame Datenübermittlung ist vom Grundsatz der Zweckbindung nicht ausgeschlossen.[9]

5 Zusammenfassung

Ein für ämterübergreifende Prozesse optimierter Workflow ermöglicht eine synchrone Nutzung der Daten unterschiedlicher Fachverfahren, vermeidet damit unnötige Doppeleingaben, bündelt Informationen und übermittelt sie zur gemeinsamen Bearbeitung an Drittbehörden. Trotz des damit verbundenen ämterübergreifenden

[9] BVerfGE 65, 1 (61 ff.).

Datenumgangs wird durch einen XML-basierten, an die jeweilige Fachbehörde angepassten, Zugriffsschutz die Einhaltung des datenschutzrechtlichen Zweckbindungsgrundsatzes gewährleistet. So wird sowohl das Ziel eines bürgerfreundlichen und zugleich effektiven sowie kostengünstigen Verfahrensablaufs verwirklicht als auch der Grundsatz der „informationellen Gewaltenteilung“ gestärkt.

Literaturverzeichnis

[AC+03] Andrews, T.; Curbera, F.; Dholakia, H.; Goland, Y.; Klein, J.; Leymann, F.; Liu, K.; Roller, D.; Smith, D.; Thatte, S.; Trickovic, I.; Weerawarana, S.: Business Process Execution Language for Web Services Version 1.1, 2003.

[ACF03] Audersch, S.; Courvoisier, T.; Flach, G.: eFormsDirect – XML-basiertes E-Government-Framework für intelligente Formulare auf der Basis von XForms. In: XMIDX Workshop, Berlin, 2003.

[AFS06] Audersch, S.; Flach, G.; Schulz, J.: Semantikbasierte eGovernment-Dienste für komplexe, ämterübergreifende Verwaltungsprozesse. Eingereicht zu: Berliner XML-Tage (XMLT), Berlin 2006.

[Bu99] Bull, H. P.: Aus aktuellem Anlaß: Bemerkungen über Stil und Technik der Datenschutzgesetzgebung, RDV 1999, 148.

[Fr05] Franz, A.: Semantik-gestützte Workflow-Steuerung und Dienste-Komposition in organisationsübergreifenden eGovernment-Umgebungen. Diplomarbeit, Universität Rostock, 2005.

[He87] Heußner, H.: Zur Zweckbindung und zur informationellen Gewaltenteilung in der Rechtsprechung des Bundesverfassungsgerichts. In (Brandt, W.; Gollwitzer, H.; Henschel, J. F., Hrsg.): Ein Richter, ein Bürger, ein Christ: Festschrift für Helmut Simon, Nomos-Verlag, Baden-Baden, 1987.

[Ku99] Kutscha, M.: Datenschutz durch Zweckbindung – ein Auslaufmodell?, ZRP 1999, 156.

[RPG01] Roßnagel, A.; Pfitzmann, A.; Garstka, H.-J.: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des BMI, 2001.

[Si86] Simitis, S.: Von der Amtshilfe zur Informationshilfe – Informationsaustausch und Datenschutzanforderungen in der öffentlichen Verwaltung, NJW 1986, 2795.

[TE98] Tinnefeld, M.-T.; Ehmann, E.: Einführung in das Datenschutzrecht. R. Oldenbourg Verlag, München Wien, 1998.

[Tu96] Tuner, L.: Zur Notwendigkeit einer Entflechtung von Amtshilfe und Datenschutz, CR 1996, 591.

[WS06] Web Services Policy 1.2 - Framework (WS-Policy). W3C Member Submission 25 April 2006. *http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/*

[XE02] XML Encryption Syntax and Processing. W3C Recommendation 10 December 2002. *http://www.w3.org/TR/xmlenc-core/*

[XS02] XML-Signature Syntax and Processing. W3C Recommendation 12 February 2002. *http://www.w3.org/TR/xmldsig-core/*

[Yi04] Yildirim, N.: Datenschutz im Electronic Government. Deutscher Universitäts-Verlag, Wiesbaden, 2004.

[Ze01] v. Zezschwitz, F.: Konzept der normativen Zweckbegrenzung. In (Roßnagel, A., Hrsg.): Handbuch Datenschutzrecht, München, 2003.