Datenschutzfragen bei der Etablierung einer Arbeitsprozess-integrierten e-Learning-Lösung

Andreas Zinnen[1], Sybille Hambach[2],Andreas Faatz[1], Stefanie Lindstaedt[3,4], Günter Beham[3,4,] Eicke Godehard[1], Manuel Goertz[1], Robert Lokaiczyk[1]

[1]SAP Research CEC Darmstadt
Bleichstr. 8
64283 Darmstadt, Germany
{andreas.zinnen, andreas.faatz, eicke.godehardt, manuel.goertz, robert.lokaiczyk}@sap.com

[2]Fraunhofer Institute for Computer Graphics Rostock
Joachim-Jungius-Str. 11
18059 Rostock, Germany
sybille.hambach@igd-r.fraunhofer.de

[3]Know-Center
Inffeldgasse 21a
8010 Graz, Austria
{slind, gbeham}@know-center.at

[4]Technische Universität Graz (Institut für Wissensmanagement)
Inffeldgasse 21a
8010 Graz, Austria

Abstract: Heutige Forschungsprojekte im e-Learning-Umfeld vernachlässigen zu oft den Bezug zum Datenschutz und werfen damit Fragen des ethischen Forschens auf. Das vorliegende Papier analysiert Datenschutzfragen bei der Etablierung eines sozio-technischen Systems im Umfeld kleiner und mittlerer Unternehmen (KMU). Wir beziehen uns auf das Beispiel eines noch prototypischen e-Learning-Systems. Dieses liefert dem Mitarbeiter eines KMU wissensintensive Medienartefakte, die zu den aktuellen Arbeitsaufgaben passen. Um diese Artefakte auswählen zu können, speichert und verwaltet das System kritische Daten wie die Kompetenzen der Benutzer, die bisher ausgeführten Arbeitsschritte, bisher ausgeführte Interaktionen mit Medienartefakten oder anderen Benutzern, die sich im System manifestieren. Wir zeigen, wie ein solches Daten verarbeitendes System die OECD-Datenschutzrichtlinie mit ihren Grundprinzipien Bekanntmachung, Zweckerklärung und -bindung, Zustimmung, Sicherheit, Auskunftspflicht, Zugang sowie Haftung berücksichtigen kann.

1 Einleitung

Wir beobachten gegenwärtig ein Spannungsfeld durch mangelnde Berücksichtigung von Datenschutzfragen in der Entwurfsphase von sozio-technischen Systemen. Dieses Spannungsfeld entsteht, wenn Daten gesammelt, gespeichert und verarbeitet werden. Die Erwartungshaltung an den Schutz solcher Daten steigt mit der systemabhängigen Möglichkeit, die Einträge der entstehenden Datensammlung den Individuen oder eindeutig definierten Gruppen zuordnen zu können. Die unangemessene oder für den Nutzer nicht vorhandene Auskunft des Systems oder der Systembetreiber zur Datensammlung, -speicherung und -verarbeitung sind hier oftmals Ursache für Schwierigkeiten im Zusammenhang mit dem Datenschutz.

Als Entwickler komplexer e-Learning-Systeme stehen wir also vor der Herausforderung, sowohl den Schutz als auch die Verwendung von Daten in sozio-technischen Systemen adäquat zu gewährleisten. Die Empfehlung der OECD [OECD] sowie die EU-Richtlinien 95/46/EC [EU04] und 2002/58/EC [EU02] beschreiben die Prinzipien Bekanntmachung, Zweckerklärung und -bindung, Zustimmung, Sicherheit, Auskunftspflicht, Zugang sowie Haftung. Sie müssen vor der Inbetriebnahme eines Systems in einem Unternehmen gewährleistet sein.

Das vorliegende Papier spezifiziert Aspekte speziell für e-Learning-Systeme im Unternehmensumfeld, geht von den genannten Richtlinien aus und zeigt den Abstimmungsbedarf mit Organisationseinheiten wie Betriebsrat, Rechtsabteilung und unternehmensinternen Datenschutzbeauftragten. Am Beispiel des arbeitsprozess-integrierten e-Learning-Systems APOSDLE werden die einzelnen Richtlinien reflektiert und Umsetzungsmöglichkeiten aufgezeigt.

Das Ziel eines unternehmensinternen e-Learning-Systems wie APOSDLE, das dem Benutzer Lern-Ressourcen ad hoc entsprechend seinen Arbeitsaufgaben und Kompetenzen zur Verfügung stellt, liegt in der Erhöhung der Arbeitsproduktivität. Dies geschieht durch die Einbeziehung der alltäglichen Arbeitsprozesse und des gegebenen Arbeitsumfelds, nach Möglichkeit nahtlos und unter Berücksichtigung aller Rollen, die ein Wissensarbeiter in einem solchen Szenario einnehmen kann [LI06]. Ein solches System macht es zwingend erforderlich, kritische Daten wie etwa Kompetenzen der Benutzer, die von ihnen ausgeführten Arbeitsschritte, und ihre Interaktionen mit anderen Benutzern des Systems zu speichern und zu verarbeiten. Solche Daten könnten beispielsweise bei einer innerbetrieblich nicht abgestimmten Leistungsmessung missbraucht werden

Wir haben drei Dimensionen des Datenschutzes in sozio-technischen Systemen identifiziert (Abbildung 1) und werden im Folgenden die technische und die rechtliche Dimension anhand des e-Learning-Systems APOSDLE exemplarisch behandeln.

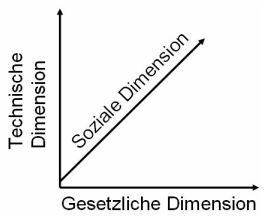

Abbildung 1 Drei Dimensionen des Datenschutzes

Das Papier gliedert sich wie folgt. Abschnitt 2 liefert eine Zusammenfassung der Datenschutzgrundlagen in der Europäischen Union, wo die Direktive 95/46/EC die Basis der Datenschutzgesetze darstellt. Abschnitt 3 stellt die Grundprinzipien des Datenschutzes in deutschen Unternehmen dar und bezieht die Instanzen Betriebsrat, Rechtsabteilung und Datenschutzbeauftragte mit ein. Abschnitt 4 zeigt die Grundfunktionalitäten eines Arbeitsprozess-integrierten e-Learning-Systems auf. Für ein solches System wird Abschnitt 5 schließlich Aspekte zum Datenschutz herleiten und technische Details bei der Umsetzung ihrer Entwurfselemente erläutern.

2 Datenschutz in der Europäischen Union

Die allgemeine Erklärung der Menschenrechte legt sich in §12 [UR84] auf folgende Formulierung fest:

"Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen."

Alle Mitgliedsstaaten der Europäischen Union haben die europäische Menschenrechtskonvention (ECHR) [ECHR] unterzeichnet. Mit dieser hohen Wertschätzung der Menschenrechte in Europa geht die Tatsache einher, dass der Schutz des Privatlebens ein hier hoch entwickeltes Rechtsgebiet darstellt. Artikel 8 der ECHR gewährt Personen grundsätzlich "das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz", wobei in Ausnahmefällen bestimmte Einschränkungen und Interpretationsspielräume möglich sind und auch vom Europäischen Gerichtshof angewandt werden.

1980 hat die OECD den ersten Versuch unternommen, den Schutz von Privatpersonen (dort als Datensubjekte bezeichnet) in den „Empfehlungen des Rates zu Richtlinien, die den Schutz der Privatsphäre und den grenzübergreifenden Fluss persönlicher Daten gewährleisten" genauer zu spezifizieren. Die Grundprinzipien dieser Initiative [OECD] sind:

- Bekanntmachung ("notice"): Datensubjekte sollten davon in Kenntnis gesetzt werden, wenn ihre Daten gesammelt werden.

- Zweckerklärung und -bindung ("purpose"): Daten sollten nur für einen ausdrücklich angegebenen Zweck und nicht darüber hinaus verwendet werden.

- Zustimmung ("consent"): Daten sollten nur mit ausdrücklicher Zustimmung des Datensubjektes weitergegeben werden.

- Sicherheit ("security"): Daten sollten vor allen Formen potenziellen Missbrauchs abgesichert werden.

- Auskunftspflicht ("disclosure"): Datensubjekte sollten darüber informiert werden, wer ihre Daten sammelt.

- Zugang ("access"): Datensubjekte sollten Zugriff auf ihre Daten haben und damit verbunden die Möglichkeit, die Daten zu korrigieren.

- Haftung ("accountability"): Datensubjekte sollten die Möglichkeit haben, die Sammler der Daten für die obigen Prinzipien haftbar zu machen.

Da die OECD-Richtlinien nicht bindend waren, wichen die Datenschutzgesetzte in Europa stark voneinander ab. Die Europäische Kommission entschied sich zur Vereinheitlichung und erließ 1998 die Richtlinie 95/46/EC. Diese definiert in § 2a persönliche ("personenbezogene") Daten als "alle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Nach diesem sehr weitgreifenden Verständnis handelt es sich auch dann um persönliche Daten, wenn Informationen durch wie auch immer geartete Verfahren mit einer Person verknüpft werden, die Person selbst über eine solche Verknüpfung aber nicht verfügt und auch nicht in der Lage wäre, die Verknüpfung herzustellen. Einige Beispiele persönlicher Daten sind das Geburtsdatum, die Adresse, Kreditkartennummer, polizeiliche Führungszeugnisse und vieles mehr. Beispiele für die angesprochenen Verknüpfungen wären die einer Kreditkartennummer zugeordneten Einkäufe, die eine Person tätigt.

Der Begriff "Verarbeitung", der in der Richtlinie 95/46/EC gebraucht wird, bezeichnet "jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten".

Die Verantwortung für eine Verarbeitung personenbezogener Daten, die die Privatsphäre respektiert, liegt nach der Richtlinie bei der "Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet" (§2b). Diese Verantwortung existiert nach §4 auch dann, wenn die Verarbeitung durch nicht in der EU Ansässige, aber physikalisch (zum Beispiel durch Geräte) innerhalb der EU stattfindet.

Persönliche Daten sollten überhaupt nicht verarbeitet werden, Ausnahmen sind entlang der folgenden drei Kategorien organisiert:

- Transparenz: Das Datensubjekt hat das Recht auf Information über die Erhebung seiner persönlichen Daten. Der für die Verarbeitung Verantwortliche muss nach §10 und 11 seine Kontaktdaten, den Zweck der Verarbeitung, die Empfänger des Verarbeitungsresultats und alle anderen Angaben, die ein faires Verfahren sicherstellen, liefern. Die Verarbeitung ist möglich, wenn eine der nachfolgenden Bedingungen gilt:

1. Das Datensubjekt hat sein Einverständnis erklärt.

2. Die Verarbeitung ist im Rahmen eines Vertragsabschlusses oder einer Umsetzung des Vertrags notwendig.

3. Die Verarbeitung ist zur Einhaltung einer rechtlichen Verpflichtung notwendig.

4. Die Verarbeitung ist notwendig, um die lebensnotwendigen Interessen des Datensubjektes zu sichern.

5. Die Verarbeitung ist notwendig, um eine Aufgabe öffentlichen Interesses wahrzunehmen.

6. Die Verarbeitung ist notwendig, um Interessen der Controller und Adressaten der Daten zu legitimieren.

Das Datensubjekt hat das Recht auf Zugang zu all seinen persönlichen Daten und kann, falls diese nicht in Übereinstimmung mit der Datenschutzrichtlinie verarbeitet werden, Maßnahmen bis hin zur Löschung und zum Rückzug besagter Daten aus der Verarbeitung verlangen (§12).

- Legitimer Zweck: Eine Bearbeitung der Daten kann nur gebunden an einen legitimen Zweck erfolgen. (§6b)

- Verhältnismäßigkeit: Persönliche Daten dürfen dann verarbeitet werden, wenn die Verarbeitung in einem angemessenen Verhältnis zum Zweck der Verarbeitung steht.

EU-Richtlinien wenden sich an die Mitgliedsstaaten und fordern diese auf, sie in der nationalen Gesetzgebung umzusetzen. Der nächste Abschnitt wird sich mit der Lage in Deutschland befassen.

3 Datenschutzprinzipien am Arbeitsplatz – die Situation in Deutschland

Der folgende Abschnitt gibt einen Einblick in die Organisationseinheiten, die beim Datenschutz am Arbeitsplatz in Deutschland beteiligt sind. Die EU-Richtlinie 95/46/EC regelt und begrenzt den freien Datenverkehr und das Sammeln persönlicher Informationen auch an deutschen Arbeitsplätzen. Unternehmen, die den E-Mailverkehr, die Internet- oder Telefonnutzung ihrer Mitarbeiter verfolgen und dies nicht mitteilen, können in den allermeisten Fällen verklagt werden. Trotzdem ist die Rechtslage nicht vollständig klar, wenn man beispielsweise die Praxis einiger Unternehmen betrachtet, ihren Mitarbeitern das Verschicken privater E-Mails zu untersagen.

Die (rechtliche) Verantwortung für die Datenverarbeitung obliegt dem Unternehmen selbst, aber auch dem Einzelnen, der im Auftrag des Unternehmens Daten verarbeitet. Mitarbeiter kommen in vielfältiger Weise mit dem Datenschutz in Berührung. Dies geschieht nicht nur die Entwicklung von Software zur Datenverarbeitung, die Zusammenarbeit mit Kunden oder Lieferenten oder bei der Mitarbeit in Zusammenhängen, wo persönliche Daten gesammelt und verarbeit werden. Es passiert auch beim intranetbasierten Zugang zu persönlichen Daten oder als Datensubjekt, dessen persönliche Daten vom Unternehmen verarbeitet werden.

Drei organisatorische Einheiten überwachen die Auslieferung Datenschutzkritischer Produkte innerhalb des Unternehmens (siehe Abbildung 2).

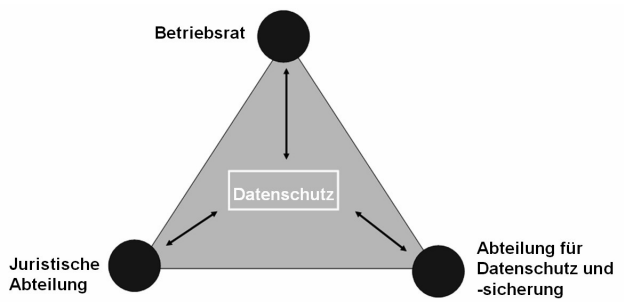

Abbildung 2 Überwachung Rollout durch 3 organisatorische Einheiten

Die Juristische Abteilung vertritt das Unternehmen vor Arbeitsgerichten und berät die Geschäftsleitung und die Personalabteilung bei der Umsetzung rechtlicher Änderungen. Der Betriebsrat vertritt die Beschäftigten und handelt auf der Unternehmensebene als lokales Komplement überregionaler Arbeitsverhandlungen.

Die Abteilung für Datenschutz überprüft alle Vorgänge, bei denen das Unternehmen aktiv in datenschutzrelevante Fragen verwickelt ist und unterstützt sowohl das Unternehmen als Ganzes als auch einzelne Mitarbeiter bei der Lösung dieser Fragen. Eine Arbeitsprozess-integrierte e-Learning Lösung muss in Abstimmung mit den drei genannten Organisationseinheiten erfolgen. Wir wenden uns nun einem konkreten Fall eines solchen e-Learning-Systems zu.

4 Klärung von Datenschutzfragen: das Beispiel eines arbeitsplatzintegrierten e-Learning-Systems

Im folgenden Abschnitt beschreiben wir ein e-Learning-System und setzen es in Bezug zu den Rahmenbedingungen, die in den vorherigen Abschnitten zur rechtlichen und organisatorischen Theorie und Praxis des Datenschutzes identifiziert wurden. Die vorgestellten Lösungsansätze erstrecken sich auf zwei der in Abbildung 1 dargestellten Dimensionen, nämlich auf die rechtliche und auf die technische.

4.1 Das System und die darin gesammelten Daten

Das e-Learning-System APOSDLE stärkt die Produktivität von Wissensarbeit, indem es dem Wissensarbeiter an seinem Arbeitsplatz zu alltäglichen Arbeitsaufgaben so genannte Wissensartefakte (mit Wissensrepräsentation versehene Dokumente) zur Verfügung stellt und Interaktionen mit anderen Benutzern ermöglicht. Von daher müssen dem System bestimmte Daten über den Benutzer (in seiner Rolle als Arbeitender, als Lernender, als Kommunikationsteilnehmer) zur Verfügung stehen, damit es seine volle Funktionalität entfalten kann:

- Unterstützung beim Arbeiten: APOSDLE identifiziert Nutzerbedürfnisse und bietet eine kontextspezifische Unterstützung entlang der Lernziele, die sich aus konkreten Arbeitsaufgaben ergeben. Das bedeutet, dass APOSDLE den Kontext am Benutzerarbeitsplatz (Windows-Desktop) erfasst, insbesondere den aktuellen Arbeitsschritt, die Historie der Systeminteraktionen und den Systemzustand - all dies möglichst umfassend bezogen auf die Betriebssystemebene.

- Unterstützung beim Lernen: APOSDLE hilft Wissensarbeitern bei der selbst bestimmten Wissensexploration, -anwendung und -reflexion. Das Lernen findet im Arbeitsprozess statt, so dass Lernprofile beispielsweise aus der Abfolge durchgeführter Arbeitsschritte generiert werden und die Auswahl der Wissensartefakte steuern können.

- Unterstützung von Kooperation: APOSDLE ermöglicht den Wissensaustausch und die kooperative Wissenserarbeitung über das jeweilige Rechnerumfeld am Arbeitsplatz. Dabei werden aus Wissensartefakten (zum Beispiel Chatprotokollen) sukzessive Lernressourcen. Das System schlägt geeignete Kooperationspartner für die Diskussion spezifischer Probleme oder Fragestellungen vor. Beide Kooperationspartner müssen der Kooperation zustimmen.

Die Unterstützung erfolgt somit nicht in einer separaten oder separierbaren Lernumgebung, sondern am Arbeitsplatz des Wissensarbeiters selbst. Lernen und Wissensmanagement gehen genauso fließend ineinander über wie Lernmaterialien und Dokumente, die ursprünglich gar nicht fürs Lernen konzipiert waren, nun aber durch das integrative System dafür aufbereitet werden [LI07]. APOSDLE kontextualisiert die zum Wissenstransfer erforderliche Kommunikation auf der Grundlage von [WE05,Goe04] und versucht über die Analyse der ausgeführten Prozessschritte Rückschlüsse auf die erreichten Lernziele des Benutzers zu setzen.

Die Grundarchitektur des Systems ist Client/Server-basiert. Datenschutzaspekte erstrecken sich sowohl auf die Clientanwendung, wo kritische Information gesammelt wird, als auch die Serverseite und ihre Speicherfunktionalitäten.

APOSDLE verarbeitet persönliche Daten. Bereits in der Phase der Erforschung seiner sozio-technischen Grundprinzipien geschieht das in unabhängigen rechtlichen Einheiten und wirft Datenschutzfragen auf, die bei einer Verwertung der Projektergebnisse an Unternehmen und Betreiber übergehen.

Die Pflege der Wissensartefakte und der Modelle zur Abbildung von Arbeitsaufgaben auf Lernzielen im System ist essentiell für die Funktionalitäten in APOSDLE. Darüber hinaus basieren einige Funktionalitäten, zum Beispiel zur Initiierung und Unterstützung von Kooperation, auf zuvor gesammelten Daten über das Verhalten der Systembenutzer. Aus Datenschutzgründen ist jedoch die Pflege vielen Stellen freiwillig. Darüber hinaus werden kritische Werte so codiert, dass eine Leistungsüberwachung anhand der gesammelten Informationen nicht möglich ist.

Aktivitätserkennung: Um den gegenwärtigen Arbeitsschritt zu erkennen, schreibt die Kontextmonitor-Komponente des APOSDLE Clients auf dem Rechner des Nutzers (innerhalb des Unternehmens). Diese Daten liegen den Modellen der Aktivitätserkennung zugrunde und untergliedern sich in Nutzerinteraktionen und den Systemzustand. Nutzer-Interaktionen mit Tastatur und Maus (zum Beispiel die Position der Maus, eingegebene Terme) mehrerer Testnutzer werden gesammelt, allerdings nicht im Klartext, sondern zu Hashwerten verrechnet und für statistische Analysen herangezogen, indem Korrelationen zwischen aggregierten Elementarereignissen und Einzelaktivitäten mit Verfahren des maschinellen Lernens bestimmt werden. Der Systemzustand umfasst Aktivitäten im Dateisystem (Zugriff/Löschen/Änderung von Verzeichnissen/Dateien/Dokumenten), Aufruf (Starten/Beenden von Anwendungen), Verschicken/Empfangen von e-Mails, Besuch/Markierung von Webseiten, Dokumentinhalte, Navigationsverhalten (besuchte Seiten und E-Mails), Ausdrucke von Dokumenten. Die Daten werden nicht im Klartext sondern als Hashwerte gespeichert und für statistische Analysen weiterverarbeitet um den entsprechenden abstrakten Nutzerarbeitsschritt vorherzusagen und geeignet durch Lernmaterial zu unterstützen..

Kooperation: Um die Suche nach Kooperationspartnern im Unternehmen zu unterstützen, wie für APOSDLE beispielsweise in (LO071) beschrieben, speichert das System Benutzerdaten:

- Daten zur Kooperationsinitiierung: Zur Initiierung einer Kooperation sind unternehmensinterne Identifikatoren wie Postadressen, E-Mailadressen, Telefonnummern, Messenger IDs etc. erforderlich. Benutzer können sich mit Hilfe dieser Identifikatoren und der entsprechenden Kooperations-Werkzeuge gegenseitig kontaktieren, die Kontakte aber auch jederzeit ablehnen. Die Daten zur Kooperationsinitiierung sind (in der Regel) für alle anderen Benutzer des Systems sichtbar.

1. Daten über den Benutzer: Name, Vorname und eine Porträtaufnahme sowie Angaben zur organisationalen Einbindung sind Teil der allgemeinen Daten zu einem Benutzer. Die Nutzer können die Aufnahme des Fotos in diese allgemein zugänglichen Informationen verweigern.

2. Daten über ausgeführte Arbeitsaufgaben: Um Relationen zwischen offenen Fragen im Arbeitsprozess einerseits und andererseits Experten, die diese Fragen beantworten könnten, herzustellen, speichert das System Informationen über die von den Nutzern durchgeführten Arbeitsschritte (welche und wie viele) und die bearbeiteten Wissensartefakte oder Lernmaterialien. Auch die getroffene Auswahl von Lernmaterialien hängt von der Erfassung der Arbeitsschritte ab.

3. Kooperationsdaten: Es werden weiterhin Daten über die Kooperation gesammelt, zum Beispiel die Identifikatoren für die Teilnehmer an der Kooperation, Start- und Endzeitpunkt, Transskripte der Kooperation (je nach verwendetem Werkzeug), Angaben zur Kontextualisierung, Notizen der Kooperationspartner etc. Diese Daten werden einerseits zur Aufbereitung neuer Wissensartefakte (siehe unten), andererseits zur verbesserten Kontextualisierung von zukünftigen Kooperationen verwendet. Es ist somit beispielsweise möglich, die Auswahl von Experten oder der für eine Kooperation empfohlenen/bereitgestellten Werkzeuge zu optimieren. Der Benutzer kann die Speicherung dieser Daten ablehnen, allerdings ist dann nur eine sehr rudimentäre Unterstützung bei der Kooperationsinitiierung möglich.

- Aufbereitung neuer Wissensartefakte: Inhalte, die die Benutzer als Nebenprodukt der Kooperationen erstellt haben (z.B. Transskripte, Notizen etc.) können als zukünftige Lernmaterialien aufbereitet werden. Die Speicherung und Veröffentlichung solcher neuen Wissensartefakte erfolgt nicht automatisch. APOSDLE stellt Möglichkeiten der Nachbearbeitung zur Verfügung, und stets müssen alle an der Kooperation beteiligten Parteien ihr Einverständnis zur Veröffentlichung geben.

5 Wie werden in APOSDLE die Kernanforderungen der Datenschutzrichtlinie adressiert?

Zwei Komponenten wurden speziell entwickelt, um sicherzustellen, dass Nutzer nur auf Informationen zugreifen können, zu denen sie auch die Zugriffsrechte besitzen: der Privacy Enhancement Service und der Security Manager.

Der Security Manager ist verantwortlich für die Überprüfung der Nutzerdaten während login/logout und deren Überprüfung innerhalb von Sessions.

Der Privacy Enhancement Service verwaltet die Privacy Enhancement Policy. Diese besteht aus einer Mengen von Regeln, die jede Organisation in der APOSDLE eingesetzt wird individuell festlegen kann. Hierzu gehören Regeln zur Aggregation von Benutzerdaten, zur Verwendung von Benutzerfeedback, zur Behandlung von Cooperation Events und vieles mehr. Der Privacy Enhancement Service muss von jedem Platform Service vor Rückgabe von Daten an den Benutzer aufgerufen werden. Er stellt insbesondere einen Filter dar, der sicherstellt, dass nur Informationen zur Verfügung gestellt werden, auf die der Benutzer auch Zugriffsrechte hat.

Auch beim Loggen von Kontext Informationen am Arbeitsplatz müssen Vorkehrungen zum Datenschutz getroffen werden. Hier sammeln diverse Sensoren hoch sensitive Daten wie private Chats oder besuchte URLs. Das Einführen von Mechanismen zur Verschleierung von Daten gewährleistet die Einhaltung geltender Gesetze und erhöht das Vertrauen des Benutzers in das System. Hier werden zwei Szenarien betrachtet. Im ersten Szenario werden nur Informationen gesammelt, die auf dem elektronischen Arbeitsplatz des Benutzers aufgenommen werden können. Darüber hinaus werden die gesammelten Daten auch nur lokal bearbeitet, so dass keine weiteren Personen Zugriff auf die Daten haben. In diesem Szenario ist das lokale Speichern von Informationen über einen langen Zeitraum sicherheitskritisch. In Szenario 2 wird nach dem Sammeln und Auswerten der Informationen auf der lokalen Maschine eine Anfrage an den Server geschickt, der dem Benutzer passende Materialien anbietet. Hier muss die Sicherheit des Nachrichtenkanals gewährleistet werden. Darüber hinaus muss sichergestellt werden, dass keine kritischen Daten auf dem Server gespeichert oder weitergegeben werden.

6 Zusammenfassung

Der vorhergehende Abschnitt hat entlang der Kernfunktionalitäten Hinweise auf den Umgang des Systems APOSDLE mit datenschutzkritischen Fragen geliefert. Wir kehren nun die Beobachtungsweise um und zeigen, wie die Grundprinzipien der europäischen Datenschutzrichtlinie in APOSDLE umgesetzt werden. In der Praxis betrifft das die organisatorische Ebene: zusammen mit den für den Datenschutz verantwortlichen Einheiten (Betriebsräten, Rechtsabteilungen, Datenschutzbeauftragten) hat das Projekt eine Vorgehensweise entwickelt und verschriftlicht.

Nutzer können diese Vorgehensweise (und das resultierende "privacy statement") annehmen (für eine einzelne Sitzung oder generell) oder jederzeit verwerfen, wobei im letzteren Falle die kontextabhängige und situative Adaptivität aus APOSDLE verloren geht (das System bietet dann einen Gastzugang). APOSDLE entspricht folgendermaßen den Grundprinzipien der EU-Richtlinie und erfüllt die notwendigen Voraussetzungen zur Unterzeichnung der "Privacy Policy" durch den Nutzer:

- Bekanntmachung ("notice"): Datensubjekte erfahren, wann Daten gesammelt werden. Die Art der Daten ist in der Privacy Policy aufgeführt und formuliert die im vorherigen Abschnitt gezeigten Daten zur Aktivitätserkennung und Kooperation. Im Falle einer Ablehnung der Privacy Policy werden sämtliche vorhandene Daten anonymisiert und, falls dies nicht möglich oder zielführend ist, verworfen.

- Zweckerklärung und -bindung ("purpose"): Die Verwendung der Daten, die in APOSDLE anfallen, ist an den Zweck, eine optimale kontextabhängige Zusammenstellung von Lernressourcen und Experten zu liefern, gebunden. Dies manifestiert sich ebenfalls in der der "Privacy Policy".

- Zustimmung ("consent"): Neben der Datenaufzeichnung zur Aktivitätserkennung (siehe Ausführungen unter "notice") fallen bei der Kooperation Daten an, deren spätere Veröffentlichung als Lerninhalt der Nutzer ganz oder teilweise ablehnen kann. Weiterhin fallen Daten über die Kooperation an, die für eine spätere Kooperationsinitiierung verwendet werden und mit deren Speicherung der Benutzer sich ebenfalls einverstanden erklären muss. Die Art der Daten muss in der "Privacy Policy" aufgeführt sein.

- Sicherheit ("security"): APOSDLE verwendet auf der Clientseite eine Verschlüsselung durch Hash-Werte, um die elementaren Nutzeraktionen zu speichern. Die resultierenden Dateien liefern immer noch genügend Informationen zur Identifikation von Benutzeraktionen durch maschinelle Lernverfahren [LO072], sind aber nicht mehr menschenlesbar. APOSDLE kann so konfiguriert werden, daß nur Teile der elementaren Nutzeraktionen gespeichert oder verschlüsselt werden. Bei Nichtverschlüsselung ist die Umwandlung (Hashing) nach nutzerseitigen Korrekturen möglich. Serverseitig beruht das Konzept auf dem Rahmenwerk WSS Security [WSS].

- Auskunftspflicht ("disclosure"): Die "Privacy Policy" stellt die verschriftlichte und ins System eingebundene Manifestation der Auskunftspflicht dar.

- Transparenz: Das Nutzerprofilmanagement gewährt jedem Benutzer Zugriff auf sein eigenes Profil und die aggregierten gesammelten Daten (z.B. Durchführungen von Arbeitsschritten, Erreichung von Lernzielen). Hierbei unterstützt das Nutzerprofilmanagement die Benutzer bei der Interpretation der vorgefundenen Daten und erlaubt das selektive Löschen von Daten.

- Zugang („access“): Mehrere Werkzeuge in APOSDLE sind auf die nachträgliche Modifikation gesammelter Daten durch den Benutzer abgestimmt: so bietet eine Kooperations-Management-Komponente die Möglichkeit, auf sämtliche Kooperationen einschließlich der darüber gesammelten Kooperationsdaten und der in der Kooperation erarbeiteten Lernmaterialien zuzugreifen. Das Nutzerprofilmanagement mit den Kerndaten wie Name und Kontaktinformation, sowie die mitgeschriebenen Daten zur Aktivitätserkennung sind zugänglich.

- Haftung ("accountability"): Die Haftbarkeits-Erklärung ist Teil der Privacy Policy.

Danksagung: APOSDLE ist teilweise gefördert durch das 6. Rahmenprogramm (FP6) für Forschung und Entwicklung der Europäischen Kommission im Information Society Technologies (IST) Arbeitsprogramm 2004. Das Know-Center wird im Rahmen des Österreichischen COMET-Programms - Competence Centers for Excellent Technologies - gefördert. Das Programm steht unter der Schirmherrschaft des Österreichischen Bundesministeriums für Verkehr, Innovation und Technologie, des Österreichischen Bundesministeriums für Wirtschaft und Arbeit und des Landes Steiermark. Die Abwicklung des Programms erfolgt durch die Österreichische Forschungsförderungsgesellschaft FFG.

Literaturverzeichnis

[ECHR] European Court of Human Rights, URL: http://www.echr.coe.int/echr/ [Stand: 29.02.2008]

[EU02] Directive 2002/58/EC of the European Parliament and of the Council

[EU04] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[GOE04] Goertz, M.,Ackermann, R.,Schmitt, J.,Steinmetz, R. (2004) Context-aware Communication Services: A Framework for Building Enhanced IP Telephony Services. International Conference on Computer Communications and Networks (ICCCN) 2004, 272--279, Oct 2004.

[HR84] Die Allgemeine Erklärung der Menschenrechte, URL: http://www.unhchr.ch/udhr/lang/ger.htm [Stand: 29.02.2008]

[LI06] Lindstaedt S., Mayer H. (2006). A Storyboard of the APOSDLE Vision. Poster submitted to the First European Conference on Technology Enhanced Learning (EC-TEL 2006), October 01-04, 2006, Crete, Greece.

[LI07] Lindstaedt, S.; Scheir, P.; Ulbrich, A. (2007). Scruffy Technologies to Enable (Work-integrated) Learning, EC-TEL 2007, Crete, Greece, 17-20 September 2007

[LO071] Lokaiczyk, R., Godehardt, E., Faatz, A., Goertz, M., Kienle, A., Wessner, M., & Ulbrich, A. (2007) Exploiting Context Information for Identification of Relevant Experts in Collaborative Workplace-Embedded e-Learning Environments EC-TEL 07

[LO072] Lokaiczyk, R., E., Faatz, A., Goertz, M. (2007). Towards Improving Privacy and Security in Context-Aware Workplace-Embedded e-Learning Environments through Data Obfuscation. *Workshop on e-Learning* 2007 ISSN 1613-0073 187-196

[OECD] Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data, 1980, URL: http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html [Stand: 29.02.2008]

[WE05] Wessner, Martin (2005): Kontextuelle Kooperation in virtuellen Lernumgebungen. Lohmar: Eul Verlag

[WSS] Web Services Security: 3 SOAP Message Security 1.0 (WS-Security 2004)