A Data-Centric Approach for Privacy-Aware Business Process Enablement

Stuart Short, Samuel Paul Kaluvuri

A Data-centric Approach for Privacy-aware Business Process Enablement

Stuart Short[1] and Samuel Paul Kaluvuri[1]

[1] Sap Labs France, 805, Avenue du Docteur Maurice Donat,
BP 1216 - 06254 Mougins Cedex, France
{Stuart.Short, Samuel.Paul.Kaluvuri}@sap.com

Abstract. In a SOA context, enterprises can use workflow technologies to orchestrate available business processes and their corresponding services and apply business rules or policies to control how they can be used and who can use them. This approach becomes a bit more complex when a set of business processes includes services that derive outside the company's domain and therefore can be difficult to align with existing rules/policies. In the privacy and security domain, access control and policy languages are used to define what actions can be performed on resources, by whom, for what purpose and in what context. In this paper we propose an approach for dealing with the inclusion of internal and/or external services in a business process that contains data handling policies.

Keywords: privacy; policy; BPM; SOA; web services

1 Introduction

Privacy on the internet or in information systems usually refers to data that is of a personal or sensitive nature [2]. This information can be used to identify somebody (personal identifiable information) and may be used in a manner that was not intended. With the onslaught of tougher laws (e.g. Sarbanes-Oxley SOX [18]) and regulations, businesses and more to the point, system administrators, are being asked to put in place mechanisms (e.g. Control Objectives for Information and related Technology CobiT [19] that can enable a compliant environment and ensure that information is being handled correctly.

It can be a difficult task to translate the idea of privacy into technology, let alone develop privacy preserving mechanisms [5]. Furthermore, there may be issues over the use of personal information for genuine business interests on the one hand and the right of the individual to maintain control over how their personal data is used [6] [7] on the other hand. This trade-off [8] has lead to an increase in both corporate self-regulation and government intervention [9] in the form of data protection and privacy laws [10]. One way for an organization to deal with privacy concerns is to control its processes and the flow of information. Business Process Management is a systematic

way to achieve this goal although its use is mainly to create business value and operational efficiency for competitive advantage [11] [12].

Service Oriented Architectures (SOA) are commonly used as a way to design business processes and loosely coupled services (a set of related business functions) can be dynamically composed or orchestrated to meet the needs of the designer and end-users. Although traditional workflows rarely leave the boundaries of the enterprise for security, privacy, sharing ability, firewalls reasons [13] there has been a definite move towards collaborative workflows. With the existing SOA and BPM approach combined with greater collaboration and tougher regulations on how data is consumed, process designers need to be able to track how data flows and ensure that the business processes are compliant.

In this paper we propose a two-fold solution for dealing with the inclusion of internal and/or external services in a business process. Firstly, in a workflow, policy or system administrators are able to describe policies on activities in a business process and data objects. Furthermore they are able to identify inconsistencies with activities or web services that are mapped or linked together in a process. For instance, if an activity states that it can be used by certain participants in a certain context and the following activity disagrees with one of these elements then the binding with a data object will trigger an alert or warning on the designer's interface.

The second part of the proposed solution permits the workflow to import policies that are attached to an external or internal service. In the former case, when the service is consumed with the data handling policies, it would be seen as accepting a Service Level Agreement (SLA) with an external party and confirming that the consumer of the service will adhere to whatever rules are in place. Once the SLA is imported with the service the policy administrator is prompted to align the naming of potential recipients to the system's identity management engine. This ensures consistency of integration and lessens the chance of ambiguity.

The paper is outlined as follows: Section 2 first lists the requirements for a privacy-enabled BPM. The idea of data-centricity in BPM is detailed in Section 3. The underlying approach to a prototype implementation is then discussed in Section 4. We finally compare the approach presented in this paper with related work and outline future directions for investigation.

2 Requirements for a Privacy-Enabled BPM

When designing a process an administrator can apply access control by assigning roles to activities ensuring that only those who are authorized to perform a given task can do so. Our approach extends this principle by allowing the process designer to include not only role assignment but also to express how the web service and the data contained within should be consumed and how long it can be used for. Furthermore the nature of web services permits their use in different contexts and environments, therefore the data handling or service consumption policies should always stay with the web service so that the initial requirements are respected. In order to do this a policy structure is needed that is capable of describing the aforementioned conditions

and permit a means to evaluate whether a web service is consumable thereby making the business process compliant.

The following are functional requirements for a BPM engine that will assist a process designer in being compliant both with internal and external web services used in a process:

2.1 Policy Language

In order to express policies on a web service in a business process, the workflow engine should use a language that has a well-defined structure. An example of this can be seen in XACML [4]. This language uses the structure of Subject, Action and Resource (plus optional conditions or rules that may have to be satisfied) and provides a processing model that renders a decision on whether a resource should be accessed or not.

2.2 Policy Viewer

To facilitate the writing of policies, the BPM application should allow the designer the ability to define policies and to assign them to activities in the business process. Therefore a policy viewer should be integrated into the BPM suite that links with an identity management engine and allows for the mapping of roles or recipients from web services to the roles specified in the identity management engine, if not done so already.

2.3 Sticky Policies

Furthermore, there should be a means to import policies that belong to internal and external web services, into the viewer. In our solution we propose a way to include the policies in the web service description language file and then to populate the properties of the viewer. In this way we are ensuring that downstream usage of web services respects the original intention of use specified in the services' policies. Sticky policies [20] [24] are strictly associated to a piece of data and should be composed whenever data aggregation happens. Expressing a condition for each piece of data is a means for a data provider to declare how personal data is to be used. Even if privacy policy languages like P3P [1], EPAL [22] or Prime [23] exist they lack the notion of sticky policies or the complex composition of services or policies for resolving possible conflicts [21].

2.4 Policy Checker

Once the binding of a web service to a task or activity is completed and the policies have been attached, there should be a means to check if there are policy conflicts between services. For example, when it is stated that a web service should not be consumed for marketing purposes and the subsequent activity/web service in the

process permits this, then there is a conflict of purpose or, in other terms, a violation of the web services policy.

2.5 Policy Language

By including a validity period for a web service's policy, the process designer can be reminded that the service's policy is out-of-date and he needs to reload/re-import the WSDL [3] file. This feature ensures that the service consumer has the most current policy and therefore remains compliant.

3 Privacy in BPM/Web Services

Web services are consumed in a business process purely on the basis of their business and technical functionality however this approach is limited when it comes to dealing with privacy concerns. Services can be aligned to business rules and assigned to be used by specific users however this approach is time-consuming and is limited in its expressivity. A web service policy is a way to stipulate how the service has to be consumed, for example, it can be stated that the service can be only consumed by certain entities such as a person and they have the right to do a certain action in a specific context. Sticking a policy to a service means that when the service is invoked, the data that is sent and received will adhere to the stated policy that travels with it. . This facilitates process composition by identifying the appropriate web services. The process designer should be allowed to narrow the scope of certain policies as long as it is not compromised. For instance, if the web service stated that the data within a service can only be consumed within a certain time period, e.g. 50 days, perhaps internal practices deem this retention period too long, then this should be narrowed to comply. This would be also the case for the purpose of using the service and for the proposed recipient.

3.1 Policy Model Overview

Privacy of data in a business process can be achieved by attaching data privacy policies (privacy policies) onto data objects.. Hence directly attaching a privacy policy to a data object would make a business process more rigid and not offer the process designer the opportunity to change the services as and when required for process optimization.

In the proposed model (Fig. 1) the privacy policies are attached to an input and output of an activity. This in effect implies that an activity states its intentions of using the data that is required by it (consumption), this is the input privacy policy, while the output privacy policy states how the data that is generated by an activity should be used.

The output of an activity if it has to be used again by any other activity in a business process has to be mapped to data fields contained in a single data object or

many data objects. The output privacy policy attached to an activity is then attached to the data fields that are mapped to the output of an activity. Through this method, privacy policies can be attached to data fields in a data object.

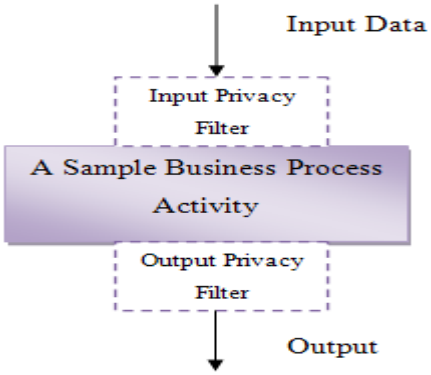

Fig. 1. Input and Output of an Activity.

3.2 Privacy-aware BPM Use Case

This section introduces a scenario that illustrates the need for data handling policies in a business process. When a bank customer/borrower submits an application for a loan, the loan origination process is initiated. This process entails the formalization, evaluation and eventual decision on the borrower's request. In order to do this, three main actors may be involved within the bank, namely, pre-processing clerk, post-processing clerk and a manager.

The pre-processing clerk receives a loan request from a customer and starts the application. Once the loan applicant's identity has been verified the post-processing clerk evaluates the customer's credit rating both through internal and external rating mechanisms. The latter is a trusted third-party credit bureau that can derive information about the applicant from various sources including publicly available records. In the event that the rating meets the requirements of the bank, the clerk selects the appropriate bundled product and forwards the application to the manager for final evaluation and eventual signature. On approval a loan account is then opened for the loan applicant.

Supposing that the information in the loan origination scenario contained restrictions on how it should be processed then it should be possible to include these in a BPM while designing a process. Furthermore, a system administrator should be able to test whether there are inconsistencies between policies. For example, the loan applicant may inform the pre-processing clerk that she wishes to express restrictions on who can perform a task, for what purpose and how long the data can remain in the system. The applicant states that the information supplied may only be used for administrative needs and may not be used for marketing; that marketing research analysts may not read this information and that the information is only to be used for the lifespan of the application unless successfully processed. The clerk includes these

requirements while inputting the customer's information and an alert is triggered, at design time, if the subsequent consuming service or activity conflicts with this.

The credit bureau could specify that only a manager could request information from its service, with the intention of administrative purposes and may only store the information for a certain period of time. Given that the bureau is an external service there should be a means for it to express itself in these terms and also for the consuming service to receive this information and align it with its own system requirements.

4 Privacy-enabled BPM/Web Services

When we talk about privacy we are referring to enabling a system with the means to deal with expressions on how data is processed. In the context of BPM and SOA we would see this as providing a means for process designers to control how data is handled in a web service composition, respecting the privacy concerns of parties to the orchestration. Whether these web services are internal or external, the down-stream usage of data maintains the original conditions of use. This data-centric approach can involve the use of data handling policies (DHP) 2 that can be attached to data. In the loan origination process example, the bank may have a policy that the sensitive information or personal identifiable information (PII) of the customers who apply for a loan, will not be sent to an entity that will use this information for other reasons than is intended by the current process. The PII could be attributes such as age, address or ethnic background. It can specify that the data provided by the customer in a loan application will only be consumed for a certain reason (purpose), for a certain length of time (retention period) and by a certain person (potential recipient). The process designer has to ensure that any external services that are used in the process have to comply with these data handling policies.

When the process under-design has a large amount of activities, a privacy manager tool is required to handle these policies and inform the process designer of the conflicts. In the loan origination scenario, the credit bureau should not receive information about the loan applicant that is not needed in the rating check.

4.1 Policy Language Structure

A privacy model is required that encapsulates the key privacy attributes in a business process. The model also has to facilitate the policies to be saved in existing standard languages like XACML:

```
<Subject>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name">
   <AttributeValue>PostProcessorClerk</AttributeValue>
  </Attribute>
 </Subject>
 <Resource>
```

```
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#string">
     <AttributeValue>Ethnic_Background</AttributeValue>
    </Attribute>
   </Resource>
   <Action>
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
          DataType="http://www.w3.org/2001/XMLSchema#string">
     <AttributeValue>Deny</AttributeValue>
    </Attribute>
</Action>
```

The privacy attributes considered in the proposed model are Purpose Specification, Recipient Specification and Retention Obligation.

4.1.1 Purpose Specification

The purpose attached to data is useful in regulating the unintended usage of the data. The data that is collected by a service to do a certain task (for example: providing an insurance quote) must be used only for that purposes that the data provider intends. The purpose is the intention of using the data provided or the intention for which the data should be used. Purposes can vary within different domains. However, having a purpose attached to a data gives the data owner (or data generator) some control over the downstream usage of the data.

This ability to specify the purpose, for which data can be used, helps the process designers (PD) to understand clearly how the data from external enterprise services should be used. It also provides some level of guarantee to them (PD) about how their data is consumed by the external enterprise services. This has a positive effect on collaboration as organizations can know the intent of data consumption by all participating parties.

4.1.2 Recipient Specification

The Recipient specification allows the data provider and the data consumer to be aware of the users/roles that have access to the data. A data provider can stipulate that the data provided by it should only be accessed by only Managers or any role higher than that.

A recipient is the user/role that has the access to the data that is being consumed or a user/role that can access the data being provided. The recipient specification is of vital importance when enterprises are sharing sensitive information. Recipient specification is closely related with access control policies. In a business process access control, information is usually associated with activities (tasks) and not on the data itself. This is where the recipient specification proves useful by providing the process designer the means to explicitly state the recipients for the data that is generated or provided to an activity.

Recipient specification has more significance in automated activities, because the data that is provided to these services could be stored in databases. If the automated activity is invoking a external web service, process designers would be wary to provide sensitive information without knowing who has access to the data stored by these external services.

4.1.3 Retention Obligation

The retention period of data is of vital importance in information security. In business processes, there are two major compulsions to have a data retention policy in place for organizations, namely, compliance to government regulations and improving the trust of consumers in an organization. When data is a business process consumed by automated activities which have external services, running on servers located in different geographical locations and governed by different data protection regulations, it becomes challenging for a process designer to design a business process that adheres to the data protection regulations that are in place. For example, a business process designed for travel booking by the HR portal of an enterprise located in France uses an external service that books the hotels in China and is governed by Chinese data protection laws, a process designer would be wary to share his personal information (governed by data protection laws in France) to a service that runs under Chinese data protection laws which are very strict and always under the ambit of the state.

Thus by adding a data retention clause in the privacy policy in the business process, an external service that is consuming data is “obliged” to accept the data retention period set by the process designer.

4.2 Human and Automated Activities

Business Process Management software permits an orchestration of services to fit a business need, for instance, a process designer may wish to establish a new loan approval process that involves different services within the organization. Authorizations can be assigned to the process as a whole and to the individual parts or activities. This is done in line with the roles or groups that have been defined in the identity management engine, which is accessible by the BPM. This ensures that there is an accepted system-wide authorization schema in place that should be adhered to when designing processes.

Human activities in BPM are an illustration of this as the designer can assign limited users to an activity and thereby enable them to contribute (view, edit, append or generate) to both the input and output of that activity. The authorized person may be allowed to perform the allocated task however there is no means to prevent the input data being used in a manner that was not intended. In a banking scenario, a bank clerk may be authorized to collect customer information for the purpose of a loan application but perhaps the customer does not wish that this data be used by the bank’s marketing department and be a potential target for an insurance policy.

Automated activities do not allow for the same access control as they are web services that are consumed in the business process. The designer selects the appropriate methods and attaches them to the automated activity. Exposing business processes as web services facilitates system integration as any technology can be used, such as Java and .NET, and the designer just needs to locate, identify and communicate through a WSDL file. Also this approach provides for greater efficiency as services can be easily reused in other business processes.

Given the automated nature of these type of activities and the lack of access control and user information, privacy preservation becomes more critical. As this may be an external service there may be a possibility that it resides on a server in a country that has different data protection laws. Therefore information exchanged with this service should be regulated in some manner.

4.3 Policy Consistency Check

To facilitate the process designer to specify privacy policies on the aforementioned activity types in a BP and to check for the consistency of these properties, a privacy validator tool has been developed as a plugin for SAP Netweaver BPM (Fig. 2). The tool has a User Interface for the process designer to attach policies on activities, perform the consistency check and inform the process designer of any policy mismatches. In this instance the Clerk PostProcessor has filled in a data retention period that will conflict with the period specified in the previous activity, input customer data. When the policy check is run there is a warning on the UI and the error details detailed in the Problems tab.

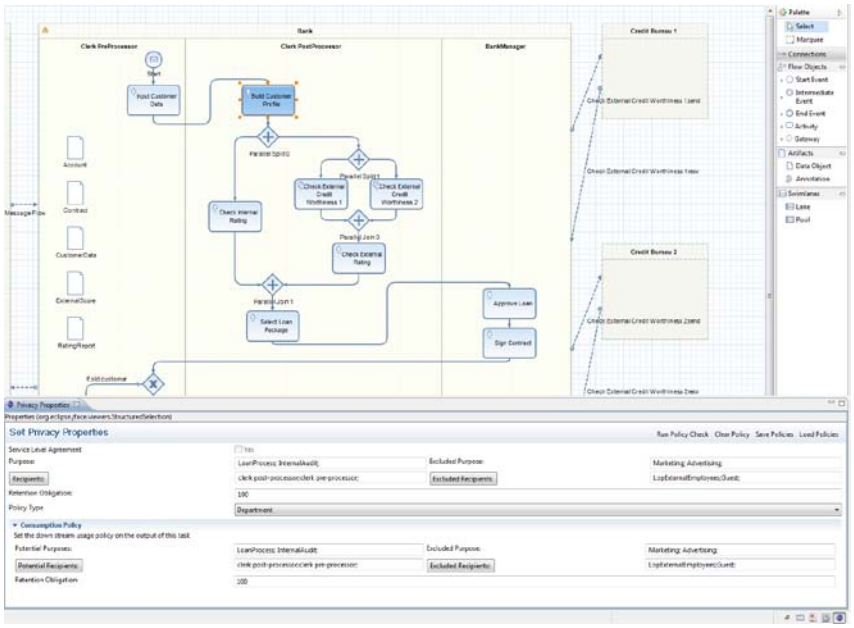

Fig. 2. Policy Checker.

A web service provider can specify the location of an associated data handling policy file to the WSDL file through the usage of the documentation tag available in WSDL. The documentation tag can contain the URL of the policy file. When the process designer imports a WSDL file for automated activities in the process under-design, the privacy validator tool will extract the URL from the WSDL file, retrieve the file contained in the specified location, parse it and display it in the privacy view for the process designer to view the policy. A wizard permits the mapping of roles to the internal user management system in the case of external services in order to comply to its internal structures. A sample WSDL containing the URL of the policy file is shown below:

```
  <wsdl:definitions
targetNamespace="http://example.com/sample/ws/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:tns="http://example.com/sample/ws/">
  <wsdl:documentation>
  @PolicyLink=Yes
  @PolicyURL=http://example.com/samplePrivacyPolicy.xml
  </wsdl:documentation>
  <wsdl:types>
  <!-- --- -->
</wsdl:types>
```

In a business process, the context data, that is the data generated by an activity or the data provided to an activity is stored in Data Objects (DO). A DO contains the actual data that acts as an input to an activity or collected as an output from an acitivity. In a privacy aware workflow, the data should have an associated data handling policy when it is consumed by activities in the BPM. The privacy tool developed will enable the process designer to attach policies to activities. The policy of an activity consists of two parts: Consumption Policy and Provider Policy. Consumption Policy states how an activity will be consuming the data provided to it. While the Provider policy specifies how the data that is provided by an activity should be used.

When the output of an activity is mapped into the data fields of a data object, the provider policy of that activity is attached to those data fields. When the outputs of two or more activities are mapped into the same data field, the provider policies of those activities are merged into a single policy for the data field. However, if the policies of those activities are conflicting with each other, the process designer is informed through a warning message. This data object has a data handling policy that is mapped as an input to another activity and the consumption policy of the activity is matched against the policy of the data object and if there are any conflicts the process designer is informed through an error message. The process designer can thus, choose to change the policies on an activity to resolve the conflict or if it is an external service, he/she can negotiate with the service provider for an acceptable policy. The sequence diagram [Fig. 3.] gives an overview of the steps involved in the policy check.

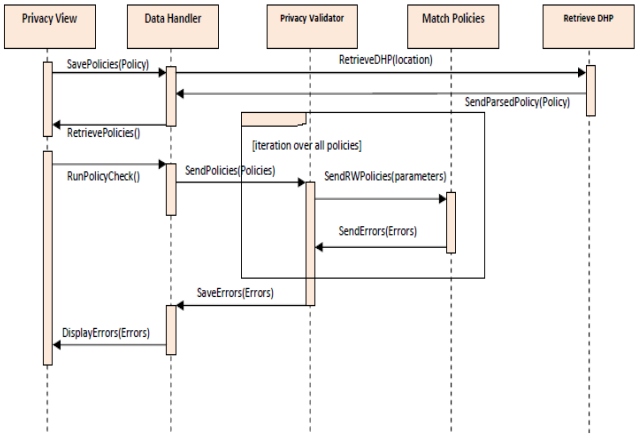

Fig. 3. Sequence Diagram of Policy Checking.

5 Related Art

In [6] the model chooses the approach of assigning a purpose to the workflow considering it as a unit of work that cannot be interrupted. The user roles have purposes associated to them. When an activity in a workflow that has a user role includes a purpose that is conflicting with the purpose of the workflow, then the user role is denied access to perform the task. However, a workflow is an orchestration of activities, both human and automated and each activity can have a purpose associated with it and especially automated activities that consume external services should have downstream usage associated with them. And though denying access to a user role that is conflicting with the purpose of the workflow enforces privacy at run time, it does not aid in the design of privacy aware business processes. Also there is no data retention period specified. For compliance purposes data retention periods would be necessary and also external services used in workflows might want the organization to assure that the data it is providing would be deleted after a certain amount of time.

In the CoopFlow approach [15], the privacy on a workflow results abstracting the workflow of an organization and providing only the minimal amount of activities that are needed for cooperation between workflows of different organizations. The privacy in this context is on the internal activities of an organization and not on the data. Though data privacy could be a result of the abstraction of some activities and some internal data, it is not the main aim of this methodology.

The proposed XML-based notation called BPeX[16], describes a Business Process Model as a hierarchical tree-based structure. The model preserves all the relationships between the different activities and entities of a business process model. The BPeX, is then extended to support P3P policies. The policies are attached to a pool. It then attaches a purpose to each BPM element. The recipient information is attached to message flows that go outside the pool. The policy enforcement is done by using an XPath Matching on the BPeX file. A Boolean value "isP3pCompliant" is used as a flag to state the compliance of each activity with the P3P policy.

The policies are nevertheless attached to the pool and not at the activity level which can hamper the consumption of external services that have their own privacy policies. Activities can have different purposes, or recipients, for example, an external web service which is used as automated activity, can have its own privacy policy. The recipient list is attached to message flows from an internal pool to an external pool, which is based on an assumption that internally every office and every department within the organization have no privacy restrictions on them, which is not the case in most of the organizations.

In [17] a subject notion is introduced that is added to the workflow design; the subject is the user. The workflow management system can then access the subject attribute, and from that retrieve the user's privacy policy and thus can enforce the privacy policies of the user in the workflow. It also introduces auxiliary data properties that are attached to data elements and these can be used in real time for various functions in the workflow. The privacy properties of the user are then retrieved for each activity that is performed by the user and then the policies based on

the policy of the user's data is hidden or generalized. They do not consider the bindings of activities in a business process.

6 Conclusion

This paper discussed privacy issues in the context of service oriented architectures in business process management. A solution based on data handling policies was used to add conditions to the use activities or web services in a BPM application. Furthermore the solution allowed for the import of policies attached to web services. A consistency check is able to be carried out by deploying bound activities in design time. Following alerts, the process designer is aware of any conflicting issues and is able to either remove the activity/web service or amend the consuming service's policy in order to adhere to the previous activity/web service. The proposal needs to integrate fully with a BPM application and also with a standard policy language and engine. Furthermore the approach will be evaluated in terms of scalability and compared to other matching mechanisms. These issues will be investigated in the context of the European project Primelife. Recent interest in moving towards data-oriented architectures [25] and other work in data centric security management [26] may influence future work.

Acknowledgements. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483. The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

References

1. Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P/
2. Primelife, European project, http://www.primelife.eu/
3. WSDL specifications, http://www.w3.org/TR/wsdl
4. XACML specifications, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#XACML20
5. Miller, S., Weckert, J.: Privacy, the Workplace and the Internet. Journal of Business Ethics, pp. 255--265 (2000)
6. Eddy, E. R., Stone, D. L., Stone-Romero, E. F.: The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. Personnel Psychology, 52(2), pp. 335--358 (1999)

7. Culnan, M., Smith, H., Bies, R.: Law Privacy and Organizations : The Corporate Obsession to know v. the individual right not to be known. In: Sitkin, S., Bies, R. (eds.) The legalistic organization, pp. 199--211, Thousand Oaks, CA (1994)
8. Milne, G. R., Gordon, M. E.: Direct mail privacy-efficiency trade-offs within an implied social contract framework. Journal of Public Policy & Marketing, 12(2), pp. 206--215 (1993)
9. Milberg, S. J., Smith, H., Burke, S. J.: Information Privacy: Corporate Management and National Regulation. Organization Science, pp. 35--57 (2000)
10. Dresner, S.: Data protection roundup. Privacy Laws Bus. (U.K.) (33) January, pp. 2--8. (1996)
11. Noel, J.: BPM and SOA: Better Together. White paper, IBM (2005)
12. Malinverno, P., Hill, J. B.: SOA and BPM are Better Together. Gartner, pp. 3--11 (2007)
13. Chen, Q., Hsu, M.: Inter-Enterprise Collaborative Business Process Management. International Conference on Data Engineering, pp. 253--260 (2001)
14. Jafari, M., Safavi-Naini, R., Sheppard, N. P.: Enforcing Purpose of User via workflows. WPES November, (2009)
15. Chebbi, I., Tata, S.: Workflow abstraction for privacy preservation. In: Weske, M., Hacid, M., Godart, C. (eds.) Proceedings of the 2007 International Conference on Web Information Systems Engineering. LNCS, pp. 166--177. Springer-Verlag, Berlin, Heidelberg (2007)
16. Chinosi, M., Trombetta, A.: Integrating Privacy Policies into Business Processes. Journal of Research and Practice in Information Technology, vol. 41, No. 2, pp. 155--170 (2009)
17. Alhaqbani, B., Adams, M., Fidge, C., ter Hofstede, A.H.M.: Privacy-Aware Workflow Management. BPM Center Report BPM-09-06, BPMcenter.org (2009)
18. Sarbanes Oxley Act of 2002, http://uscode.house.gov/download/pls/15C98.txt
19. Information Systems Audit and Control Association (ISACA), CobiT4.1: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf
20. Ashley, P., Powers, C., Schunter, M.: From privacy promises to privacy management: a new approach for enforcing privacy throughout an enterprise. In: NSPW '02: Proceedings of the 2002 workshop on New security paradigms, pp. 43--50, New York, NY, USA, ACM (2002)
21. Bandhakavi, S., Zhang, C.C., Winslett, M.: Super-sticky and declassifiable release policies for flexible information dissemination control. In: WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society, pp. 51—58, New York, NY, USA, ACM (2006)
22. EPAL: Enterprise privacy authorisation language. http://www.zurich.ibm.com/pri/projects/epal.html
23. Prime: Privacy and identity management for europe (prime). https://www.prime-project.eu/prime products/
24. Mont, M. C., Pearson, S., Bramhall, P.: Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. Technical report, http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf (2003)
25. Data4BPM(BEDL) http://public.dhe.ibm.com/software/dw/wes/1004_nandi/1004_nandi.pdf
26. Grandison, T., Bilger, M., Graf, M., Swimmer, M. Schunter, M., Wespi, A., Zunic, N., O'Connor, L: Elevating the Discussion on Security Management - The Data Centric Paradigm. In: Proceedings of the 2nd IEEE/IFIP International Workshop on Business-driven IT Management. pp. 89--93. IEEE Press, Piscataway, NJ (2007)