SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document Type: Deliverable

Title: # Contractual Framework

Editor(s) Joseph Alhadeff, Brendan Van Alsenoy

Work Package: WP6

Deliverable Nr: D6.2

Dissemination: PU

Preparation Date: December, 2009

Version: 3.0

The TAS³ Consortium

	Beneficiary Name	Country	Short	Role
1	KU Leuven	BE	KUL	Coordinator
2	Synergetics NV/SA	BE	SYN	Partner
3	University of Kent	UK	KENT	Partner
4	University of Karlsruhe	DE	KARL	Partner
5	Technische Universiteit Eindhoven	NL	TUE	Partner
6	CNR/ISTI	IT	CNR	Partner
7	University of Koblenz-Landau	DE	UNIKOL	Partner
8	Vrije Universiteit Brussel	BE	VUB	Partner
9	University of Zaragoza	ES	UNIZAR	Partner
10	University of Nottingham	UK	NOT	Partner
11	SAP Research	DE	SAP	S&T Coord.
12	EIfEL	FR	EIF	Partner
13	Intalio	UK	INT	Partner
14	Risaris	IR	RIS	Partner
15	Kenteq	NL	KETQ	Partner
16	Oracle	UK	ORACLE	Partner
17	Custodix	BE	CUS	Partner
18	Medisoft	NL	MEDI	Partner
19	Symlabs	PT	SYM	Partner

Contributors

	Name	Organisation
1	Joseph Alhadeff	ORACLE
2	Brendan Van Alsenoy	KUL (ICRI)
3	David Chadwick	KENT
4	Lex Polman and Kenteq Legal	KETQ
5	Quentin Reul	VUB
6	Louis Schilders	CUS
7	Klemens Böhm	KARL
8	Luk Vervenne	SYN

Contents

1 Executive Summary

The objective of TAS³ is to develop a secure, yet adaptable technical infrastructure that enables the creation, maintenance and exchange of personal information between multiple service providers in a user-centric fashion. TAS³ relies on the concept of a Trust Network that is governed by business requirements, technical requirements, policy requirements and legal requirements. This deliverable focuses on the development of a flexible and adaptable contractual framework for all TAS³ participants and general policy requirements that shall support the Trust Network by defining and enforcing enterprise policies at the level of individual service providers.

Changes in jobs, residences, and professional and social relationships are more frequent occurrences than ever before. Information must be portable and accessible to meet the needs of organizations, individuals and society as a whole. Providing this portability and flexibility is also key to remaining competitive and enabling growth in the information society and digital economy. TAS³ enables an infrastructure of trust, security and privacy to meet the needs of today's more global and mobile society. TAS³'s development is geared to compliance with privacy laws and provides for both user control and organizational functionality of records. TAS³ thus combines security and privacy with technology, policy and law to create a trust infrastructure predicated on verifiable information governance.

TAS³'s approach which co-ordinates the development of contract, policy, technology and business requirements at the inception of the project improves on existing models of privacy by design (often limited to embedding privacy technology at the design stage). This broader and earlier collaboration across the 4 elements mentioned above creates a more seamless support of privacy, which in turn enables and enhances trust for data subjects. In many design and development situations the interdependent nature of the 4 elements is insufficiently optimized. In TAS³, interactions across entities are designed to enhance system optimization. Information collection, access and transfer proceed in accordance with data minimization; legal and compliance obligations are supported in audit protocols, and required enterprise policies supplement security, use limitation, and other data protection requirements. This optimization also occurs at the ecosystem rather than just enterprise/organization level, thereby providing more seamless and end-to-end integration of requirements across the 4 elements of the Trust Network. Obviously recourse to national data protection authorities and courts always remains possible in case of non-compliance. TAS³ however also seeks to provide the data subject with more simple paths to compliance enforcement that can be accomplished entirely from within the TAS³ Network.

The TAS³ contractual framework exists and operates at three levels: Ecosystem, Transaction and Technical. The Ecosystem level provides the general binding of rights and obligations across all parties, including general terms and conditions, required technical implementations and requirements for policies at the level of individual organizations. The Ecosystem contract is drafted in counterpart forms

adapted to the role of the individual user/entity, but with large commonalities for the core aspects of the TAS³ Ecosystem.

Transaction level contracts provide an opportunity to supplement or enhance controls and instructions related to a specific role in a transaction. Because these contracts need to be tailored to the specific context of the transaction, we are exploring how to develop standard contracts for different types of transactions with attached schedules to provide the customization as well as dynamically generated contracts at the time of the transaction. This modular drafting will lessen the need to involve legal counsel at every transaction and thus increase speed and reducing cost.

Obligations are put in place at the technical level through sticky policies and other privacy management and negotiation elements of the architecture. As these obligations are expressed through technical means that may never be explicated in writing, they are explicitly supported and accepted by the parties as binding through agreement to the Ecosystem contract.

Since the contractual framework binds all parties, it is horizontal in its very nature and is relevant to all TAS³ work packages. The contract and policy frameworks, which will be described in this document, are mostly dependent upon both the Legal Requirements previously defined in TAS³ D6.1 as well as the Architecture requirements developed in TAS³ D2.1. The requirements that were identified in WP 1 (TAS³ D1.2, D1.4 as well as the consideration of the current state of the art in TAS³ D1.1) serve as inputs to this document. Conversely, WP6 has in turn identified its own requirements and provided input to both D1.2 and D1.4 (annex 4). The Demonstrator projects set forth in TAS³ D9.1 serve both as inputs to the contractual framework and will serve in continued iterations as proving grounds for testing actual contract terms.

The TAS³ Network is an example of Privacy-by-design and enables organizations to be more transparent as to their obligations and accountable for their proper exercise. These concepts of Privacy by Design and accountability are important developing trends in privacy in the EU as set forth in the 2009 Privacy Update Annex V to TAS³ D6.1. The collaborative design of TAS³ resulting in mutual support across disciplines (law, policy technology) is an end goal of Privacy by Design and yields greater levels of accountability.

2 Introduction

The objective of TAS³ is to develop a secure, yet adaptable technical infrastructure that enables the user-centric creation, maintenance and exchange of personal information between multiple service providers and the data subjects involved. TAS³ is organized as a Trust Network combining business, privacy, policy and legal elements to provide services in a user-centric architecture. The ability of users to effectively exert control over their personal information is an essential aspect of privacy and more of an ideal than a reality in today's information society.

Changes in jobs, residences, and professional and social relationships occur more frequently than ever before. Information must be portable and accessible to meet the needs of organizations, individuals and society as a whole. Providing this portability and flexibility is also a key to remaining competitive and spurring growth in the information society and digital economy. Giving the data subject back the control over his personal information will ultimately also create new and more balanced relationships between individuals and organizations.

TAS³ enables an infrastructure of trust, security and privacy to meet the needs of today's more global and mobile society. TAS3's development is geared to compliance with privacy laws and provides for both user control and functional requirements of organizations. TAS³ thus combines security and privacy with technology, policy and law to create a trusted infrastructure predicated on verifiable information governance.

Today, privacy and security needs are being addressed through disparate approaches: Identity management frameworks, privacy by design approaches, model contract frameworks and a myriad other approaches that are neither designed to interact nor managed to enable end-to-end privacy or security. Combining the four elements of the TAS³Trust Network at the design stage of the project enhances and supports more effective user control. Contracts are supported by policies which are in turn supported by the technical architecture that enables user control. Business processes are also modelled to be compliant with the technical architecture and the legal requirements expressed in both policies and contracts. Finally, the logging and audit protocols support required investigatory, compliance and oversight needs.

This deliverable will focus on the contractual and policy framework requirements that will support TAS³ and appropriately bind all parties to their respective obligations, as well as outline the required policy framework that will support technical requirements and needed access and use controls through policies designed and the infrastructure level and implemented at the enterprise/organization level. This multi-tiered approach – harmonizing ecosystem and enterprise level requirements and obligations – allows tailoring and customization to specific roles, needs and technologies. Furthermore, developing the legal and policy requirements in tandem with technology and business requirements facilitates binding the participants to both use the novel architectural elements of TAS³ and to respect of the relevant obligations. Contracts and policies play an important role in ensuring, for example, that

information legitimately accessed for one purpose is not later used for other, unrelated or unauthorized purposes.

The combination of technology, policy, business, and legal requirements is an important step forward in advancing the current state-of-the-art with regards to implementation and enforcement of data subject rights. Users are being challenged more and more by complex, information-based technologies that are being introduced in everyday life on a continuous basis. The data subject's potential lack of knowledge on how these technologies work and what their related information processes are makes it difficult for them to exert any effective control over their personal data. While the EU has put in place some of the most stringent privacy requirements, users may not be familiar with details regarding these rights or knowledgeable of the means through which they can be enforced. TAS³'s approach to provide users with controls that are embedded in a technical architecture, enforced throughout business processes, and supported by appropriate contracts and policies better enable users to understand and enforce their rights.

The TAS³ network also helps to clarify and enforce obligations towards and among service providers. Many well-intentioned service providers attempt to comply with data protection laws, but are often lacking sufficient expertise in technology, law and/or policy. This holds particularly in the case of small and medium-sized enterprises. An Ecosystem approach in which privacy and security are coordinated and designed into the system can be an important step forward in addressing these issues. Consequently, TAS³ presents an approach which may be beneficial for both users and service providers alike.

3 Background

Within the EU, and in a number of other jurisdictions, individuals have legal rights related to the processing of data which identifies them or otherwise relates to them. At EU level these rights are articulated primarily in the Data Protection Directive of 1995 (Directive/95/46/EC – hereafter referred to as 'the Directive'). The Directive sets forth requirements on how information may or must be collected, used, disclosed, stored, secured and retained. These rights and obligations were detailed in TAS³ D6.1.

While well established and respected, the application of the Directive to today's global information flows is presenting an ever-increasing challenge. Compliance with the Directive is typically predicated on concepts of notice and consent. Individuals (Identifiable individuals are referred to as "data subjects") are supposed to be provided with clear notice of collection and proposed use of information. Data subjects must then choose whether or not they wish to provide their consent for the processing of their personal data. This approach has significant limitations however when data is processed throughout extended value chains and passes through multiple organizations. In the following sections we first look at the potential limitations of the current approach, and then proceed with investigating how these concerns may be remedied within TAS³.

3.1 Notice and consent

Notice in online environments is often provided through privacy policies on the websites of the collectors of the information. Those collectors that determine what information is to be collected and how it will be used are referred to as Data Controllers. Those that merely execute the instructions of a Data Controller are referred to as Data Processors.[1] Once notice is provided, data collectors must obtain the clear and affirmative consent of the data subject that they are permitted to use the information in a manner consistent with the purposes specified in the notice. While this seems straightforward in concept, it is much more complex in practice. To a large extent, users have been unable to appropriately exert control over their information. While laws in the EU and other jurisdictions are effective in requiring that care be taken in securing the information and providing rights to the individual in terms of collection, sharing and use of the information, there is no real mechanism to provide effective control over the information, especially beyond the initially transacting parties. Data subjects may have reasonable confidence that the information directly collected by a company for a specific purpose is safe with that company. However many services require that information be passed along a value chain comprised of other companies, some even residing outside the jurisdiction of the initial collector. Exerting control beyond the direct collector of information absent a Trust Network like that proposed in TAS³ is difficult. The current legal frameworks were drafted before the need to manage the lifecycle of information in an ecosystem or extended value chain became readily apparent.

[1] A more complete set of privacy definitions can be found in TAS³ D6.1 and in annex 3 of this deliverable.

Currently, exercising control over the information requires a laborious and sequential oversight of each relationship. Control in such relationships is difficult to execute by data subjects because of inequalities of knowledge and experience related to information of a specialist nature (medical, legal, etc.) as well as their lack of knowledge related to the design and operation of systems. Furthermore, there are limitations in how effective the oversight of the relationship can be when information is transferred across a value chain, sometimes unbeknownst to the data subject. Organizations collecting and using the information also face challenges. Even though they have more knowledge of types of information and system operation, that does little to minimize the overhead and burden of providing security and privacy without compromising either organizational or user functionality or trust.

The technical details of today's backend systems and the potentially global value chains they support have grown ever more complex. Part of the innovation behind the TAS[3] project is to apply technology supported by and coordinated with policy and legal frameworks at the infrastructure level to create a shared and more efficient architecture for enhanced security and privacy. Technology has created both the potential and expectation that relevant and useful information shall be available across the lifecycle of these new relationships. Previously, this information, while about a specific and identified person, was treated as if it was the property of the organization collecting or using the data. TAS[3] enables information to be functional and accessible within a user-centric framework.

3.2 Accountability and accountable systems

As was detailed in TAS[3] D6.1, privacy experts are now looking at concepts of accountability and transparency to supplement notice and consent. Accountability is a concept promoted in the OECD Data protection Guidelines; PIPEDA, the Canadian Privacy Act; and the APEC Privacy Principles, which are focused on assuring that obligations flow with the data. The Accountability model of the Canadian Privacy Act for instance places the onus on the transferor of information to assure that the data recipient has the capacity to process or otherwise treat the information in a manner similar to that prescribed in Canada.

In the EU, Notice and Consent are implemented under an adequacy model. This model requires that in instances where organizations from non EU-countries will receive information on EU data subjects, they must be found to support an "adequate protection of data" prior to transfer. While accountability is not strictly defined in the Directive, it is addressed by requirements such as notice, access, notification to supervisory authorities, liability etc.

While both models address a similar set of data protection principles, the former accountability model may provide for a level of flexibility which is more naturally adaptable to today's information flows. Adequacy requires a government-to-government finding, while accountability enables a multifaceted approach to compliance, potentially including elements of contractual, technology, policy and business requirements.

The preceding analysis only provides a comparison between two legal framework models. There is however also a more nuanced analysis of accountability, which is even more important to our current analysis. In today's global information society, the amount of information that is accessible through Internet-based systems – search engines, social networks, blogs, and archives – implies that vast amounts of personal information are accessible to a large number of entities. Use of that information cannot effectively be controlled through a notice/consent/access methodology alone. Furthermore, the increased complexity of systems and information flow dramatically increases the challenges towards oversight by data protection authorities. A number of DPAs are currently evaluating the complementary role that accountability systems might fulfil. Accountability concepts, and their incorporation into systems, are part of processes in the OECD as well as initiatives developed by the Irish and Spanish Data Protection Authorities.[2] It was likewise an area of explorations and discussion in a recent Rand Study Commissioned by the UK Information Commissioner[3]. The then UK Information Commissioner provided this informative diagram (Figure 1) in his discussion of accountability at the recent EU Data Protection Commissioners' Conference in Edinburgh[4]:

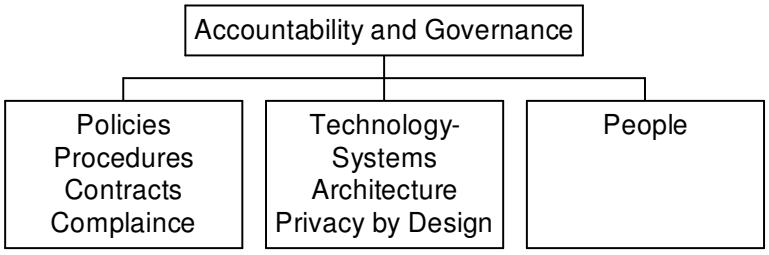


Figure 1
Accountability and Governance Model Proposed by Commissioner Thomas

Commissioner Thomas correctly highlighted the multiple elements needed to address accountability. These elements are essentially the same elements that are incorporated in the TAS³ governance model: Policies, Procedures, Contracts and Technology. As we look at today's challenges in technology and systems design, it also is useful to consider this description of how to address security and

[2] See TAS3 D6.1 at section 4.
[3] N. ROBINSON, H. GRAUX, M. BOTTERMAN & L. VALERI, 'Review of European Data Protection Directive, TR-710-ICO, for Rand Europe, May 2009, available at http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf. 2009, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf
[4] Thomas Richard, Data Protection in the European Union, Promising Themes for Reform, European Privacy and data Protection Commissioners' Conference, Edinburgh, 24 April 2009 http://www.privacycommission.be/nl/static/pdf/seminarie-privacyrichtlijn/data_protection_in_the_eu_nl.pdf.

privacy concerns in a recent Sun White Paper of Engineering for Data Protection and Accountability:[5]

> *Addressing today's security and privacy challenges can be summarized as getting the right data to the right people at the right time. Security and privacy challenges can also be summarized as preventing unauthorized access throughout the data lifecycle. This implies simplifying access for the right people while making access by the wrong people cumbersome, expensive and easily detected. Success in this endeavor depends on a combination of people, processes and technology. Technology is designed to facilitate authorized access in a repeatable and auditable fashion, and the systems themselves can be designed to promote data governance in a way that enhances accountability for the organizations that build and manage them.*

Building information accountability models into system-based controls on use and disclosure are an important step in re-empowering data subjects to control their own information. Uses of trusted services providers, reputation engines, policy mediation and decision support tools that can validate credentials and provide trustworthy information, can assist data subjects in choosing good service providers and engaging in trustworthy transactions. The ability to have systems that validate credentials and information also enable organizations transacting with data subjects to rely on the information they are receiving with a much higher degree of confidence. These accountable systems and architectures help restore trust in online environments and help assure information availability, utility and integrity.

3.3 User-centricity

User-centricity is an essential element of TAS³, but is a concept rife with nuance and subject to different interpretations. The majority of today's systems, policies, processes and contracts are designed in a provider-centric fashion. They are defined with essentially only the providers' business processes, models and technical needs in mind.

User-centric systems, on the other hand, are designed to enable users to regain control over their personal data by supporting user controls and dedicated architectural elements. TAS³ goes beyond traditional (mainly technical) user-centricity approaches by also enabling user control in contractual tools and organizational policies. This holistic design and development approach creates a user-centric ecosystem, as opposed to merely a user-centric implementation of technology.

[5] Sun Technical White Paper, 'Engineering for Data Protection and Accountability', May 2007, available at http://www.sun.com/software/products/identity/wp_eng_data_protection_accountability.pdf.

User-centricity is referenced in a number of FP7 projects, but perhaps defined most simply in PERIMITER[6] (a project related to networking), as "putting users in the center". For communications networks, this means replacing the dominant interests of the operator with those of the consumer. This user-centric design concept has been extensively discussed in the context of user-centric identity management systems (IdMS). Two major notions of user-centric IDM have emerged: relationship-focused and credential-focused user centricity. As is implied in the names, the former focuses on providing user control over relationships while the second focuses on user control over credentials.[7] TAS³ is designed to enable elements of user control over both. Giving the user back the control over his personal information will also reshape the relationships between individuals and organizations.

TAS³ enables user-centricity through both the trust services and privacy controls that users can exert through designated interfaces, as well as via the system controls which are designed to both implement and favor the rights of the user. This user's interface will provide him/her with a so-called 'dashboard', which enables a complete view of his or her personal data (digital identities, credentials etc) within the network. The same interface will also enable users to access information concerning types and reputations of services providers. These user controls provide for an enhanced transparency, which is relevant both to compliance and accountability. Those technical controls are supplemented by contractual obligations, which all organizational participants will be bound to. As will be described in further detail later in the deliverable, those obligations also exist in relation to overall policies that apply to all participants, to a specific organization's policies, and to the transactions themselves. In TAS³, user-centricity is thus both a project objective and built into the design.

The following table summarizes some of the most important elements of user-centricity in TAS³; a more detailed description of these controls is provided in section 6.2.2 and annex 5.

Control	Benefit
Services are user initiated – pull system • Services are identified and verified as part of architecture and process • Consent is a default condition of the system	User initiated processes • Process functions can be identified and mapped / limited needs • User consent required
User can use pseudonymous / anonymous credentials	Expands user options related to risk mitigation and disclosure

[6] PERIMITER, 'User-centric paradigm for seamless mobility in future Internet', available at http://cordis.europa.eu/fetch?CALLER=FP7_PROJ_EN&ACTION=D&DOC=215&CAT=PROJ&QUERY=011aa1a082b8:914a:460f8894&RCN=86612

[7] Bhargrav-Spantzel, Camenisch, Gross, & Sommer, User Centricity: A Taxonomy and Open Issues, DIM ,06, November 3, 2006, Alexandria, Virginia, USA, http://www.akiras.de/publications/papers/BCGS2006-User-Centricity_-_Taxonomy_and_Open_Issues.DIM_06.pdf

• Make decisions as to which credentials to use and when to re-identify	
User can define privacy preferences related to: • Categories of Recipients • Processing permissions • Purpose • Time of availability • Additional controls; depending on the type of service	Privacy controls accessible through usable interface, which may include a policy definition tool. The ability to set these preferences which are enforceable throughout the architecture, enable users to have greater confidence that their preferences are respected across complex value chains.
User is provided with policy management, discovery and negotiation tools and has access to reputation services. • User has ability to provide feedback into the system related to service reputation etc.	User is provided with more and better information to inform decisions, selection tools to help narrow decisions and execution tools to help take action. • User benefits from community use of system and experiences across service providers
User is provided with ability to verify processing operations upon his personal data after the fact through dashboard interface	Enhanced transparency towards user – user becomes integral part of the accountability model

Figure 2: Summary Table of TAS³ User-Centric Functions and Benefits

4 Testing the thesis: Employment and Health

TAS[3] creates a generally applicable, secure yet adaptable technical infrastructure that enables the processing of distributed personal information. Information, however, needs to be considered in terms of the context and processes that are part of its lifecycle. Data is collected; stored; distributed; archived, possibly in anonymized/aggregated form and then either deleted or refreshed. Those functions, which may be played out in a number of iterative steps, comprise the information lifecycle.

The functionality of TAS[3], likewise, needs to be tested in some real information lifecycles. To that end the Architecture will be demonstrated in pilot applications related to two topics, one for the creation and maintenance of electronic employability portfolios and the other for electronic health/medical records. New social norms related to work, flexible job functions, more routine dislocations and changes in the workplace environment coupled with the nature of education, skills and work related information which must be maintained across a work lifecycle, require greater accuracy, control and portability of records related to education, skills and work. Similarly, greater longevity and mobility of the individuals coupled with advances in health care and complexity of treatment, payment, and operation of medical and health systems has lead to parallel requirements for health records.

In these demonstrator projects, and in TAS[3] as a whole, four main variables that enable user trust are:

- Trust in information – all participants must have confidence in the data;
- Trust in the parties – new tools such as reputation engines and trust mediation services will allow users to have more confidence in engaging in online transactions;
- Trust in the system/governance architecture, - all participants must have faith that the systems and governance mechanisms will be effective in delivering the services and protections specified; and
- Appropriate user control – this may be as much perception as reality, but the data subject must feel that he or she can do more than just participate in the system, they need to feel that they can effectively exert control through accessible and usable tools and interfaces.

The contractual and governance framework is essential to leveraging these variables to enable the desired trust infrastructure. Since the contractual and governance framework also requires testing, this deliverable will focus on the demonstrator projects, but the intention is for the concepts to remain generally applicable to infrastructure deployed in other disciplines or jurisdictions.[8]

[8] It should be noted, however, that sectors and jurisdictions have variances in their legal requirements, which must be addressed in the contractual framework as applied.

4.1 Complexity of information flows

Technology provides great strides in securing and assuring trust during the course of a transaction between identified parties. But as our lives, jobs, transactions, and social interactions become more complex we are no longer dealing with pure one-to-one relationships. Transactions today can involve multiple organizations that make up a value chain. Transactions may also operate across numerous value chains. There is a lack of easy predictability as to who will need to be involved in a potential transaction or interaction. This is even more acute when subcontracting takes place, as the ultimate consumer is not necessarily aware of all the service providers in the chain. When the consumer is purchasing prescription medicine at the drug store the threat may be limited because the user can rely on more common and tangible ways of evaluating her relationship with the vendor and his trustworthiness. These familiar guideposts are not available when she is accessing a personalized electronic health service, where she does require supplemental information on the service provider and other entities that are given access to her personal data in order to make an informed decision.

Lack of predictability is also caused by the uncertainty of the data subject's future location or condition. While a routine checkup may be within the scope of prediction, when a person breaks an ankle on a flight of stairs, who treats them and where is not predicable. Therefore who is given access to the user's personal data may not be known in advance, yet the patient still needs to provide consent to the processing performed by these "unknown" parties. In the employability domain, whilst there may be some quantification and predictability of potential employers for a person with a defined skill set in a specific region, there is much less predictability related to the worker who is laid off or the one required to move to care for an aging parent.

4.2 The Data Subject Perspective

In many cases today's data subject is only really aware of collection and processing being undertaken by the direct collector of the information – the organization with which the individual is transacting business. As value chains and technologies become more complex and involved, it becomes far less realistic that data subjects shall be able to understand or track the processing, security, information flows and parties involved in any such transaction. The TAS^3 architecture provides user interfaces and system tools to assist the data subject in creating policies to deal with these complexities as part of the solution. The use of a contractual framework designed to complement and support the technology further provides assurance that information will be used in an accountable manner that is consistent with the preferences the end-user has specified and compliant with the applicable legal requirements.

4.3 Solution approach

Despite the greater number of entities and greater complexity of the interactions, systems must be able to provide the information needed to accomplish the transaction and must do so in ways that:

- Allow individuals to make choices and exert appropriate controls;
- Allow individuals to provide their consent for the use of their PII;
- Assure that uses of information are consistent with the legal obligations of the relevant jurisdiction; and
- Provide an architecture and governance system that has the transparency and accountability to engender trust.

Technology, in the form of the TAS^3 Architecture, will significantly enable trust, but cannot do so without an appropriate governance framework compromised of a contractual and policy framework. This is the case for a number of reasons. The first and most practical reason is that it's inefficient to try to place all of the burdens on technology. A multifaceted approach of technology, policy, practice and people, supported by audit, oversight, and accountability better distributes responsibilities across functions and uses checks and balances to assure that compliance exists. This is especially true in the more complex environments that include multiple intersecting or sequential value chains. In those cases there is no centralized point of control, as there is within an enterprise that controls the infrastructure and related policies. In the case of a unitary value chain, there may be a large enough player (e.g. a university or government entity), which can require other value chain participants to adopt a technical infrastructure and relevant policies and procedures. In the case of multiple value chains, or ecosystems, there is generally no central point of control that can dictate infrastructure or policies.

5 Organizational models

5.1 TAS³ structure

TAS³ is focused on developing a technical architecture that is implemented through appropriately modelled business processes and supported by an appropriate contractual and policy framework. While the demonstrator projects provide a good basis for testing these elements, they involve known entities with pre-existing relationships. In order to assure the flexibility of the framework and its application in less defined environments, the consortium has outlined the potential business models for large-scale deployment of TAS³.[9] The central underlying notion is that a number of entities will collaborate to provide TAS³-enabled services. This group of collaborating entities as a collective is referred to as a 'Trust Network' (TN). The following entities are currently presumed to be involved in such a Trust Network:

- **Data Subjects**: also referred to as individuals or end-users
- **TAS³ Participants** including:
  - Service providers and service requestors of application-specific services (e.g. employability ePortfolio, eHealth Personal Health Record);
  - Service providers and service requestors of Trusted Third Party services (e.g. Credential Validation Services, Reputation engines, Identity Providers, intermediaries)
- **TAS³ Governance Entities**, which may include:
  - A top level Trust Guarantor, and/or
  - A Trust Network Governing Board (consisting of stakeholders, including user representatives)
  - In a number of cases, governmental entities may also be involved.

As far as organizational models are concerned, the simplest scenario would involve a powerful central entity that already has the respect, authority and position to anchor a Trust Network. Governments and large hospital networks might be in a position to operate in this fashion. Absent a strong entity to anchor trust, a Trust Network may come into existence either through simultaneous agreement of a substantial number organizations acting as cofounders (Trust Consortium), or through a Trust Consortium Convenor (TTC). A Trust Consortium Convener is an entity with technical or administrative skill but insufficient authority or funding to be a natural anchor and unable to find enough entities of the proper type and stature to be cofounders. The TCC will define the architecture and commence its development while continuing to find appropriate cofounders or other anchors to take over.

[9] The document outlining the TAS³ business model was initially incorporated in D2.1 (Architecture) as Annex D (v17). It is currently being developed further and in its next iteration will appear as a stand-alone document (D11.10).

The parties to a Trust Network, referenced above, only represent one of many potential Trust Ecosystems. In fields of employment and health we are likely to have multiple ecosystems.

Regardless of which organizational model is adopted, the interactions among the participants to the Trust Network will need to be co-ordinated in some fashion in order to ensure compliance with both business and data protection requirements. A review of federated communities is informative to see how these issues are managed under these approaches, and is provided in the following section.

5.2 Federation and communities

Federation concepts are being applied in groups, such as the Liberty Alliance[10] and the credit card industry, to create trust infrastructures around identity management and assurance. Specifications such as the Identity Governance Framework (IGF)[11] are additionally being developed to better deal with technical interoperability requirements across an ecosystem. Groups like Liberty have also considered the contractual and policy requirements of the ecosystem.[12] The credit card industry uses an identification paradigm since based on government identifiers and historical transactional information that can be used for identity verification. From a TAS[3] perspective, the most interesting aspect of the credit car industry federation does not come from identity management, but rather the contractual framework, which binds obligations across the various participants.

5.2.1 Liberty Alliance Organizational Models

Liberty Alliance has developed approaches to policies and technical infrastructure that are predicated on the existence of federated groups of entities which are bound in so-called 'Circles of Trust'. They have also considered how Circles of Trust can help organizations comply with EU data protection requirements. These Circles of Trust are an informative way to look at methods of organizing within and across ecosystems. At a high level, the basic models of federation fit within the continuum of the potential organizational models outlined in the TAS[3] Business model: Centralized Model (Trust Anchor), Collaborative Model (Trust Consortium), and Consortium Model (Trust Consortium Convener). These models, set out in Figure 3 below, were most recently referenced in collaborative work between the Ontario Privacy Commissioner and the Liberty Alliance on Federated Privacy Impact Analysis.[13]

[10] http://www.projectliberty.org/

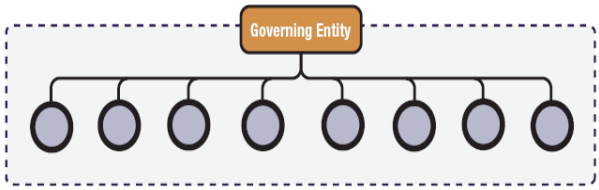
[11] www.projectliberty.org/liberty/content/download/3500/23156/file/overview-id-governance-framework-v1.0.pdf. – See Annex 2 for a mapping dataflows/functions.

[12] www.projectliberty.org/liberty/content/download/2962/19808/file/Liberty%20Legal%20Frameworks.pdf

[13] A. Cavoukian, 'Building Privacy and Trust-enabled Federation: Federated Privacy Impact Assessment (F-PIA)', 2009, 23p., available at http://www.ipc.on.ca/images/Resources/F-PIA_2.pdf

Collaborative Model

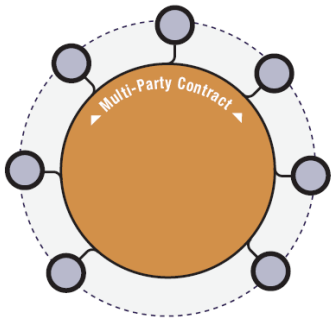
In the collaborative model, a group of founding members or member forms an entity that establishes the rules for the operation and governance of the ecosystem, as well as overseeing day-to-day control of the system.



Described as the most complex of the models of federation, but with the greatest flexibility, this model is paradoxically likely to require the most rigid privacy rules…. These controls are put in place to ensure that the indefinite membership and flexibility may not be exploited to extract PII for inappropriate uses. Assurances of minimum disclosure and strict technical enforcement of privacy guidelines will require audits and accurate user reporting to engender appropriate trust in verifiable privacy. The Governing Entity in the model will be the central authority for privacy compliance.

Consortium Model

In the second model, a small number of founders form a consortium via a multi-party contract that sets the rules and governance for the ecosystem. Based on reasonably autonomous founders, the risk to privacy in the consortium model is that one or more of the founders may have a significantly different privacy model. With respect to the exchange of PII, the contractual agreement by which the federation is formed must be specific as to the common privacy elements.



The privacy rules created for such a federation will need to be clear on the limits of the assertions that can be made for the consortium. It is very likely that the privacy assertions of the whole federation will be the 'lowest common denominator' of the founders. Where consortiums develop from a common industry with a common expectation of practice, this may not present a significant bar, but in cross-industry consortia, this could generate friction.

Centralized Model

In the centralized model, a single founder sets the rules and governance for the ecosystem, and contracts individually with each other member. This approach provides the founder with a significant amount of control, and significantly less control to the other members. The centralized model ensures that data flows through, or with the awareness of, the single founder, which implies that privacy assertions can be made and verified by that organization. This architecture also allows for the possibility of the single founder incorporating the data protections identified and afforded by the privacy rules to be contractually incorporated into the federation, in a highly uniform manner

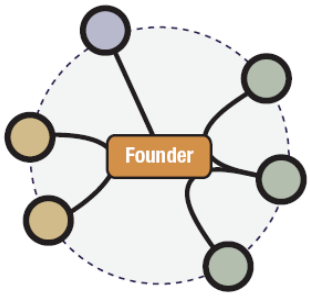


Figure 3: Liberty Alliance Federation Organizing Models[14]

5.2.2 The Credit Card Industry Organizational Model

While Liberty's work on the IGF and contractual framework are informative; the largest scale example of a working federated organizational construct exists outside of Liberty, namely in the credit card industry. The credit card industry has demonstrated a massive scalability to technology, policy and contract obligation. While everyone understands that they sign cardholder agreements, the importance of that contractual underpinning may not be evident.

Credit card networks have detailed policies related to payments, funds clearing, cardholder rights, and charge-backs to merchants, just to name a few. They also have sophisticated back end networks to verify, validate, authenticate and audit transactions. These functions are supported by some of the most advanced fraud detection technologies on the back end to find both aberrant patters of card use that might indicate fraud as well as potential issues related to internal controls. Beyond that, the major card companies/associations: AMEX, Discover, JCB, MasterCard and Visa International collaborated to develop the Payment Card Industry Data Security Standard (PCI DSS: see Annex1). The have also develop similarly detailed standards related to payment applications[15] and PIN Entry devices[16].

These PCI-based standards help the card industry define the infrastructure that all players except cardholders, will need to consider and they develop and deploy infrastructure.

The credit card companies address end-user needs through security programs like Verified by Visa as well as security and identity theft training. Other card

[14] *Ibid*, 14.
[15] See https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
[16] See https://www.pcisecuritystandards.org/security_standards/ped/index.shtml

companies like American Express are looking at digital signature technologies and encryption, which are used in the Blue Card and Express Pay offerings. All of these features inure to the benefit of the consumer with enhanced security with either little burden and, in some cases, even enhanced convenience. The combination of these end-user controls coupled with sophisticated backend systems and enhanced merchant, vendor and support requirements under the PCI standards helps create greater trust in the infrastructure and enhances compliance with numerous legal requirements.

5.3 Path forward

In the preceding sections, we have reviewed a number of existing implementation models as well as possible organizational models for federated environments. As we explore the contractual framework model and begin the contract drafting process, we need to focus our activities on a more limited number of models.

Discussions within the TAS³ project revealed that there are two main organizational models for TAS³: a centralized and a distributed model. Despite the fact that the names seem to indicate significant differences in the models, the differences are more a matter of degree than completely distinct models.

In essence, entirely centralized (all functions and control in one entity) and entirely distributed (no centralized functions or control whatsoever) models exist as the two end points of a continuum. It is highly unlikely, if not impossible, that either extreme could be implemented. Even within an individual organization some centralization and some distribution of controls and function inevitably takes place. The centralized and distributed models that we will discuss in the subsequent paragraphs are neither entirely centralized nor entirely distributed, but rather represent the likely implementations of TAS³, taking into account the functionality it supports.

In the centralized model, there is a strong central entity which dictates the architecture, policies and contractual framework of the Trust Network towards all participants. This central entity also manages and operates the technical platform which supports the interactions among the participants. It decides in advance which types of organizations shall be allowed to become part of the Trust Network, and which services shall be offered. The central entity also oversees compliance and each participant is answerable to this entity. As indicated earlier, governments and established health networks might have the ability to organize their Trust Network in such a manner.

In the distributed model, the TAS³ technical architecture is implemented and operated in an entirely distributed environment– each participant operating those parts of the architecture which are relevant to its operations. The Trust Network is relatively ‘open’: any organisation which is capable of satisfying the criteria of participation is eligible to join and offer its services. However, even in the distributed model there are several functions which are centralized. For instance, functions like intake, complaint handling, and oversight need to be centralized in order to provide a certain level of continuity and trustworthiness of the Trust Network.

The most distinguishing feature among the centralized and distributed model is of course the level of centralization of operations. The choice for either model shall be premised largely upon the nature of the relationships of the participants to the Trust Network. The more organizers and participants resemble a consortium of equals, the more likely functions and controls will be distributed. Where a strong player exists who has the ability to impose its rules upon other, relatively smaller entities, the more likely that functions and controls will centralize.

The centralized model obviously lends itself to assure high levels of trust. There is great uniformity and a high level of assurance that the policies (which are defined centrally) are followed. The strong direction of the core will likely implicate the central entity as co-controller for data protection operations and entails a higher exposure to liability. In the distributed model the 'administrators' of the Trust Network also carry a certain liability exposure, but the organizational responsibility of each participant is tailored more to its actual role with no single entity acting as a guarantor in relation to other participants, except to the extent of shared responsibilities . The distributed model relies primarily on commonly agreed reference architecture to promote assurance in the security and trustworthiness of the network. This assurance is conditioned on the proper implementation of the architecture and model policies by the participants. Distributed models will therefore also need to have some more central processes of assurance review, some of which may be delegated to a central authority or trusted entity.

Contracting paradigms in the distributed model were thought to be more complex and challenging. Because the distributed model is more complex, we expect that it will be easier to derive the contractual framework for the centralized model once the framework for the distributed model has been clearly established. Thus the first contractual framework will be drafted for the distributed model.

6 Developing a Contractual Framework

6.1 Fundamental elements of the contract

In order to develop a contractual framework four familiar terms must be established: “Who”, “What”, “Where” and “How”:

- The “Who” is all of the participants including the end-users, service providers/requestors, trusted service providers and Trust Guarantors,
- The “What” refers to the nature of what is being bound, or more accurately what is each party obligated or entitled to.
    - A term inherent in every contract is also the “what if”, which refers to needed flexibility and contingency planning. This can also be considered as methods of reducing and addressing foreseeable risk. The “what if” factors will be considered in the iterative development and operation of the demonstrators. For example, break glass functionality would be a 'what if” scenario.
- The “How” refers to the method and operation of the contractual framework.
- The “Where” refers to the jurisdiction(s) involved. For the purposes of this draft of the contractual framework, the where has been limited to the countries of the EU, more specifically those where demonstrators will take place. No further review of issues related to ‘where’ will be undertaken in the current draft.

6.2 Contract definition process

The start of any process definition has to be an understanding of the main and ancillary purposes of a system. Defining the actors, their interests, rights and obligations is a critical second step, which are defined in general in the Architecture (D2.1), but more specifically in the Pilot projects descriptions (D9.1). Thus the first two steps comprise the definition of the needs of the organizations and users. From there, understanding their interactions in terms of data flows and roles completes the foundation scoping which is required to develop a contractual framework. Again, these are documented in the architecture and pilot descriptions, though from a contracting perspective we will address types of service providers rather than try to define the possible universe of services and providers. This step then takes into account employees and other actors by associating them to roles in the ecosystem.

Those roles will be critical in assigning the rights and obligations they have within the context of data flows. This foundation is needed before system controls and the overall governance framework can be specified. They in turn need to be defined before allocation across technology, policy and contract can occur. An obvious but unstated step in the process has to be an understanding of the possible role and functionality of each of the technology, policy and contract elements. This step can happen at any time as an organization goes through a number of these processes. This step will be part of the learning process that

should be captured at the system level to assure that it is preserved beyond personnel turnovers.

We caution that the actors, flows and roles are a foundation that is likely to change over time so that there needs to be flexibility and continuous or periodic evaluation and redefinition built into the system. The addition of new actors, the evolution of roles and the changing needs of the system are part of this change requirement. For a framework to be effective and to better understand how to structure the "How" and "What if" a dataflow map – a compendium of information flows across parties and possibly jurisdictions with associated rights and obligations related to the information flow – is needed.

6.2.1 Contract and policy hierarchy

The above are standard process steps in developing a contractual framework. The process has highlighted three important facts in determining how to organize the contract and policy frameworks:

1. One of the main purposes of TAS³ is to provide the user with effective control over their personal data across the TAS³ Architecture. Data subjects will interface through a TAS³ client, with policy definition and identity and data management tools. The TAS³ client will likely be in the form a 'dashboard' which is provided by a trusted service provider of the user's choice. This dashboard provider is also likely to host the personal data store of the user and have the ability to initiate audits related to the use of personal information. All entities that come in contact with data subject information, must respect any policies (instructions) the data subject has provided, and abide by those set forth in the general terms & conditions.
2. Certain information on service providers (privacy policy, reputation) needs to be disseminated in order for data subjects and certain providers of trusted services (reputation engines) to do their jobs
3. Service providers will interact with each other and exchange information in providing services to data subjects. They may also require assurances related to security or otherwise place policies and restrictions on the processing of the information.

With these elements in mind it is clear that all parties to the TAS³ architecture need to be contractually bound. As in the credit card situation that will require a contract at the architecture level which we will refer to as the Ecosystem contract. The Ecosystem contract creates the baseline of obligations and context for binding specific choices and negotiations among the parties both directly involved in negotiation as well as relevant organization that access, control, process or store the information. The Ecosystem contract will be completed in counterpart forms. In the credit card industry, the cardholder signs a user agreement, the merchant a merchant agreement, etc. Where the role of a participating organisation will be static then an additional role-based contract will be executed that addresses the general rights and obligations of that role. Policies are also defined at the Ecosystem level addressing issues like privacy, security, and, access and use controls for the various service providers.

Credit cards systems however don't allow for cardholders or merchants to create new policies for each transaction. This is an essential element of TAS³, so contracts must also exist dynamically at the transaction level. These contracts-on-the-fly are also essential to dealing with service providers that might have multiple roles and may at times be controllers of personal information, while at other times mere processors. Finally, TAS³ policies may also be expressed in technology – sticky policies, and policy mediation tools. The outcomes of these technical processes must be binding on the organizations receiving the policy instructions and need to be supported in contracts that address the technical level. The policy framework must likewise recognize and incorporate the technical level of policy definition, mediation and management.

This the resulting hierarchy is a three-tiered contractual framework – Ecosystem, Transaction/Role and Technology contract levels and Policy Frameworks to support the Ecosystem and Technology level issues.

6.2.2 User-centricity and process optimization

Because TAS³ is designed from the outset in a user-centric manner, TAS³ has a significant focus on the needs of the individual users, as they will be the main source of the overall controls applied across data flows. As the design of the system will occur before users can specify controls, the established legal rights of individuals (specified in D6.1) will form part of this needs analysis. Other possible needs and desired functions will be obtained by reviewing demonstrator projects, gaining intelligence on requirements from the rich and diverse experience of partners and through outreach to users and organizations representing user interests. Even though needs may be defined from the user out, requirements will flow down from the Ecosystem/Transaction level with increasing granularity required to cover operations. The contract process must operate across tiers, as individual roles are likely defined at the organization level while some rights may be associated at the community or Architecture level.

The TAS³ contractual framework is designed in conjunction with participant policies and technology implementations to assure an integrated and cross-supportive structure. To that end, part of the requirements analysis was developed to better understand how technology contract and policy could be more interactive. In order to optimize both user control and the proper allocation of functions across the Trust Network, we must continually consider:

- What issues can be addressed adequately through technology?
- What issues, which are being addressed in technology, would still benefit from the support of binding contractual obligations?
- What are issues that could not be completely addressed by technology and need to be accommodated as needed in policy and contract?
- What technology functions are need to support the oversight of and compliance with the contract and policy requirements?

6.3 Governance and architecture

Because of the strategic nature of the relationship between contractual framework and the technology, policies and process, it is important to understand the capacity of technology to either enforce some of the contractual process or otherwise support it. The other side of that concept is the importance of knowing the limitations of technology in terms of feasibility, capacity and technology to know what functions are best allocated to contracts or policies.

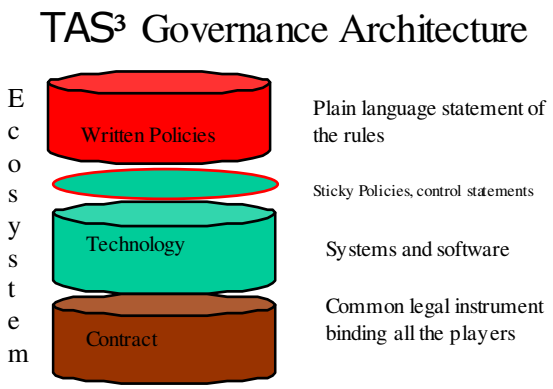


Figure 4 – TAS³ governance architecture

The architecture diagram in Figure 4 above sets out the 4 main elements of the Trust Network, which comprise the governance architecture. Each of these elements has distinct functions but needs to interrelate with the other three to form a whole. In most cases, technology is the main focus and has become the basis of privacy or security by design movements. TAS³ has opted for a more collaborative and broader-based design from the outset. Thus written policies may dictate requirements of technical infrastructure and security policies for participants, which help TAS³ extend and harmonize security requirements across participating entities. The technology architecture requires the use of tools that enable data minimization and audit two functions that are required for compliance and oversight. Sticky policies carry instructions from data subjects on the use or disclosure of information; these are part of the hard wiring of user controls. Finally the contractual framework binds the participants to their obligations from the need to use the TAS³ architecture elements, to supporting the binding effect of sticky policies.

It is important to understand that in the TAS³ architecture there is the concept of sticky policies which operate as small instruction steps to enforce policies and can be seen as creating 'mini' contractual bindings. In both cases these sticky policies will create some challenges in the application of contractual frameworks as the exact lineage of these sticky policies to existing legal regimes is more by example and correlation that in statute or case law. The challenge is less in the actual binding, since that will be achieved through the ecosystem contract, but rather the situation where an end-user claims the negotiated outcome was not consistent with her specified preferences. There is little experience in courts to demonstrate the operation of the system and legal chain of obligation through the

operation of the application. FIDIS (Future of identity in the Information Society)[17] has done interesting work in exploring concepts of contracting and personhood and the need to adapt the traditional doctrines of contract law to accommodate software agents and other machine-to-machine interactions and negotiations.[18] Furthermore the interrelation between contracts and operational policies of the organization or infrastructure need to be defined as the project progresses.

An interesting contracting model to apply to TAS³ is the Master Services Agreement (MSA). MSAs are used by large commercial enterprises that wish to simplify contracting for multiple services/projects from one or many vendors. In the B2B commercial context, companies often enter into a Master Services Agreement that creates the overall contractual relationship between the parties but then execute work orders pursuant to the MSA detailing specific functions and requirements. In many ways the TAS³ architecture will utilize some of these techniques – developing a master agreement at the Architecture/ecosystem level supplemented by other agreements at the more transactional level that provide relevant details. An example from the education/employment demonstrator could be developing mechanisms to incorporate relevant Accreditation of Prior Learning requirements or the 'Common European Principles for the Validation of Non-formal and Informal learning'. In the context of healthcare, enabling choices related to access to records, which are by nature very context specific. Technology is essential in supporting and executing these requirements, but the contractual framework is necessary to create the binding that enables and facilitates remedial action to be taken against parties who fail to meet their obligations.

Interesting work in this area also took place within the PRIME project, with their development of so-called "Drag and Drop Agreements" (DADAs).[19] These 'click-through' agreements were used to provide just-in-time notice with a sufficient level of detail to tailor data to need, whilst promoting data minimization. Developing a symbol-based system where data elements could easily be associated with recipients through a drag and drop functionality further supported usability. This approach enabled greater transparency for and understanding by the user. We will refer back to this approach as we develop the dynamic, transactional contract-on-the-fly models. We hope to further enhance this contracting model by testing the feasibility of developing a technologically enabled model. Our current direction of exploration uses the concepts underlying object based programming and service oriented architectures to develop a repository or reusable contract elements associated with business functions and role attributes. Supplemental contractual addenda could be assembled on-the-fly and presented for signature/acceptance prior to a service providers participation in a transaction.

[17] See http://www.fidis.net

[18] See FIDIS, Future of Identity in the Information Society; Bridging the accountability gap: rights for new entities in the information society, D17.3 at 28-37, April 28, 2009, http://fidis-wp17-del17.3-rights_for_new_enetities_def.pdf

[19] See PRIME, Privacy and Identity Management for Europe, Framework V2, D14.1.b at p. 53, July 2006, http://pub_del_D14.1b_ec_wp14.1_V1_final.pdf

6.4 Defining the "Who"

6.4.1 Actors

The essential elements of any contract are the parties - both those that sign and those that may be obligated under the contract. An organization, for example, may sign a contract that requires it to perform certain services as part of the engagement. The employees of the organization will of course perform those services. The person who engaged the organization for services can rely on that contract alone, while the organization needs to have separate contracting documents with its employees, which bind them to performing services for the organization as directed by management or though appropriate processes; often in the form of work orders.

As we pointed out in the introductory examples, the TAS^3 infrastructure creates a challenge in identifying the "Who" seeing as the circumstances in which data processing will be requested or required will not always be easily predictable. Thus in identifying the parties to a contracting framework as opposed to a transaction, one needs to identify potential signatories and possible parties impacted by having rights or obligations. While the specific terms of a contract may need to be narrowly tailored to the facts of a situation a contractual framework that is deployed at the ecosystem and infrastructure level needs greater flexibility. After identifying possible parties from individuals to the various types of organization it is useful to categorize them in a way that rationalizes them into a more manageable group. The categorizations are usually based on common interest, function or type with further grouping based on similarity of obligation or right.

An important organizational and classification concept comes from privacy laws, which create differing obligations based on the service provided and nature of the relationship. Under the Directive, a data controller, i.e. the person or organization deciding what information to collect and how to use it (the "purposes and means" of the processing) has a different level of obligation compared to the data processor that merely takes the needed actions to execute the controller's instructions. Within TAS^3, service providers are not only divided into 'controller' and 'processor' categories, but, from a contractual perspective, we will need to be able to differentiate between controllers and processors to properly associate obligations. This issue will be addressed in further detail in the following subsection.

Transacting parties will be comprised of service providers (controllers and/or processors) and individuals. While correct, this classification does not provide sufficient utility in application and classification of roles and functions. We may wish to consider a more detailed list of categories where their role as controller or processor is used less as a classification tool and more as a way of defining obligations. We should always recall that the same entity might be either a processor or controller depending upon the context of the service or application.

Whether in healthcare, employment or any other setting four main types of parties/roles to a transaction exist:

- The end-user – this is the natural person that is often also referred to as the data subject.
- Infrastructure providers – these are providers and operators of technical system components, which may not have any direct contact with the user.
- Providers of trust services – these can be reputation engines, entities charged with authentication and vetting services, oversight authorities etc
- Relationship-based Service providers – these can be doctors, employment services, or other parties with whom the user has an ongoing relationship

It immediately becomes apparent that with the exception of the end-user, an entity may play more than one role depending on context. A relationship-based service provider in one instance (an organization that provides skills training, for example) may also be part of the trust infrastructure at a later point in time as a credential validator. These classifications are not meant to be permanently linked to parties, but rather inform their obligations based on the role(s) they are playing in a particular transaction or information exchange. From a contractual architecture perspective, specific clauses specifying requirements and obligations may be associated with their role. By grouping these entities according to function it is hoped that we can define communities of interest with shared objectives and commonalities of obligations.

Accommodations will of course need to be made in terms of the requirements based on additional factors. While general obligations across these classifications shall be fairly consistent, details will vary to accommodate the different types of transactions and varying nature of the information. All relationship service providers have obligations of due care and security, but the nature of that care and level of security has to be appropriate to circumstances. Thus the provider that posts a resume as part of a relocation service may be reasonable in taking different precautions to secure information than the medical practitioner exchanging diagnosis information with a hospital. Thus one of the critical features of the contractual framework is appropriately linking the "Who" with the "What".

Before further defining the "what", it is necessary to clarify that while parties may play more than one role, the obligation of all of the roles will be bound by contract. Thus a party acting as a controller will be bound to all the requirements of the controller. From a contractual point of view, these are articulated in the various forms of model contract clauses.[20] It is interesting to note that TAS³ will likely result in a higher level of requirements for both controller and processor than that which is strictly required under the Directive. Particularly, TAS³ will require participating entities to be vetted in order to join a TAS³ enabled system. As part of the qualification and participation into a TAS³ system, organizations are bound by contract at three levels – the general

[20] There are two versions of controller-to-controller clauses ("controller contract"), those promulgated by the EC and those promulgated by a business coalition headed by the International Chamber of Commerce (ICC) and recognized by the EU in 201 and 2005 respectively. The Commission had also promulgated a set of Controller to processor clauses and the ICC is currently in negotiation with the Commission on an alternative version of those clauses.

ecosystem requirements, the requirements of the organization in their specific role and the requirements of the transaction. This vetting process and the requirements associated with it will not only embody the legal requirements of controllers and processors, but go to a level of specification that is beyond most, if not all, of the national implementations of the Directive.

Finally as we consider the "who" the comments of the Commission on the most recent version of the Alternative Model Contract provisions for controller-processor transfers submitted by the ICC[21] is informative. The Commission recognized that transfers might occur among processors. This processor-to-processor flow is gaining in significance as processing becomes more specialized and less tied either temporally or geographically to the location of the data subject. This greater complexity of processing and data flows, further highlights the need to think of solutions at the ecosystem level in the context of a strategic approach that combines technology, policy and contract in a mutually supportive and interdependent manner.[22]

6.4.2 Distinguishing 'data controllers' from 'data processors'

The goal of the TAS³ contractual framework is to ensure that all members of the TAS³ network are appropriately bound to obligations in accordance with the nature of their participation and the processing operations they will perform. This contractual framework must, however, also consider the qualification of participants in terms of the roles provided in the Directive, seeing as these role and their implications are mandatorily defined.

Controllers, as the parties who exert dominion over the processing of personal data, are responsible for ensuring compliance with all the requirements of the Directive which are applicable towards this processing. Processors, who merely execute instructions at the direction of the controller, have a more limited subset of those obligations while the responsibility (and liability) rests on the controller for assuring that they are carried out with proper security and in a manner compatible with the requirements of the Directive (see also infra; section 6).

Given the fundamental importance of the qualification as either a controller or a processor, it is essential to be able to determine in which capacity an entity is performing a particular processing operation. Despite this reality, technological developments since the enactment of the Directive have made it increasingly difficult to apply the distinction between 'data controller' and 'data processor' in practice.[23] Contemporary business models for data processing are structured quite differently than at the time the Directive was adopted, and more and more entities have come divide their respective responsibilities in a way, which does

[21] http://www.iccwbo.org/uploadedFiles/ICC/policy/e-business/pages/Model%20clauses%20Toolkit.pdf

[22] It should be noted that in work related to the revision of the Directive and the e-Privacy Directive, as well as in expert groups exploring the development of international consensus on data protection, questions have been raised about the differentiation and even the continued utility of the controller/processor classifications.

[23] C. Kuner, 'European Data Protection Law – Corporate Compliance and Regulation, second edition, Oxford University Press, New York, 2007, p. 71-72.

not allow for an easy distinction between data controllers and data processors.[24] This is particularly the case when several autonomous (or relatively autonomous) entities collaborate to realize a certain application or service. The distinction especially becomes more clouded the more each participant has a stake in or receives some benefit from the processing. Much may be clarified by investigating the respective business models and practices of each entity involved, but it often remains debatable from what point an entity has sufficient input in determining the 'purposes and means' to be considered a controller.[25]

These issues are amplified by the fact that processing operations are being carried out across increasingly complex value chains. These complex value chains also result in the greater contractual complexity. For instance, it is becoming common for an organization contracting for complex services to not only seek out one implementer or primary service provider who can manage the relationships and make the necessary arrangements with other service providers, but also specifies some of the subcontractors and some of their roles. This is differs from the previous subcontractor model where an integrator was hired and would bring the service providers of its choice to the contract or proposal. In the newer model, the participants to the value chain and their functions may be defined by the entity contracting for the service. Thus the primary contractor has not chosen all of the other providers nor defined all of their functions. This creates situations where the contracting model does not necessarily reflect the control model. The concept of co- and sub- processors in these models becomes much more relevant and, may not fit neatly in current paradigms of contracting or even agency law.

The current difficulties in determining which entity acts as a 'controller' and which entity is merely acting as a 'processor' are caused mainly by the vagueness and ambiguity of the criteria currently set forth by the Directive. When several entities collaborate, e.g. to realize a shared service, the assessment of which entity or entities determine(s) the 'purposes and means' of the processing depends for a great deal on the vantage point one maintains during this analysis. If 'the processing' is considered from a very high level, i.e. as the entirety of operations that are needed to realize a particular service or output, one is likely to reach a different conclusion than if one were to 'zoom in' on the individual processing operations which are performed to realize that service or output. In addition, while the Directive acknowledges that the 'purposes and means' of the processing might be determined by more than one legal entity, it does not articulate any criteria for determining what constitutes a sufficient level of decision-making power in order to be considered a co-controller. Nor does it mention how the structure of their collaboration might affect their respective obligations.[26]

---

[24] Ibid, p. 72.

[25] B. Van Alsenoy, J. Ballet and A. Kuczerawy, 'Social networks and web 2.0: are users also bound by data protection regulations?', Identity and Information Society (IDIS) Journal, October 2009, p. 4-5, available at http://www.springerlink.com/content/u11161037506t68n/?p=352e04236b974655a1271b94c857ff67&pi=32.

[26] See also T. Olsen and T. Mahler, 'Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II', *Computer Law & Security Report*, 2007, issue 23, 419.

The aforementioned difficulties in mapping the roles provided by the Directive to the individual actors who collaborate to realize a shared service also arise in the context of TAS³. In order to enable a more accurate assessment as to when which actor shall be considered to assume the role of either controller or processor, we shall first look at the possible 'degrees' of collaboration, from a data protection perspective, among otherwise autonomous entities. Next we will analyze a number of case studies which may serve to derive additional guidance for interpreting the criteria currently set forth by the Directive.

6.4.2.1 Different degrees of collaboration

Organisations can collaborate with one and other in a wide variety of manners. Their collaboration may be limited or extensive, frequent or sporadic. From a data protection perspective, a limited form of collaboration might involve singular exchanges of relatively small amounts of personal data in light of a particular occurrence (e.g., a transfer of an accreditation of prior learning (APL) by an educational institution to a prospective employer in light of a job seeker's application). A more elaborate form of collaboration might involve sharing of data and other resources on a continuous basis, which may or may not be accompanied by distribution of tasks responsibilities and tasks to achieve a particular goal.[27]

Sharing of information and resources among collaborating entities shall typically be based on mutual agreement, but the basis upon which this agreement is reached may vary significantly. Their collaboration might be driven by a commonly defined purpose, with each entity receiving a similar benefit from their collaboration. The collaboration might also be founded in the respective business models of each participant, with each collaborating entity processing the data and utilizing the resources for its own distinct purpose.

Art. 2 (d) of the Directive implicitly acknowledges that the 'purposes and means' of the processing might be determined by more than one legal entity.[28] However, this provision does not articulate any criteria for determining whether an entity exercises a sufficient level of decision-making power in order to be considered a co-controller. The preceding paragraphs have illustrated that co-operation among autonomous entities, who may in one or more respects be considered to act as data controllers, can take place in many different ways. A controller may have some degree of collaboration with others, without necessarily 'jointly determining the purposes and means' of a particular (set of) processing operation(s). Additionally, one can also conceive of different degrees or levels of joint decision making power among collaborating entities.[29] Olsen and Mahler have provided a useful visual representation of different degrees of collaboration among controllers, which shall act as a starting point for our further analysis:

---

[27] Ibid, 418

[28] Art. 2(d) provides that 'the controller shall mean the natural or legal person, public authority, agency or any other body which *alone or jointly with others* determines the purposes and means of the processing of personal data' [italics added]. See also T. Olsen and T. Mahler, *l.c.*, 419.

[29] T. Olsen and T. Mahler, *l.c.*, 419.

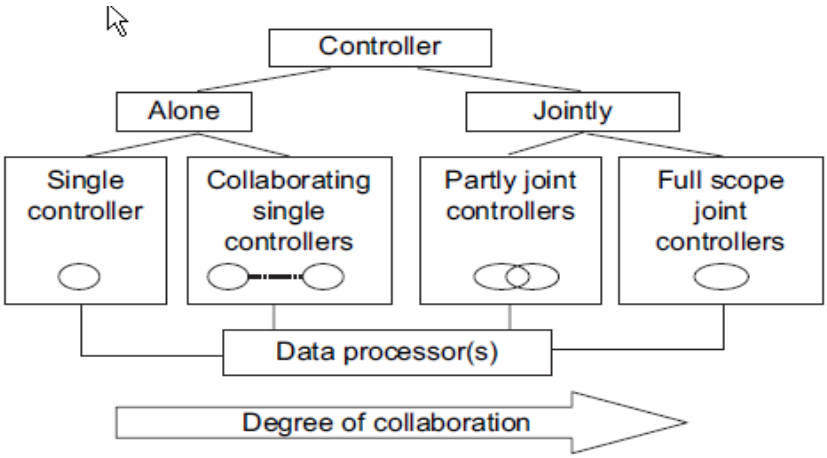


Figure 5: Degrees of collaboration among controllers[30]

a) Single controller(s)

The most straightforward scenario is that in which there is only one entity acting as a controller, without having any relationship whatsoever with other data controllers.[31] This controller might be carrying out the processing by itself, or rely on the services of a processor. Insofar as the latter only acts pursuant to instructions provided by the former, there is relatively little doubt as to which entity is legally responsible for ensuring compliance under data protection law.

b) Collaborating single controllers

In this scenario, there is collaboration among data controllers, but they do not make any joint decisions about the purposes and means of any particular processing operation.[32] These 'collaborating single controllers' might exchange personal information with one and other, but each entity has its own reasons to process the personal information, and each entity independently determines the manners in which it does so. The APL scenario described above will typically fit this model. An educational institution processes personal information relating to students and graduates for its own purposes. It will most often be free to determine how it processes this information and to whom it makes the information available. The employer who receives the information will proceed to process it for its own reasons and in a manner which has been autonomously defined by the latter. In other words, in this model there is collaboration among controllers, but they each determine the purposes and means for the processing of personal information more or less 'in isolation' of one and other.

b) Partly joint controllers

[30] *Ibid*, 419.
[31] *Ibid*, 419
[32] *Ibid*, 419.

The third type of controller collaboration envisages instances in which one or more controllers jointly determine the purposes and means of certain processing operations, while other processing operations are performed separately under the sole control of one controller.[33] An example of this form of co-controllership might arise when several (otherwise autonomous) businesses decide to create a common web portal for purpose of communicating with their (current or prospective) customers. In this scenario the collaborating entities are likely to be considered joint controllers for the processing operations which are accomplished on the jointly controlled portal, but as single controllers with regard to further processing carried outside of the portal.[34] Other examples may include conferences and joint promotions where two or more entities may develop a program/promotion that reflects a joint collection of information from the data subject for the purpose of the conference or joint promotion, but creates an individual relationship between the data subject and each participating organization. This may also include third parties or agents that have facilitated the conference or promotion as processors of information.

It is our working hypothesis that the qualification of partly joint controllers may also be appropriate when two autonomous entities collaborate to realize a shared service; whereby (1) each has separate tasks, but has defined the manner in which it performs them autonomously and (2) these entities are working together to provide a joint service or other functionality and whereby (3) each collaborating entity is aware of the purpose of the processing from the outset.

c) Full scope joint controllers

Collaborating entities shall be considered to be acting as 'full scope' joint controllers when they jointly determine the purposes and means of all the data processing operations involved in a particular application or in the provisioning of a particular service.[35] In this scenario the collaborating entities shall be jointly responsible for compliance with all applicable data protection requirements. An example might be the joint processing of personal data by two or more research institutions as part of a common research project.[36]

Now that we have outlined, on a conceptual level, the main forms of collaboration among controllers, we will proceed with the analysis of a number of case studies so that they might help to derive additional guidance as to how to distinguish between controllers, processors and co-controllers among entities operating under a framework of collaborative agreement.

[33] *Ibid*, 420.
[34] *Ibid*, 420
[35] *Ibid*, 420.
[36] *Ibid*, 420.

6.4.2.2 SWIFT

The Society for Worldwide Interbank Financial Telecommunication ('SWIFT') is a worldwide financial messaging service which facilitates international money transfers. SWIFT was organized in 1973 by a group of European banks that wanted to develop a new method to send payment instructions to correspondent banks in a standardized manner.[37] SWIFT has since characterized itself as an 'industry-owned cooperative supplying secure, standardized messaging services and interface software'.[38]

All kinds of European financial institutions (not just banks) use the 'SWIFTNet FIN Service' for the worldwide transfer of messages related to financial transfers. The types of personal data that are transmitted in these messages range from the names of the beneficiary and the ordering customer, reference numbers, to unstructured text information.[39]

In order to help safeguard its customers against data loss and to facilitate resolution of potential disputes, SWIFT stored all messages for a period of 124 days at two operation centers, one within the EU and one in the United States. As part of its post-9/11 anti-terrorism initiatives, the US Department of Treasury issued a subpoena to obtain access to the databases which were maintained in the United States.[40] SWIFT complied with the subpoenas, although certain limitations to in relation to the access by the US Treasury were negotiated.

Despite the fact that SWIFT had always considered itself to be a mere processor of the instructing financial institutions, the Article 29 Working Party held that SWIFT acted as a data controller for both the normal processing of personal data under its SWIFTNet service as well as for the further processing by onward transfer of personal data to the US Treasury.[41] The main reasons advanced to support this conclusion were that[42]:

- SWIFT does more than just act behalf of its clients. It has taken on specific responsibilities which, by their nature and scope, went beyond the usual set of instructions and duties incumbent on a processor;
- The management of SWIFT operates in the context of a formal cooperative network which determines both the purposes and means of data processing within the SWIFTNet service;

---

[37] Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)', WP128, 22 November 2006, 10, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm

[38] Ibid, 10.

[39] Ibid, 8.

[40] See also B. C. Treacy, 'Lessons from SWIFT: the 'controller' v 'processor' dillema, Complinet, 9 January 2008, 2, available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/2103/Treacy_SWIFT_1.08.pdf

[41] Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)', *l.c.*, 11.

[42] *Ibid*, 11. See also B. C. Treacy, *l.c.*, 2.

- SWIFT management decides what personal data is processed via that service, and the level of information that is provided to financial institutions in relation to the processing;
- SWIFT management is able to determine the purposes and means of processing by developing, marketing and changing the existing or new SWIFT services (e.g., by determining the standards applicable to its clients as to the form and content of payment orders without requiring their prior consent);
- SWIFT provides added value to the processing, such as the storage and validation of personal data and the protection of personal data with a high security standard;
- SWIFT management had the autonomy to take critical decisions in respect to the processing, such as determining the security standard to be applied to the data and the location of its operating centers;
- SWIFT management negotiates and terminates with full autonomy its services agreements and drafts and changes its various contractual documents and policies.

While acknowledging that some elements suggest that SWIFT may have acted as a processor in the past, the Article 29 Working party considered that the effective margin of maneuver SWIFT management currently possesses precluded a qualification of a mere processor. On the other hand, SWIFT was not considered to be as acting as the sole controller. Despite the fact that the management structure of the SWIFT cooperative had evolved over time in a manner which rendered its management far more independent than it was initially, their founders retained their qualification as data controllers in the sense of the Directive.[43] Consequently, there existed a joint responsibility among the financial institutions and the SWIFT cooperative for the processing of personal data via the SWIFTNet FIN service. However, the level responsibility was not considered to the same among all the participants. In particular, the Article 29 Working Party argued that[44]:

> '[…] joint responsibility does not necessarily mean equal responsibility. Whilst SWIFT bears primary responsibility for the processing of personal data in the SWIFTNet FIN service, financial institutions also bear *some* responsibility for the processing of their clients' personal data in the service' [italics added]

Unfortunately, the Working Party did not provide any further clarification or guidance as to how to define the exact boundaries of responsibility among these 'jointly responsible' entities.

In terms of the conceptual model of degrees of collaboration outlined above, it appears as if the relationship between SWIFT and the participating banks are

[43] Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)', *l.c.*, 12

[44] Ibid, 13.Similarly, in its executive summary the Working Party indicated that 'Both SWIFT and instructing financial institutions share joint responsibility, *although in different degrees*, for the processing of personal data as "data controllers" within the meaning of Article 2(d) of the Directive.'

seen as a collaboration among 'partly joint controllers'. While SWIFT management had become sufficiently independent to be qualified as data controller for processing within the SWIFTNet service, the instructing financial institutions also acted as data controllers, but 'in different degrees'. The responsibility of the latter seemed to be based in first instance on their ability to exert 'some' influence over the policy of the SWIFT cooperative.[45] In addition, the instructing banks retained the ability to decide autonomously about the means used when settling payment instructions.[46] Several alternative or rival services for the transmission of these financial messages were still available to them. Even if the level of influence of individual participants towards the SWIFT cooperative had become significantly reduced, they were still under an obligation to assess the possible implications and privacy risks for their clients when they sign up to any messaging service.

6.4.2.3 Authentication services

In 2003, the Article 29 Working Party issued a Working Document on on-line authentication services.[47] Although the Working Party did not include an extensive analysis regarding the question of controllership at that occasion, it is nevertheless useful to summarize the guidance it provides as this document dealt particularly with authentication services.

a) .NET Passport

.NET Passport is an on-line authentication service operated by Microsoft designed to enable single-on among websites of participating service providers.[48] The basic information flow can be summarized as follows:

- prior to visiting the website of the participating service provider, the end-user will first authenticate himself towards .NET Passport by presenting his username and password;
- if successful, the .NET Passport authentication server will generate an 'authentication ticket' (which includes the Passport Unique Identifier – PUID) and transmit this to the relying service provider.[49]

There are three actors involved in this protocol: an end-user, an authentication service provider (.NET Passport) and a service provider (relying party). As to the roles and responsibilities of the latter two, the Working Party clarified that[50]:

- .NET Passport is considered to be acting as data controller for the processing operations it performs to provide the authentication service (e.g., account creation, identification, credential issuance, profile information);

[45] *Ibid*, 12.
[46] *Ibid*, 12.
[47] Article 29 Data Protection Working Party, 'Working Document on on-line authentication services', WP 68, 29 January 2003, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm.
[48] *Ibid*, 5.
[49] *Ibid*, 3-5.
[50] *Ibid*, p. 9 and 14. See also T. Olsen and T. Mahler, *l.c.*, 418.

- the participating service providers are considered to be acting as data controllers in respect of their own processing operations (e.g. account and profile information maintained by this service provider).

In terms of the conceptual model of degrees of collaboration among controllers, both Microsoft and the relying service providers are to be seen as 'collaborating single controllers'. During authentication of the end-user, Microsoft (through the .NET passport service) is acting as a controller towards all the processing operations which are performed to complete this authentication. Its control also extends to the generation of the 'authentication ticket', and the processing involved in transmitting this ticket to the relying service provider in a meaningful manner. The service provider, from its part, is acting as a controller with regards to its decision to rely upon the authentication services provided by Microsoft, the collection of the 'authentication ticket' provided by the .NET Passport server, as well in relation to all additional personal data processing it performs after it has received this confirmation of authentication. In other words, each entity is to be considered as a controller their own processing operations, without any clear instance of co-controllership. The service provider's decision to rely on the .NET Passport authentication service is a decision which falls within the realm of control of the former, but it does not follow that Microsoft and the relying service provider become 'co-controllers', or otherwise become 'jointly' responsible for any of their operations. Each entity only carries responsibility for those processing operations of which it does in fact itself determine the 'purposes and means' (providing an authentication service and customer information and account management respectively). [51]

b) Liberty Alliance

The Liberty Alliance is a group of companies, non-profit organizations and governments who collaborate with the aim of establishing open standards for federated identity management. The Liberty Alliance is not a separate legal entity, but a collaborative network in which different entities participate pursuant to their terms of agreement.[52]

One of the areas in which the Liberty Alliance Project has developed technical specifications is single sign-on. Single sign-on is understood as the ability of the consumer to, after having authenticated once with a particular Identity Provider, to interact with various Service Providers within a 'Circle of Trust' (CoT) without needing to re-authenticate.[53] One of the main differences with the .NET Passport

[51] To the extent that there would be a real 'negation' among the .NET Passport authentication service and the relying service provider as to the format or content of the 'authentication ticket', with both parties exercising actual decision-making power in that respect, it could be argued that for those particular elements they 'jointly' determine the purposes and means (this aspect of) of the processing operations involved in the generation of the authentication ticket.

[52] Article 29 Data Protection Working Party, 'Working Document on on-line authentication services', *l.c.*, 11-12

[53] A 'Circle of Trust' is described as 'a federation of Service Providers and Identity Providers that have business relationships based o the Liberty Alliance architecture and operational agreements with whom Principals can transact business in a secure and

model is that the Liberty specifications are based on the assumption that there will be more than one entity providing authentication services. Any time a user account has been federated among Service Providers; the Service Provider managing the federated account will be able to act as an authentication service towards other Service Providers who are part of the same Circle of Trust.

The Working Party considered the Liberty Alliance protocol to be 'neutral' from a data protection perspective.[54] It allows compliance with the Directive but does not require it. As far as the obligation to comply with the Directive is concerned, the Working Party made the following observations[55]:

- the Liberty Alliance is responsible as far as the technical development of the project is concerned;
- each Service Provider that implements Liberty specifications bears the responsibility of complying with data protection legislation when operating its 'Liberty-enabled' web services;
- Service providers within a Circle of Trust become data controllers at the time users visit their websites;
- the different participants should have clear contractual agreements in which the obligations of each party concerning data protection aspects are made explicit.

Even though the Liberty protocol was considered to be 'neutral', the Working Party stated that the Liberty Alliance should make sure that their specifications allow the organizations that implement and use them to comply with the Directive. The Working Party additionally encouraged them to develop recommendations and guidelines that motivate companies to use the technical specifications in a privacy-compliant or even privacy-enhancing manner. However, even though designers are expected to take data protection issues into consideration when developing technical specifications, it is primarily the organisations that implement these specifications that are responsible for compliance with data protection legislation.[56]

When analyzing the Working Party's observations concerning the roles of entities participating in a Circle of Trust, it appears that their relationship may also be characterized as a 'collaboration among single controllers'. Each participating organization is considered to act as a data controller for the processing of personal data relating to its end-users. Its choice to exchange personal data pursuant to Liberty specifications is made pursuant to its ability to determine the purposes and means of the processing. The organization that acts as an

---

apparently seamless environment'. Article 29 Data Protection Working Party, 'Working Document on on-line authentication services', *l.c.*, 12.

[54] Ibid, 12.

[55] Ibid, p. 12 and 14-15.

[56] T. Olsen and T. Mahler, *l.c.*, p. 418. Although certain language in the Working Document of the Article 29 Working Party seems to suggest that Liberty Alliance, as designers of a technical specification, bears responsibility for data protection compliance (see p. 14-15 of the Working Document), it is unclear on which ground such responsibility is based. (*Ibid*, 418.) The Liberty Alliance does not as such mandate implementation of their specification in any particular instance. Of course, if the developed protocols were to impede compliance this could significantly discourage organizations from implementing those specifications.

Identity Provider acts as a data controller when transmitting identity information, whereas the Relying Party receiving this information acts as a data controller towards the collection and further processing of this information (as well as towards any other personal data it processes about its customers from that point on).

6.4.2.4 Then Internal Market Information (IMI) system

The Internal Market Information (IMI) system is an ICT tool designed to facilitate information exchange among Member States. In particular, IMI aims at providing support for the practical implementation of Community acts that require an exchange of personal data between Member States' administrations, such as Directive 2005/36/EC on the recognition of professional qualifications and Directive 2006/123/EC on services in the internal market.[57] More specifically, it provides national administrations with needed support in determining the scope and validity of credentials presented by an EU citizen from a different Member State.

The IMI project officially started in 2005 in the context of the IDABC program.[58] It was created pursuant to the Commission's Decision 2004/387/EC (the 'IDABC' decision)[59], in particular art. 4 thereof; in combination with the Professional Qualifications Directive and the Services Directive. The Commission made a first attempt to regulate the data protection aspects of the implementation of IMI in Decision 2008/49/EC.[60] This Decision was later supplemented by the Commission in the form of a Recommendation 'containing data protection guidelines for the IMI system' (hereafter: the Commission Recommendation on IMI).[61] These documents specify inter alia the finality of the IMI system, the roles of the actors involved, the retention period of personal data processed via IMI, how notice is to be provided, etc.

The IMI system is structured as a network which allows the 'competent authority' of a given Member State to identify its counterpart in another Member State and to exchange information using the IMI network. In addition to its search function, IMI provides users with a set of pre-translated menus, as well as standardized questions and procedures to support the information exchange.[62]

---

[57] Recital (4) of Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), 2009/329/EC, O.J. L 100/12-28, 18 April 2009.
[58] See also http://ec.europa.eu/idabc/en/document/5378/5637 (last accessed 22 July 2009).
[59] Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), O.J. L/144, 30 April 2004, as corrected by O.J. L/181, 18 May 2004, p. 25.
[60] European Commission, 'Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data', 2008/49/EC, O.J. 16 January 2008, L13/18-23.
[61] Commission Recommendation of 26 March 2009 on data protection guidelines for the Internal Market Information System (IMI), 2009/329/EC, O.J. L 100/12-28, 18 April 2009.
[62] See Article 29 Data Protection Working Party, *Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)*, WP140, 20 September 2007, p. 4, available at http://ec.europa.eu/internal_market/imi-net/docs/art_29_wp_opinion_en.pdf (hereafter: 'Article 29 Opinion on IMI')

One of the examples provided in the Commission Recommendation on IMI is quite illustrative in this regard[63]:

> "A German doctor resident in Berlin marries a French man and decides to start a new life in Paris. The German doctor wants to practice her profession in France and therefore submits titles and diplomas to the Order of Doctors in France. The person dealing with the file has doubts about the authenticity of one of the diplomas and uses IMI to check with the competent authority in Berlin."

The service provided by IMI is a way quite similar to (part of) the services TAS[3] will offer in the employability scenario. A relying party may be presented with an assertion that a particular user has obtained certain qualifications, but may wish to obtain further assurance from the relevant Authoritative Source. The Accreditation of Prior Learning use case deals specifically with this issue.

The Commission Recommendation on IMI is valuable both to our current analysis and future approach because it also provides additional clarification as to the issue of joint controllership among participants to IMI. Under section 4 it is stated that[64]:

> 'IMI is a clear example of joint processing operations and joint controllership. For example, whilst only the competent authorities in the Member States exchange personal data, the storage of these data on its servers is the responsibility of the European Commission. Whilst the European Commission is not allowed to see this personal data it is the operator of the system who physically processes the deletion and rectification of the data.
>
> In other words and as a result of the allocation of different responsibilities between the Commission and the Member States:
>
> a) Each competent authority and each IMI coordinator is a controller with respect to its own data processing activities;
> b) The Commission is not a user, but the operator of the system, responsible, primarily, for maintenance and security of the system;
> c) The IMI actors share responsibility with respect to notice provisions and rights of access, objection and rectification.
>
> In complex scenarios of joint controllership like IMI, it seems most efficient from the perspective of compliance to embed data protection in the system from the beginning […] and to define a compliance framework as provided in these guidelines. Compliance with the framework is the responsibility of all IMI actors and users.'

Although these guidelines provide a relatively clear outline of the responsibilities of the participants to IMI, there is still some ambiguity in the language pertaining to the exact role each entity assumes within this collaboration, in

[63] Commission Recommendation on IMI at L/100-15.
[64] Ibid at L/100-17.

particular with regards to the role of the Commission. While the introductory section identifies IMI as a 'clear example of joint processing operations and joint controllership', it only explicitly qualifies the participating competent authorities as 'controllers'. The Commission is labeled an 'operator', without a clear accompanying statement as to whether this implies it will be acting as a controller or a processor. The term 'operator' cannot be found anywhere in the text of Directive 95/46. Given the broad introductory statement that IMI is 'a clear example of joint processing operations and joint controllership', one could assume this means that the Commission too, similar to the competent authorities, is considered a controller in respect to its own processing activities.

However, the text of the IMI Guidelines at the same time gives the impression that the responsibilities of the Commission might be more limited in scope – or at least of a different nature – than the responsibilities of the participating competent authorities. It is our view that the Commission does in fact act as a controller in respect to its own processing operations, but that these processing operations are of a different nature than those performed by competent authorities. While it is primarily the latter that initiate exchanges of personal data, the Commission's 'physical' involvement in these operations extends only to the processing operations it performs to support these exchanges (storage, security, availability and maintenance of the IT infrastructure upon which IMI will be run, physical processing of deletion and rectification of data[65]). If this interpretation were to be followed, one could argue that the Commission's role as 'operator' towards these processing obligations would be that of a 'partly joint controller' rather than a 'full scope joint controller'. However, one must also keep in mind that the Commission has, to a large extent, determined the purposes and means of the Internal Market Information system as such. In its Decision 2008/49/EC 'concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data'[66] it set the forth the purposes of the IMI system. In the same Decision and subsequent guidelines it has also specified the parameters of the data exchange, including which types of personal data are to be exchanged in which instance, as well as the retention period of these data. The Commission has also outlined the respective roles and responsibilities of the various IMI actors (both towards their roles as users of the IMI system as well as their roles as controllers in their relationship towards the data subjects whose information they process). For these reasons, we conclude that:

- each competent authority and each IMI coordinator is in fact a controller with respect to its own data processing activities;
- the relationship between competent authorities is best characterized as a 'collaboration among single controllers';
- the Commission bears certain responsibilities in its role as 'operator' towards actual data exchanges (implying partly joint controllership if this were its only role), but nevertheless also acts as a full scope joint

[65] See L-100/17 of the IMI Guidelines and art. 3, 5 and 10 of European Commission, 'Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data', 2008/49/EC, O.J. 16 January 2008, L13/18-23.

[66] European Commission, 'Commission Decision of 12 December 2007 concerning the implementation of the Internal Market Information System (IMI) as regards the protection of personal data', 2008/49/EC, *O.J.* 16 January 2008, L13/18-23.

> controller in light of the decision-making power it has exercised and continues to exercise towards the overall purpose(s) and means (organization of collaboration, setting of parameters of exchange) of the IMI system.[67]

6.4.2.5 Conclusion

The RAND technical report reviewing the European Data Protection Directive found that the definition of entities involved in processing and managing personal data is in this Directive are 'simplistic' and 'static'.[68] It stated that

> 'The relationship between processor and data controller envisaged in the Directive does not adequately cover all the entities involved in the processing of personal data in a modern networked economy. There is uncertainty about when a processor becomes a controller or vice versa, particularly in an online environment […]'[69]

The preceding sections have illustrated that the determination of which entity assumes which role can be particularly difficult when otherwise autonomous entities set up a new form of collaboration. The developments in technology and business models since the enactment of the Directive have led authors to adopt a less 'monolithic' conception of controllership with regards to personal data processing in which clearly distinct actors are participating. In the end, it becomes necessary to distinguish between the different types of processing operations and determine which role each entity plays with regards to a particular operation. In this regard it is important to distinguish between the decision-making power concerning the overall structure of an application, its security features, its generic purpose etc. on the one hand, and the other hand the decision-making power that is exercised when deciding whether or not to process personal data whilst making use of a particular application.[70]

This more granular approach was also reflected in some of the non-published background papers that preceded the Data protection Commissioners resolution in favor of International privacy Standards[71]. Instead of using the definitions of data controller and data processor which have a number of overlapping definitional elements, the papers referenced responsible parties and service providers. The definitional difference between the two is that the 'responsible party' decides whether to have the information processing service, while the 'service provider' provides the service. This cleaner definition eliminates some of

---

[67] This conclusion is based on the roles and their definitions as they are currently provided in the Directive and the guidance provided in the Opinions of the Article 29 Working Party (in particular the SWIFT decision). As we will elaborate further in the conclusion of this section, there may be a need *de lege ferenda* to revise the criteria for allocation of responsibility currently set forth by the Directive.

[68] N. Robinson, H. Graux a.o., 'Review of the European Data Protection Directive', Rand Europe, 2009, 36, available at http://www.rand.org/pubs/technical_reports/TR710.

[69] Ibid, 36.

[70] Ibid.

[71] Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection; 9/11/2009; http://www.privacyconference2009.org/dpas_space/Resolucion/index-iden-idphp.php

the confusion related to operational decisions which must be undertaken in providing a processing service, which some previously argued implied a co-controller rather controller-processor relationship. In addition, this cleaner definitional differentiation makes it easier for persons not expert in data protection to better understand and apply the implications of the terms.

Besides the need for conceptual clarification of both the terms and criteria that determine which entities are responsible for ensuring data protection compliance, there is also an apparent need for further specification of how the nature and structure of collaboration impacts the responsibilities and obligations of each entity involved. In this regard it is interesting to note that the Directive currently does not explicitly require joint or collaborating single controllers to contractually agree on how the processing will be organized and carried out so that compliance is assured.[72] Both doctrine and the Article 29 Working Party have called out the need for contractual arrangements among (co-)controllers, but a clear specification of this obligation and its components within the regulatory framework would appear to be very welcome. In addition, there is no mention in the Directive of how such contractual arrangements might impact the distribution of responsibilities for compliance with data protection regulations.[73] The Working Party has in several instances mentioned that there might be different 'degrees' or 'levels' of co-controllership, but without further specifications or clarification this creates significant legal uncertainty. We hope that the Working Party will make an attempt to address these very practical questions in its future work on controller/processor roles.[74]

6.5 Defining the "What"

Once the parties have been identified and categorized it is important to understand their functions, rights and obligations. This will constitute the "What". For the purposes of the initial contractual framework, we will presume a centralized TAS[3] trust infrastructure (anchor/founder) because the contractual framework in this situation is the most complete of the three possible architecture scenarios.[75]

All parties need to be contractually bound in order to assure that rights and obligations can be properly enforced. As in the credit card situation there are limited responsibilities on the end-user and increased responsibilities placed on those with greater control. This association between obligation, risk and control is captured in the OECD Guidelines for the Security of Information Systems and Networks[76] principle on responsibility:

> ***All participants are responsible for the security of information systems and networks.***

[72] See also T. Olsen and T. Mahler, *l.c.*, 417-418.
[73] Ibid, 421 and 418.
[74] See Draft Agenda of the 73rd meeting of the Article 29 Working Party, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/draft_agenda_73rd_meeting_en.pdf
[75] Cf. section 4.5.
[76] http://www.oecd.org/dataoecd/16/22/15582260.pdf

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

The foundation of any ecosystem is predicated on rules established at the ecosystem level, which are subsequently bound, where appropriate and relevant, to all participants. The internal/operational elements of the ecosystem are the same as the requirements placed on participants with two exceptions. The first is the need for a compliance/oversight mechanism defined at the infrastructure level (though implemented, as appropriate, across all levels) and the second is the need for external facing documents described above. These are needed to satisfy some of the notice requirements inherent in privacy laws. In defining infrastructure requirements, and the requirements that may be imposed on other participants, subgroups will also need to create public facing as well as operational documents. Depending on the organization of the ecosystem, these may either require adoption of the pertinent parts of the infrastructure documents and procedures, or it may enable groups and organizations to develop or use their own policies and procedures that are consistent with the notice and operational requirements that apply to them.

Contracting at the TAS³ ecosystem level, the level common to all parties, the general requirements of security, infrastructure and privacy will be established. The architecture level will also require that parties agree to be bound by the technical limitation on use of information that may be associated with sticky policies. The latter is important, as it will provide a written grounding for contracts that may otherwise only exist in electronic form. Parties will also accept a general binding related to respecting expressed limitations on use or sharing of personal data, using only the most limited data needed to accomplish the required task, and providing access to data only as needed by those involved in providing the specific service. Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data, must not process them except on instructions from the controller, unless he is required to do so by law.

6.5.1 Liability

Part of the TAS³ architecture will provide a complaint handling and redress feature whereby individuals and organizations can raise issues, resolve disputes and obtain redress. Nothing in such terms and processes shall preclude the individual or organization from reverting to relevant governmental authorities if they have not been satisfied with the process, unless they have accepted a

settlement in compensation for their loss and provided a release, or, in the case of an organization, otherwise waived that right contractually. The contract will not create liquidated damages per se, but all parties will be held liable for their actions to assure that any person suffering damage from an unlawful processing or processing incompatible with the TAS³ requirements will be entitled to receive redress or, where appropriate, compensation.

The Directive assigns practically all liability for damages caused by data protection violations to the controller. In the previous section we elaborated on how the issue of role definition (in terms of controllers and processors) shall be resolved with TAS³. The obligations and corresponding liabilities of all of the roles will be bound by contract. Thus a party acting as a controller will also be bound to all the requirements of the controller. In addition participating entities may be bound to additional requirements, which shall be accompanied by an appropriate liability scheme.

There is a question of whether liability should be allocated to the organizing entity/entities who can then assert rights against the specific bad actor service provider. Work remains to be done to flesh out potential liability issues in the various potential business organization models (anchor, consortia, and convenor). Issues around allocation of liability to the organizer include the diminished likelihood that an organization will want to be an organizer and the potential control that such an organization may require to shoulder a greater risk burden. Recall that significant damage from misuse of sensitive information could accrue, which might be more than a smaller service provider could cover. We are exploring better ways of associating risk allocation with responsibility. Alternatives under consideration include both external and self-insurance models.

In absence of a clear business model being defined at this point time, it is of course difficult to determine to determine the level of control (and corresponding liability) of each entity at this juncture. As the business model and demonstrators are developed further we will be able to further develop the liability model and related contract terms.

6.5.2 Security requirements & architecture implementation

The TAS³ Architecture (D2.1) outlines the various security elements (digitally signed audit trail, SSO, Web Service Standards, XACML…) that comprise the technical components of security in TAS³. The contract and policy frameworks also support security across TAS³. The Ecosystem contract will specify minimum security requirements in a schedule or an incorporated-by-reference document to facilitate updating. At a minimum, a participant will need to have:

- Documented security policy(ies) addressing physical, logical and administrative security, that are at the level of the state of the art and appropriate to the risks represented by the processing and nature of the data and define appropriate technical and organizational measures to protect personal data against:
    - Accidental/unlawful destruction

    - Unauthorized access or disclosure
- Documented Privacy policy
- Persons responsible for overseeing and enforcing security and privacy policies (security officer),
- Testing and update procedures,
- Incident/breach response and business continuity plans,
- Audit, oversight and remediation procedures,
- Policies controlling employee access and use of the Internet and system resources,
- Encryption policies for information in transit and at rest,
- Data retention and secure deletion policies

As part of a qualification and vetting process, participants will need to have these requirements vetted against the TAS³ reference model policies and procedures, or they may choose to adopt the TAS³ reference model.

TAS³ also requires that participants adopt and be tested against TAS³ technical architecture requirements. The ability to comply with architecture, policy and legal requirements will be reviewed as part of the service provider vetting process. While in the case of the security requirements, the vetting process allows for flexibility through consistent variations in policies and requirements, the architecture requirements will need to be adopted as they are. Any requests for variations to architecture implementations will need to be considered by a central architecture review team to assure the continued consistency and efficacy of the TAS³ architecture.

The vetting process must also consider the standing, reputation and solvency of TAS³ entities. To that end, organizations must provide a certificate of good standing from a governmental or other recognized organization (chamber of commerce), references to the extent that the organization may be small or recently formed and statement of financial condition or audit attestation sufficient to determine solvency/business continuity as relates to the role the organization will play. For example, an organization that provides incidental processing of information will be required to meet lower thresholds of proof and disclosure than organizations playing central roles and that retain personal data.

As we gain experience from the demonstrators and refine our operational models we will be able to better specify the technical, legal and policy requirements of security and how to associate them to provide more seamless, end-to-end security. One of the greatest challenges which needs to be addressed in the contract and policy framework is how to deal with service providers that have received authorization by the data subject but do not plan to become full TAS³ participants (and thus will not go through the standard service provider vetting process) (see also section 6.1 of the current deliverable).

Beyond those requirements, a controller is also responsible to exercise due diligence in the choice of a processor in terms of reputation, technical capacity, implementation, etc. Part of that due diligence will be fulfilled in the review and vetting process for an organization to become part of TAS³.

The vetting process must also consider the standing, reputation and solvency of TAS³ entities. To that end, organizations must provide a certificate of good standing from a governmental or other recognized organization (chamber of commerce), references to the extent that the organization may be small or recently formed and statement of financial condition or audit attestation sufficient to determine solvency/business continuity as relates to the role the organization will play. For example, an organization that provides incidental processing of information will be required to meet lower thresholds of proof and disclosure than organizations playing central roles and that retain personal data.

6.5.3 Operational data protection requirements

TAS³ is committed to providing an architecture of trust and security. We must however recognize that the proposed architecture is focused on the interactions between participants and related information exchanges. Through contract and policy requirements, TAS³ further attempts to provide assurance that TAS³ organizations are managed responsibly and in an accountable fashion. Each organization, however, must internalize and customize these requirements in a way that can be appropriate deployed in their specific context. There are likely to be pre-existing system implementations, policies, practices contracts and other factors that must be considered in implementing TAS³ requirements. For most organizations, they will likely use a gap analysis process to see where their system controls, policies, practices and contracts may need to be adapted. While the gap analysis will need to assure compliance, differences in phrasing and needed customization related to specific implementations will need to be accommodated where there is no undermining of TAS³ requirements.

6.5.3.1 Data protection requirements and implementation overview

The following table maps specific data protection requirements into both TAS³ techical/organizational measures to achieve compliance as well as with TAS³ best practices. This represents the further development of the legal requirements categorized in D6.1.[77] Both the measures listed for compliance as well as the TAS³ best practices are essential to the successful implementation of the data protection requirements set forth in the previous section. The table also cross-references other relevant TAS³ deliverables to which the reader may turn for additional clarification. This table (Figure 6)[78] provides a useful summary overview of the interrelation among the techical, business, legal and policy, components of TAS³.

[77] See TAS³ D6.1 at section 5.

[78] The tables provided here have been adapted from earlier work performed by one of the contributors in the context of the EU FIDIS project. See J.C. Buitelaar, M. Meints and E. Kindt (eds.), "D16.3: Towards requirements for privacy-friendly identity management in eGovernment", 2009, forthcoming on www.fidis.net. We have also looked at PrimeLife's 'Requirements for privacy-enhancing Service-oriented architectures' (available at http://www.primelife.eu/images/stories/deliverables/h6.3.1-requirements_for_privacy_enhancing_soas-public.pdf) and are looking to harmonize the respective requirements and implementation specifications across projects at an upcoming cluster event or in future conversations.

Legitimacy of Processing	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Relevant entities shall be charged with front-end consent registration (receiving and registering of informed consent) (intake of data subjects) 2. TAS³ shall ensure consent is obtained prior to the processing, except where mandated by law or through an exception recognized by law; and taking into account requirement that consent must be 'freely given' in order to qualify as a legitimate basis 3. Legal bases, prior authorizations and/or consent directives shall be maintained in appropriate repositories; technical policy rules shall be adapted to include these elements as policy conditions. 4. Consent registration relevant to TAS³ processes shall be documented and both technical and organisational measures shall be audited on a regular basis	1. Consent shall operate as default policy condition in authorization decisions by Policy Decision Points (PDPs) 2. TAS³ will provide user with ability to granularly express privacy preferences, in particular by: - providing users with a secure delegation service; - providing users to ability to express preferences through a 'policy wizard'; - providing a 'user call-back' service to enable subsequent consent capture (see deliverables D2.1, D3.1, D4.2 and D7.1)

Data Minimization	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. TAS³ participants shall be required to adopt privacy policies which inter alia: -specify the purposes of processing; -provide assurance that only the information which is absolutely needed for a specific purpose is collected; -explicates data life cycle management (incl. intended storage duration); -describes how access and processing capabilities are restricted within the organization so that its members are only able process personal data in accordance to	1. User-controlled attribute aggregation through 'linking' service (see deliverables D2.1, D4.2 D7.1) 2. Purpose and storage duration specification (inter alia in 'sticky policies', including obligations relating to removal); (see deliverables D2.1, D4.2 and D7.1) 3. Selective attribute disclosure during authentication: additional measures to avoid unnecessary linkability, pseudonym

what is strictly needed for the performance of their tasks / their role within organisation 2. Authoritative sources (i.e. sources trusted to provide accurate & up-to-date information) shall be designated and vetted (thereby reducing the need for unnecessary duplication) (cf. infra; data accuracy) 3. Access and processing limitations that support a sufficient level of granularity (access/data release on a 'need-to-share' basis) shall be implemented 4. Mechanisms shall be in place to respond to data requests with only that information that the requesting entity is authorized to receive 5. Policies shall be in place to restrict propagation of more attributes than needed 6. Personal data shall be removed or anonymized once the purpose for which it was collected / further processed has been completed (taking into account need for accountability at later time) 7. All technical and organisational measures relating to data minimization procedures shall be documented and audited on a regular basis	management) (see deliverables D2.1, D4.2 and D7.1) 4. Additional measures to avoid unauthorized or unnecessary monitoring (inter alia providing user choice where possible as to whether or not persistent ID or transaction ID is used) (see deliverables D2.1, D4.2 and D7.1)

Data Accuracy	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Authoritative sources (i.e. sources trusted to provide accurate & up-to-date information) shall be designated 2. Vetting of sources of attribute information - Procedures shall be established to ensure verification of each attribute with a level of assurance proportionate to the interests at stake 3. Data life cycle management procedures shall be in place, incl. review and update procedures for personal data which is being kept for a prolonged period of time 4. Procedures shall be establish specifying how to communicate and deal with suspected inaccuracies 5. Data processed within TAS³ shall be integrity protected where appropriate	1. TAS³ will enable indication of the "level of confidence" in meta-data where appropriate 2. Sticky policies will restrict unauthorized modification throughout data life cycle (see deliverables D2.1, D4.2 and D7.1)

6. In the event of indirect collection, data shall be verified with data subject where possible prior to further processing 7. Data modification rights shall be restricted to duly authorized entities 8. Appropriate security policies (e.g. use of cryptography) to ensure authenticity and integrity shall be implemented 9. All technical and organisational measures relating to data accuracy procedures shall be documented and audited on a regular basis	

Finality	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. TAS³ participants shall be required to adopt privacy policies which inter alia: -specify the purposes of processing; -provide assurance that only the information which is absolutely needed for a specific purpose is collected; 2. Restrictions and obligations wrt subsequent use shall be specified 3. All TAS³ participants shall be bound to obtain subsequent consent if the use of information changes except where mandated by law or through an exception recognized in law 4. All technical and organisational measures relating to data accuracy procedures shall be documented and audited on a regular basis	1. Purpose specification and restrictions on subsequent use in sticky policies (see deliverables D2.1, D4.2 and D7.1) 2. Context/purpose as policy condition where appropriate 3. User call-back mechanism (see deliverable D2.1) 4. Additional measures to avoid unnecessary linkability (pseudonym management) (see deliverables D2.1, D4.2 and D7.1)

Confidentiality and Security of Processing	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Appropriate identification, authentication and authorisation mechanisms shall be in place 2. Roles and responsibilities shall be defined for at least the following tasks: • performing the required authentications, authorizations and checks for every processing operation • the maintenance of logs for the different processing operations that	1. Implementation of advanced security policies to ensure confidentiality, integrity and authenticity (see deliverables D2.1 and D7.1) 2. Use of Authoritative sources in user- and access management (ABAC) in addition to RBAC; credential issuance and validation service (see deliverable D7.1) 3. Use of sticky policies (see deliverables D2.1, D4.2 and D7.1) 4. Additional measures to avoid

take place; • trusted (third) party services (e.g. attribute certification, identifier conversion etc); • updating of technical policies in accordance with permissions granted by data subject and legal developments • oversight; including regular verification of compliance, redress and point-of-contact in the event of a security breach 3. Identity life cycles shall be managed in a way which provides an assurance level proportionate to the interests at stake 4. Procedures shall be established for verification of each relevant attribute (e.g. capacity of doctor) of a requesting/asserting entity with a level of assurance proportionate to the interests at stake 5. Access and processing limitations supporting sufficient level of granularity shall be implemented 6. Appropriate security policies to ensure confidentiality, authenticity, integrity shall be implemented 7. Physical access to terminals which enable sensitive processing operations shall be restricted where appropriate 8. Restrictions and obligations shall be associated with individual data processing operation 9. TAS³ participants shall be required to adopt internal privacy policies (documenting security measures, specifying inter alia persons responsible, what to do in the event of a breach, …) and to provide education and awareness training for all persons who come in contact with personal data 10. Confidentiality agreements shall be put in place or exacted where appropriate 11. Security officers shall be designated or designation thereof shall be required where appropriate 12. All technical and organisational measures relating to security shall be documented and audited on a regular basis	unnecessary linkability (pseudonym management) (see deliverables D2.1, D4.2 and D7.1) 5. Secure & dynamic delegation service, consent as a default requirement, user call-back mechanism, dynamic policy update and policy evaluation in multiple instances where appropriate (see deliverables D2.1, D4.2 and D7.1) 6. Additional measures to avoid unauthorized or unnecessary monitoring (inter alia providing user choice where possible as to whether or not persistent or transaction ID is used) (see deliverables D2.1, D4.2 and D7.1) 7. Credential aggregation infrastructure (see deliverable D7.1) 8. BTG infrastructure (see deliverable D7.1)

Accountability	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Responsible entities and roles shall be defined for at least the following tasks: o providing notice and transparency to data subjects o the maintenance of logs for the different processing operations that take place; o front-end accommodation of the rights of data subjects such as the right of access and correction o oversight; including regular verification of compliance, redress and point-of-contact in the event of a security breach. 2. Internal responsibility and accountability mechanisms (e.g. designating 'owners' for both equipment and processing operations involving personal data) shall be adopted and/or exacted from TAS³ participants 3. Non-repudiation mechanisms shall be implemented where appropriate 4. Processing operations upon personal data shall be logged 5. Notification services shall be implemented where appropriate (e.g. notification to oversight committee in the event of suspicious behaviour) 6. All technical and organisational accountability measures shall be documented and audited on a regular basis	1. Sufficient financial solvency or insurance of members of TAS3 network shall be required 2. The asserted purposes for processing shall be registered by trusted entities to facilitate later audit 3. Appropriate entity authentication assurance levels shall be defined for each transaction (see deliverable D4.2 and D7.1) 4. Enhanced transparency mechanisms allowing direct data subject access to view the processing operations performed upon his personal data (via 'dashboard') (see deliverable D2.1)

Transparency and Data Subject Rights (notification, access, rectification, object, deletion)	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Data controllers and otherwise responsible entities shall be clearly communicated to data subjects 2. It shall be widely communicating to whom and how data subject may direct requests regarding data subject rights and how they are to be exercised 3. Internal procedures shall be adopted and/or exacted to reply to these requests in a timely manner	1. TAS³ will provide notification to the data subject and/or to the public in the event of security breach 2. Enhanced transparency mechanisms allowing direct data subject access to view the processing operations performed upon his personal data (see D2.1)

4. The source of personal data and logic of processing shall be communicated when notifying data subject of decision based on such data where appropriate 5. All technical and organisational measures related to transparency and accommodation of data subject rights shall be documented and audited on a regular basis	

Figure 6: Table of TAS³ Data protection requirements and implementation overview

At this point it is also useful to introduce Annex 4 of this document. Annex 4 is a compendium of the TAS³ legal requirements set forth in both TAS³ D6.1 and D6.2. The Annex includes not only the legal and policy requirements but also identifies several of the technical components needed to enable them. The Annex serves as the iterative working document between WP6 and the other Work Packages.[79]

6.5.3.2 Legally mandated disclosure and e-discovery

As is highlighted in the requirements described in D6.1, the Directive makes provision for organizations to provide information where legally required. A number of legal reasons ranging from lawsuits to national security may require information to be disclosed. Each of these disclosures will entail a discovery and redaction process. It is likely that these requests will not come to TAS³ as an architecture, but rather to the service provider(s) that have the specific information. Thus internal policies must be in place that is consistent with the TAS³ approach to appropriately address this issue.

In recent years there has been both great contention and confusion between data protection and e-Discovery. While some tension exists within Civil Code jurisdictions based on the national as opposed to uniform treatment of the concept across legal systems, the greatest tension is with Common law jurisdictions. Common Law, as implemented in the US, provides broader scope e-discovery that goes to issues that are, or may be, relevant to the case. Civil code jurisdictions, where discovery procedures are formally established, permit a more limited discovery directly supporting the case. E-discovery in the UK is more limited than the US, but broader than most Civil Code jurisdictions as they permit discovery of facts the case will rely on. There are also differences related to the types of items that are discoverable. Common Law jurisdictions often permit broader discovery that extend to e-mails, sensitive data, metadata, third party data; essentially, the data available on servers, back up tapes etc.

[79] As such it is a living document that has drafting variations to the more static foundation documents (TAS³ D6.1 and D6.2). As the iterative process continues, and the framework stabilizes, there will be a more direct correlation between the documents.

The Article 29 Data Protection Working Party (WP 29) has developed guidance for how to comply with E-discovery requests[80]. This guidance was developed to help determine how to meet some of the requirements of the Directive. Among the elements considered most important were: the need to have a legitimate basis for processing, whether consent was a basis for processing, how the data were secured, and application of the principle of proportionality, especially as it applied to sensitive data. WP 29 found issues with a number of the topics listed above, but managed to provide guidance on how one should treat the requests. A summary of the most important elements and the related TAS³ requirement is set out in Figure 7 below.

Guidance	TAS³ Requirement
Records retention Part of discovery includes the concept of a litigation hold – the need to preserve information that is discoverable for trial when you have notice of an action. While this was seen to be permissible processing, the guidance also suggested that it applied to only those documents currently held.	• Properly classify information • Develop records management policy with retention period and deletion/anonymization policies and processes (need secure deletion…)
Notice One of the issues related to consent, but not the only issue raised, was the need to provide notice of intended or possible processing.	• Initial privacy policy notice specify the need for compliance with legal obligations, including compliance with court orders and legitimate discovery requests • The user must in particular be informed that their actions shall be logged for audit trail purposes, and may later be released and used for the purpose of providing evidence in legal proceedings • Once data related to the data subject is being processed further for evidentiary purposes, he/she should receive additional notification. Such notification should include: identity of recipients, purpose, categories of data and reference to their rights as a data subject. Exception: instances in which there is a substantial risk that such notification would jeopardize the ability of the litigating party to investigate the case properly or

[80] See Article 29 Working Party, 'Working Document 1/2009 on pre-trial discovery for cross border litigation', WP 158, 11 February 2009, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf.

	gather the necessary evidence
Security The requirements of security apply to the court service, not just the organization complying	• This requirement, that court services also treat information securely, is outside of TAS³ control, but process could suggest a notification of security needs to the court and request for confirmation.
DPO It was suggested that the Data Protection Officer of the company be involved from the outset.	• Where feasible, in terms of size and staffing, organizations should have a person or group tasked with the responsibility for data protection. • TAS³ should have a data protection council as some of these issues may have system level impact.
Redaction process Limit first data protection to relevant data and provide only anonymized or pseudonymized data related to anyone not party to the case. Subsequently some more characteristics may be needed to supplement the more limited data provided in the first filtering, but still try to limit production to pseudonymized data. Filtering should be conducted locally, may involve trusted third party.	Discovery process: • Route request to appropriate legal authority and DPO within organization and/or TAS³ oversight committee • Review request for correctness and sufficiency. • Follow redaction process outlined in guidance • Identify possible local third parties to assist in redaction/filtering (this may be done as part of a structural process without pending litigation)

Figure 7: Table of the Article 29 WP Guidance on e-Discovery and Related TAS³ Requirements

The guidance provided for e-discovery is actually extensible to all legal requests. Thus, within the TAS³ architecture (either in a centralized capacity or at the participant level) there must be a process to review legal requests to assure that they are appropriate and compliant with legal requirements, an inventory process to gather information relevant to the request[81] and a review and redaction process to assure that only appropriate information is disclosed. To the extent possible information will be provided in aggregated, pseudonymized or anonymized form, with the understanding that some cases will require identifiable disclosures. To avoid surprise of the data subject or potential

[81] The TAS3 architecture has both audit and logging functions, which with the appropriate permissions enable actions and transactions to be reviewed within the retention period of the information. Separation of duties, policies and other controls secure such logs and audit functions.

evidentiary compromise, participants to the TAS³ process will be on notice that TAS³ will comply with legitimate discovery requests and will provide limited information responding to those requests.

7 Applying the "What" to the "Who"

We will first map some of the controller/processor obligations across the 4 categories. The processor dialogue box is more substantial because the application of the requirements to the processor have greater nuance and require more description. Then we will consider end- user/data subject rights and obligations. Note that these requirements/obligations are detailed further in annex 4.

7.1 Service provider obligations

Obligation	Controller	Processor
Collection		
Notice	Yes	To the extent that the processor is collecting information on behalf of a controller
Collection limitation	Yes	No in determining what information should be collected, but in executing the Controller's requirements of collection
Processing		
Legal basis	Yes	Relies on controller
Consent/subsequent consent	Yes	Usually relies on controller unless this function has been delegated to processor
Operational		
Accuracy	Yes	To the extent directed by the controller in terms of update, but in all cases need to maintain the integrity of the information
Retention	Yes	Pursuant to the direction of the controller as to what the retention period is
Security	Yes	Yes (Controller can require certain level security, but processor can also deploy even higher level security – especially if processor is located in a jurisdiction that has a higher security requirements than that of controller. Processor cannot provide less security than controller specifies)
Accountability		
Access	Yes	To the extent directed by controller
Other elements	Yes	Yes (again much like security, the requirements specified by the controller must be met but if

		controller were not to specify any oversight or accountability mechanisms, processor would still be responsible for taking reasonable steps as needed to provide accountability and oversight for their responsibilities.)

Figure 8: Table Applying Data Protection Obligations to Controllers and Processors

As is evidenced from the table in Figure 8, processor requirements are often conditioned upon the controller-processor relationship and the services requested. From a TAS³ contractual perspective this means that controller obligations shall be set forth in the Ecosystem contract. While a controller may delegate an actual function it cannot disclaim responsibility for the function. Processor obligations being both more variable and nuanced are harder to define in one-size-fits-all categories. Processor obligations will need an Ecosystem contract definition as well as transaction contract limitations or enhancements depending upon the definition of services.

An example may be helpful. Fact pattern:

- A university employs a service provider to extend its capacity to provide placement for its students.
- The University allows the service provider to undertake intake and customer service functions, based on University forms and procedures.
- The University remains the controller, but has asked the service provider to assume some of the controller functions pursuant to its direction.
- University credentials are validated by a national credential database run by a government organization.

The Ecosystem contract will cover the normal requirements on the service provider, including: security and appropriate internal accountability and oversight mechanisms. The Ecosystem contract will also contain a general limitation that service providers may not use the information provided for anything but the purposes needed to provide the service. The role or transaction contract will contain any specific requirements related to security and oversight that the University cares to add as well as specific requirements related to the delegated functions. While the role/transaction contract will be a written or dynamic electronic contract, it will likely be supplemented by sticky policies accompanying the data (more granular level obligations), which must be complied with by both controller and processor.

7.2 End-user rights and obligations

7.2.1 End-user obligations

The contracting process has for the most part focused on the obligations of the organizations in their various roles. The individual will also need to be bound by contract. The binding of the individual is required foremost for the sake of establishing privity and enabling the individual to have standing to take action under the contract directly as opposed to only in response to harm or as a matter of tort redress. The contractual participation of the individual however, will also bind the person to the actions they have directed or consented to. Those bindings are, of course, dependent on the fairness and transparency of the process.

Apart from the binding described above, the pertinent question to ask is: are there other appropriate responsibilities for the end-user of the system? The end-user is likely the person with the least technical knowledge, is highly vulnerable to attack at the system level, and has a high potential for compromise of his home system.[82] While any contract will have boilerplate language about the need to use the service for only those purposes specified as legitimate and may have some penalties for knowingly using the system in contravention of those purposes or otherwise knowingly causing harm (spam, hacking into other accounts, defamation…) a question arises as to whether there should be any specific system requirements on the end-user beyond use of the TAS^3 client. Potential additional requirements may include virus and other basic security protections. This is currently still an open issue which requires resolution. It could either be in the contract or a requirement of the system use, for example, to log in either once or periodically. The contract terms may provide for attestation by the user of deployment of proper technologies; perhaps even types (not brands) specified by system infrastructure or may request permission to scan the system for installed software (at the directory tree level this can be done with limited chance of privacy intrusion if the information is not maintained beyond the check) or may require a remote scan for viruses before allowing connection. The system will also likely check e-mail traffic for viruses and malware which provides another method for monitoring possible infection.

7.2.2 End-user rights

The TAS^3 infrastructure imposes very few obligations on the end-user. By contrast, as detailed below (and in even further detail in annex 5), the user is accorded with many rights. This is a natural consequence of the user-centric approach that characterizes TAS^3. TAS^3 user-centricity enables an individual to manage her identity and service provider relationships with better information and technical tools. End-user system controls are important way for data subjects to directly exercise their data protection rights.

[82] Recent press releases from Panda Security and Symantec suggest that home computers that are infected and part of botnets are significantly on the rise. Various reports also suggest that more that 23% of home computers are infected with one or more viruses.

Within the TAS³ architecture, the end-user will be granted fairly granular control over the use and sharing of her personal information. The fact that TAS³ establishes trust at the architecture level means that controls of the end-user will be applicable across the organizations participating in the information exchange, not just the one that the end-user is in contact with. This is where appropriately defining the roles of technology, policy and contractual framework are most important.

In providing end-users with control, concepts of usability and experience must also be kept in mind. How much control is enough? How much control is too much? End-users are likely less suited to micromanaging technology specifics and may not be experienced in choosing certain professional support services. If the end-user were charged for service provision e.g. resume preparation by a placement service, the end-user would have no ability, and should have no ability, to determine which payment clearing service the service provider uses. But the user does have the right to know that the processing is taking place and that it's being done legally and securely.

Certain issues of Architecture are likewise beyond the scope of end-user determination. The architecture, for example, must determine the level of transport speed and routing that is appropriate. It is impossible for detailed architecture elements to be recalibrated for every transaction. End-users have rights to know these parameters through a disclosure statement, and may be able to choose between security levels and privacy options in profile parameters, but they cannot create a completely individualized infrastructure at the architecture level.

TAS³ creates an architecture that allows for mainly three kinds or user control (see also annex 5). At the outset, the user shall define certain preferences/choices make up the user's personal privacy policy. This policy shall be used inter alia to determine what information shall be shared, over what period of time, for what purposes, and under which conditions. It will also allow the user to specify trust and reputation preferences towards services and providers. This level of policy definition goes beyond previous attempts in P3P and through the proposed PEPs and PDPs provides a more flexible architecture and deployment than EPAL. This policy creates in essence a pre-authorization for use of information that is directly related to and compatible with the terms of the personal policy.

While this general policy is intended to serve multiple purposes, it cannot adapt to all situations or replace needed consent[83] for new or unanticipated uses of information. The intersection of the policy and the transaction will be enabled by a 'call-back' process that alerts the individual to an unanticipated condition or out of policy request for use of or access to information (see D2.1). Thus, the individual is afforded needed transactional controls in TAS³. Part of the testing of the TAS³ architecture through demonstrator projects will help refine the appropriate balance between transactional and policy controls. Functionality, such as a dashboard or summary report may also provide the user with a more

[83] It should be noted that consent as required by the Directive is a default condition of the architecture, thus consent will either be given to a set of actions through a personal privacy policy choice or as needed at the transactional level.

complete picture of information access and use creating greater transparency and accountability.

The third aspect of user control in the TAS³ architecture exists at the level of the sticky policy. The importance of the sticky policy is that it provides greater effect to user controls due to the supported granularity and the fact that it accompanies the data. The combination of personal privacy policies, transactional controls and sticky policies improves the current state of the art in not only providing for better user choice, but also enhancing adherence to those choices.

8 Defining the "How"

As was highlighted earlier in this deliverable, TAS³ will rely on a contractual framework that provides proper binding of rights and obligations across all parties. The contractual infrastructure will need to be multi-level by definition: at the ecosystem level, at the level of the participating organizations and at the technical operational level. Each of these levels needs to be covered by the appropriate binding. Ecosystem contracts will give rise to obligations that cascade down and are further specified. The granularity of bindings will also attach to sticky policies, which provide the most granular operational controls. This is an essential summary of the contractual operations. Further specification of the allocation across technology, policy and contract will need to occur before the granularity of operations can be detailed. While not specified in detail at the framework level, the Ecosystem contracts will also have to define less privacy specific topics that deal with drafting within the 4 corners, severability of clauses, dealing with discovery requests, notice rules related to posting and receipt, among others. Other aspects of contract operation, which need to be supported by technology include: the ability to appropriately version and associate contract terms with transactions/interactions as well as the need to archive these terms.

In the following sections we will start by describing how the intake of organizations that wish to join the TAS³ Trust Network will be organized. It includes a discussion of the steps to be followed from initial application of the prospective TAS³ participant until their contractual binding. After this we will discuss with greater detail the different types of contracts which make up the TAS³ contractual framework.

8.1 TAS³ intake process

TAS³ is committed to developing a community of trust based on end-to-end privacy and security. Data subjects are additionally provided with user-centric controls that enable them to make informed decisions about which service providers to trust and to set the conditions for data processing of their personal data. Many of the functions that support privacy and security at the operational level are implemented in the technology and enforced throughout the TAS³ platform. However, there are clearly certain boundaries to the extent to which technology alone can assure trustworthiness of a system. In order for trust to be established in the TAS³ ecosystem, mechanisms must be provided to evaluate whether TAS³ participants have the appropriate policies and procedures in place to meet data protection requirements and to ensure that user preferences related to the processing of their personal information shall be honoured. Organizations that have these characteristics have been referred to as 'accountable organizations'. Development of organizational structures based on the principles underlying accountable organizations will also help to ensure that TAS³ participants are in fact able to comply with the requirements of the TAS³ governance framework from the outset of their participation (e.g., privacy capability maturity).

The TAS³ intake process is designed to increase assurance that prospective participants to the TAS³ Trust Network have the prerequisite capacity to uphold the obligations they will assume once they become actual members of the Trust Network. This intake process can be broken down into 4 main phases:

- Phase 1: Organizational guidance;
- Phase 2: Self-assessment;
- Phase 3: Gap-Analysis;
- Phase 4: Contractual binding

8.1.1 Organizational guidance

In the first phase of the intake process, prospective participants of the TAS³ Network are provided with guidance concerning the characteristics of accountable organizations. These characteristics ('hallmarks') should be used by prospective TAS³ participants as a template for reviewing or developing their own accountable systems and practices.

As will become evident in reading the characteristics of accountable organizations (cf. *infra*), these must be part of the corporate DNA and they are difficult to test against. This guidance is therefore initially provided more as an articulation a set of goals for participants rather than in the form of actual criteria for participation. When we describe these characteristics we will also elaborate upon how correct implementation of TAS³ can help prospective participants to become more accountable.

8.1.2 Self-assessment

Whereas the characteristics of accountable organisations may be difficult to test against, the implementation of appropriate privacy and security policies (and mechanisms) can be reviewed and evaluated. In the second phase of the intake process, the prospective participant to the TAS³ Network is provided with a self-assessment questionnaire to allow a determination as to whether or not it meets the criteria for TAS³ participation.

The self-assessment is based on concepts that underlie the requirements of the relevant EU laws on privacy and security. In order to facilitate answers, as well as the creation of online and machine-readable versions of the form, we have tried to provide a yes or no format, but in many cases a short explanation may be needed to properly answer the question or provide the context for the yes or no answer.

The self assessment process is useful in several ways. First, it helps the prospective participant to evaluate its existing privacy and security policies and assess its ability to comply with the common privacy and security elements of applicable law. It also provides the prospective participant with the ability to implement any needed remedial action prior to actually submitting its application for TAS³ participation. Most importantly however, this self-assessment will be used as part of the validation of the prospective participant.

8.1.3 Gap analysis

During the third phase of the intake process a gap analysis is performed in which the organizational policies of the prospective participant are compared to the TAS³ reference model policies.[84]

The Gap Analysis is divided into 'required' and 'addressable' elements. The required elements cannot be varied, while the addressable elements can be met in a number of ways.[85] The answers to the Gap Analysis and Self-Assessment Questionnaire will be correlated as part of the validation process.

In both the Self-Assessment Questionnaire and Gap Analysis, evidence of external certification to criteria (ISO 27001, Europrise Seal, etc) should be provided as further proof of the organization's capacity to comply with the TAS³ policy framework. (and by extension the applicable privacy and security requirements) The outcome of Gap Analysis will form the basis of a public attestation of capacity. The public attestation of capacity is a public facing statement of an organisation's capacity to comply. It provides both factual statements of capacity and information on how those statements have been supported and reviewed.

8.1.4 Contractual binding

If the prospective participant has successfully completed the three prior steps it will be asked to enter into contractual relationship. All prospective participants are required to sign the TAS³ Framework Agreement or Ecosystem Contract, which binds them to the policies, general terms and conditions of the TAS³ Network. Additionally, each participant will be required to conclude additional contracts based on the role/functions they will assume within the network as well as be bound to obligations in sticky policies.

8.1.5 Role of the TAS³ intake process

The elements of the intake process which have been outlined above work in unison to provide an enhanced level of vetting and transparency. In today's transactions, a data subject has no or limited assurance of compliance beyond the fact the service provider is obligated to comply with the law. When interacting with service providers that are part of a TAS³ network, there are several ways in which this assurance is augmented. In addition to the fact that network operates on a technical infrastructure which better enables accountability, assurance is also increased due to the fact that:

[84] The TAS³ reference model policies are currently under development and will appear in upcoming iterations of this deliverable.

[85] 'Addressable' should therefore not be confused with 'optional'. The term 'addressable' is simply used to indicate that an entity may have additional flexibility with respect to compliance, without one particular measure being mandatory.

1. the participants of the TAS³ Network have provided information on their polices and procedures that have been evaluated against the established and public policies of TAS³ Network for compatibility;
2. a summary report of the capacity to comply is provided for data subject evaluation, and
3. the participants of the Network have been contractually bound to the obligations contained in the policies and practices of TAS³.

Point 1 is the operational heart of the intake process. The intake process tools include the self-assessment, the reference model policies/requirements and the Gap analysis. The Reference model policies (security and privacy) and the requirements for use of the reference architecture represent the participation criteria of the TAS³ Network. The self-assessment provides insight into the way in which a prospective participant understands the obligations of privacy and security while the Gap analysis to the reference policies provides visibility into the way in which they have implemented systems policies and practices in order to fulfil their obligations. Correlation between the self-assessment and the Gap analysis forms an additional check seeing as failure to grasp a requirement will likely yield an insufficient implementation of the obligation.

8.2 Hallmarks of Accountable Organizations

The concept of accountability is a common element among many of the recent developments that are shaping the future of how we develop trust and compliance paradigms for privacy and data protection. It has also been a recurring theme in recent presentations of the EDPS to the EU inquiry on the review of the Directive.[86]

As we described in more detail in the Privacy Update, the Galway Project carried out important work on Accountability and the Accountable Organizations during this past year.[87] The Galway Accountability Project was overseen by the Irish Data Protection Commissioner in 2009 but will continue in 2010 under the auspices of the CNIL (French Data Protection Authority).

What follows is an extract of the hallmarks of an accountable organization based on the Galway project Discussion Paper concerning the essential elements of data protection accountability.[88] Where appropriate, we will make brief reference to how the proper implementation of a TAS³ infrastructure can help an organization meet several of these accountability hallmarks.

[86] EDPS - Data Protection Officers meeting (Brussels, 2 October 2009): After a general introduction by Peter Hustinx, EDPS, on recent developments in data protection at European and international level underlining the gradual trend towards accountability and responsibility of stakeholders…EDPS Newsletter No. 21, P.8 (October 2009)

[87] See Privacy Update 2009 in TAS³ D6.1, annex 5.

[88] Galway Accountability Project, 'Data Protection Accountability: The Essential Elements, A Document for Discussion', October 2009, available at http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf.

1. Organisational commitment to accountability and adoption of internal policies consistent with external criteria.

- An organisation must demonstrate its willingness and capacity to be both responsible and answerable for its data practices;
- An organisation must implement policies linked to the relevant external criteria (found in law, generally accepted principles or industry best practices) that are designed to provide the individual with effective privacy protection;
- An organization must deploy mechanisms to implement those policies, and monitor those mechanisms;
- Those policies and the plans to put them into effect must be approved at the highest level of the organization and
- Performance against those plans at all levels of the organisation must be visible to senior management. This commitment ensures that implementation of policies will not be subordinated to other organisation priorities;
- An organisational structure must demonstrate this commitment by tasking appropriate staff with implementation of the policies and oversight of those activities.

TAS³ will support this first set of accountability hallmarks through the use of technology supported by a contractual framework that creates a user-centric, trustworthy and compliant system. This correlated and mutually supportive development of technology policy and legal elements supports the required implementation of policies, mechanisms, oversight and performance.

2. Mechanisms to put privacy policies into effect, including tools, training and education.

- The organisation must establish appropriate technical and organisational measures ('performance mechanisms') to implement the stated privacy policies;
    - The mechanisms might include tools to facilitate decision making about appropriate data use and protection, training about how to use those tools, and processes to assure compliance for employees who collect, process and protect information;
- The tools and training must be mandatory for those individuals who oversee and are involved in the collection and deployment of personal information;
- Accountable organisations must build privacy into all business processes that collect, use or manage personal information.

TAS³ provides both performance mechanisms (e.g. policy enforcement points) as well as decision support mechanisms (e.g., reputation engines. TAS³ improves the state of the art by:

- enabling decision support for users through dashboard functions and better ways of assessing reputation;
- automating some of this decision support through transactional tools that enable trust negotiation;

- use of sticky policies that associate restrictions and obligations with the information at a granular level;
- a contractual framework that support compliance obligations across both the ecosystem and the data lifecycle.

3. Systems for internal ongoing oversight and assurance reviews and external verification.

- Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data.
- Accountable organisations establish these performance-monitoring systems based on their own business cultures.
    - Performance systems evaluate an organisation's decisions about data across the data life cycle — from its collection, to its use for a particular application, to its possible transmission across borders, to its destruction when it is no longer useful — and must be subject to some form of monitoring.
- The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to outside vendors and independent third parties.
- The organisation should also periodically engage or be engaged by the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability.
    - Where appropriate, the organisation can enlist the services of its internal audit department to perform this function provided that the auditors report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents.
    - The results of such assessments and any risks that might be discovered should be reported to the relevant entity within the organisation that would take responsibility for their resolution.

These functions are partially enabled in TAS^3, as described in previous sections, but also need to be supported by top-down corporate messaging, appropriate review and oversight of stewardship of personal information and employee awareness and training...

4. Transparency and mechanisms for individual participation.

- The accountable organisation develops a strategy for prominently communicating to individuals its privacy practices.
    - Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires.

    - The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms.
- The accountable organization clearly communicates the name, address and business number of the legal entity responsible for the organization's data processing
- Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate.

- When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice.

Transparency and communication are established in TAS[3] in a number of ways. The intake process review provides transparency about participants regarding their internal processes and their capacity to comply, while the public attestation communicates the results. Transparency and communication are also enhanced by system and organizational notices, and the capacity of the system through the dashboard to not only let users see their own data, but also to see who accessed this data and how it has been used.

5. Means for remediation and external enforcement.

- The organisation should establish a privacy policy that includes a means to address harm to individuals caused by failure of internal policies and practices.
- When harm occurs due to a failure of an organisation's privacy practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism.
- In the first instance, the organisation should identify a first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed.
- The accountable organisation may also wish to engage the services of an outside remediation service to assist in addressing and resolving data subject complaints.
    - Third-party agents, including seal programmes and dispute resolution services, can facilitate the consumer's interaction with the organisation.
- Accountability practices should be subject to the legal actions of the entity or agency with the appropriate enforcement authority. Ultimate oversight of the accountable organisation should rest with the appropriate local legal authority.

TAS[3] provides for both appropriate policies as well as complaint and redress mechanisms. The infrastructure can easily provide for third party remediation organizations (seal programs, dispute resolution services…) or other agents that can facilitate trust. These may be generic trust entities or sector specific, but should be considered at the implementation of a particular deployment of TAS[3]. TAS[3] is not meant to replace existing and effective policy and compliance infrastructures, but rather provides a flexible infrastructure enabling their

incorporation. For example, a number of groups in healthcare and employment already have specialized dispute resolution methodologies in place, the objective would be to enable them rather than recreate them in TAS³.

6. Being an Accountable Organization

Accountable organisations have traditionally established performance systems based on their own business culture. Successful performance systems share several characteristics:

- they are consistent with the organisation's culture and are integrated into business processes;
- they assess risk across the entire data life cycle;
- they include training, decision tools and monitoring;
- they apply to outside vendors and other third parties to assure that the obligations that come with personal data are met no matter where data is processed ('the obligation goes where the information flows');
- they allocate resources based on risk-assessments which take into account the potential harm for individuals; and
- they are a function of an organisation's policies and commitment.

TAS³ works in an complementary manner with an organizational culture; this last set of accountable hallmarks serve more as a checklist of organisational design and behaviour,

8.3 TAS³ Participant Questionnaire

In the previous section we reviewed main characteristics of accountable organisations. As indicated, the organisations seeking to join the TAS³ network will be provided with an overview of these characteristics as guidance for the development and review of their own policies and practices. In order to enable a determination as to whether or not the prospective participant has the capacity to comply with legal obligations of privacy and security, it will be provided with a 'Participant Questionnaire' (PQ). The completion of this PQ forms the second phase of the intake and validation process for prospective TAS³ participants.

The current draft of the Participant Questionnaire is included in annex VI of this deliverable. It will be developed and refined over the course of the project.

The current Participant Questionnaire is designed to address the requirements incumbent upon a controller – an entity that can exert dominion/make decisions over the information (rather than for a processor – an entity that merely executes operations/follows instructions on the information). As we better understand the utility of the PQ in the vetting and validation process we plan to develop multiple model questionnaires. These would cover situations of:

- Controller with access to sensitive personal data
- Controller with access to personal data
- Processor with access to sensitive personal data

- Processor with access to data
- Service provider with incidental access to data without knowledge of the nature of the data

The questions in the current questionnaire were based on a questionnaire being developed by APEC to evaluate organizations that wish to qualify their privacy policies and cross border transfer rules with the APEC Privacy Framework[89]. The utility of using this model questionnaire is that it is being developed by a multi-stakeholder drafting group, consisting of government, industry, data protection authorities and civil society as part of an APEC Pathfinder Project. The APEC Privacy Framework is based on the OECD Privacy Guidelines, but with a highlighted focus on accountability. Note that the last section of the Questionnaire focuses specifically on accountability.

8.4 The Gap Analysis

TAS³ will develop model policies for privacy and security as well as a set of model infrastructure requirements. These policies and requirements will contain elements that are considered either 'required' or 'addressable'. The required elements cannot be varied, while the addressable elements can be met in a number of ways.[90]

The Gap Analysis is the part of the intake process where the prospective participant will map their own policies and infrastructure to those required by the TAS³ Network. This process will, as the title implies, help to identify the any gaps that exist between. Where prospective participants have chosen different ways of implementing the addressable requirements, an assessment will need to be made as to the sufficiency of those implementations.

In the event that the Gap analysis demonstrates a failure of implementation of required elements, the prospective participant can either immediately remedy those deficiencies or provide a plan and timetable for achieving compliance which will then later be reviewed for sufficiency.

The final step of the gap analysis is providing a summary **Attestation of Capacity**. The purpose of the attestation is to provide a public facing summary statement concerning the compliance capability of the organization, as well as references to relevant underlying proof or certifications. This information enhances transparency and enables more informed trust decisions by users. The attestation also serves as a material public statement of the organization that

[89] http://aimp.apec.org/Documents/2009/ECSG/SEM1/09_ecsg_sem1_027.doc This is a presentation of the privacy work going on within APEC. Project 1 is the questionnaire for guidance. As the questionnaire is a non-public document, this version needs to remain in limited circulation till APEC publication which should occur next year.

[90] 'Addressable' should therefore not be confused with 'optional'. The term 'addressable' is simply used to indicate that an entity may have additional flexibility with respect to compliance, without one particular measure being mandatory.

would be enforceable by law against the organization if it misrepresented its capacity to comply[91].

An additional reason for drafting the Attestation of capacity lies in the fact that replies to the Gap Analysis and the documents presented in support may contain information at a level of specificity that could compromise the organizations underlying systems and are therefore less suited for general publication[92].

The Gap Analysis must be completed as part of the application process. All aspects of the questions must be answered. It is essential to provide sufficient detail to assess the compliance with requirements. Prospective participants are encouraged to support their applications with relevant external certifications and other objective elements of proof where they exist.

> Where gaps exist in relation to addressable elements, prospective participants of the Network must provide a detailed explanation of what processes and solutions they have implemented and why they should be considered equivalent or sufficient. Where the Gap Analysis reveals discrepancies between the applicant's policies or infrastructure and the required elements, the applicant must provide a detailed analysis of the steps it has or is taking to remediate these discrepancies, including any timeframe for completion.

8.5 Contractual binding

Clearly none of the criteria for participation set forth during the intake process are irrelevant if the prospective participant is not bound to their obligations. The intake is concluded by binding participants to the general obligations of TAS³, through the signing of the TAS³ Framework Agreement. This contract is signed by all users and participants and binds them to the general policies, terms and conditions related to the use of the TAS³ architecture.

8.5.1 The TAS³ framework agreement

The TAS³ Framework Agreement or Ecosystem contract shall have the following properties:

i. The ecosystem contract will bind signatories to the general requirements of TAS³ that embed data protection requirements as appropriate to the role.
ii. The ecosystem contract will require that signatories adopt TAS³ policies or have demonstrated that they have substantially similar policies that meet TAS³ minimum requirements
iii. The ecosystem contract will require that signatories agree to use information accessed or provided only to accomplish

[91] While most consumer protection laws would already make such a public statement enforceable against the organization, the Ecosystem Contract will also bind the organization to their Attestation of Capacity.

the services requested and to maintain the information in identifiable form for only that period of time.

iv. The ecosystem contract requires that signatories comply with any instructions restricting use of or access to data, which may be provided either technically (sticky policies etc) or otherwise from the data subject or upstream service provider.

8.5.2 Other Contracts

The TAS³ contractual framework operates on three different levels. The first level pertains to the infrastructure or 'ecosystem level (cf. supra).

The second level of the contractual framework is at the level of the participants to the TAS³ Network. This is the level at which the respective functions and roles of entities participating to the TAS³ network are contractually addressed. These contracts contain supplemental instructions and obligations in light of the specific transactions the participant is likely to engage in. The contracts of this type are referred to as 'TAS³ Participant Contracts', which supplement the TAS³ Ecosystem Contract. The contracts at this level may exist in two forms. For entities that are most likely to play one or a limited number of roles with clearly delineated functions, it may be possible to draft single role-based participant contracts to supplement the Ecosystem Contract. These contracts are likely to be of a more general application and could be concluded during the intake process. For participants with more dynamic or varying functions/roles, which are more context-dependent, it will not be possible to conclude all the relevant participant contracts during the intake process. Many role-based obligations will only be definable at the moment where it is clear which transaction is envisaged. This creates the need for a more dynamic contracting process. By specifying obligations based on roles and functions at the transactional level, we will be able to rapidly tailor the obligations of participants in accordance with the types of processing operations they are expected to perform. This contracting 'on-the-fly' (CotF) model will be developed based on the same concepts that underlie service oriented architectures or object-based programming. We will explore developing an automated process functions for associating predefined roles and obligations to participants based on uses of information.

The third level of the contractual framework is at the technical operational level. This is the level at obligations and restrictions are associated to personal data elements in the form of sticky policies.[93] . The Ecosystem Contract will ensure legal binding and effect to restrictions and obligations contained in those sticky policies by ensuring that participants agree to be bound to follow the instructions provided at the technical operational level. The latter is important as some legislation may still require the concept of a "writing" (written document) to give legal effect to such an instruction.

[93] For more information concerning use of sticky policies in TAS³ see TAS³ D7.1 (Design of Identity Management, Authentication and Authorization Infrastructure) and TAS³ D2.1 (Architecture).

8.5.3 Archiving, Versions and Limitations

There will need to be an archive and naming/versioning system which makes it possible to later determine the version of instruments that controlled any particular transaction.

At this juncture, however, it is useful to assure that we shall limit the boundaries between contract operations and user choices. An example may be informative. The TAS[3] infrastructure utilizes tools such as reputation engines which enable end-users to help select service providers either directly or through more automated means whereby reputation indicators will be required as part of a profile or discovery process. In either case, the choice of provider is part of the subjective nature of the system that reflects user control. The legal/governance framework is responsible for helping require that: providers post true and correct information; system parameters and legal frameworks are respected; that obligations are maintained; and that consequences exist for failures to comply. The contractual framework supplements and informs trust negotiation, but neither controls nor replaces it.

9 Oversight and complaint processing

No system is perfect and all systems must address the need for oversight compliance and redress. Reviewing a complaint process provides insight into contract enforcement.

1. Complaint process.
    1. Complaints are not limited to privacy violations but may include failures of service and other operational issues that do not implicate personal information. While they will be addressed in the contractual framework, they will not be dealt with in this example.
    2. A complaint related to the use/misuse or loss of personal data will trigger multiple solution paths mandated by the Ecosystem contract.
        1. While data subjects are never denied their right to consult or complain to competent governmental authorities, they are first encouraged to report the issue to responsible TAS³ organization.

            NOTE: If they cannot determine which organization that is there will be a general complaint process that enables the Trust Guarantor or its delegate to appropriately route the complaint.
        2. For complaints of a nature that implicate possible abuse of the system or other risks to the system the service provider receiving the complaint must inform the trust guarantor or delegate of the issue.

            NOTE: One of the first priorities of any incident response is to contain the incident and limit potential harm from the incident. All efforts will be made to preserve needed evidence on the source of the threat to (external) or abuse of (internal) the system.
        3. Depending on the nature of the complaint, appropriate investigatory processes will ensue. Recourse will be had to appropriate audit trail and other information needed substantiate actions and processes.
        4. As the investigatory process proceeds, there will be a requirement to keep the data subject informed of the process where appropriate.
    3. After the investigatory stage is complete, a redress phase will ensue to assure that that the data subject is provided appropriate redress. If this is in the form of compensation, the primary responsibility will lie with the service provider at fault. Should that not be sufficient or should the fault be considered to exist at a more systemic level, processes will be undertaken to determine how to appropriately allocate

liability. As was highlighted earlier, this topic is not yet completely defined.

1. Intentional or criminal acts by the service provider would be referred to appropriate legal authorities as needed and would result in termination of TAS³ affiliation
2. If a service provider is at fault, but not with intent, they may be provided with an opportunity to cure any policy, process or system issues within a defined period of time or lose TAS³ affiliation.
3. Should the actions warrant, information would also be reflected in service provider profile or reputation information.

4. A debrief of the incident will take place after the investigation is complete to determine whether elements of the Trust Network need to be updated. The response and investigatory process will also be reviewed. Part of the latter review will include a consideration of whether appropriate logging and audit controls exist to both trace and prove inappropriate actions after the fact as well as whether there might be better ways to detect them in real time. This analysis will be done in an appropriate risk analysis context.

Finally review will be had of whether changes to information collection or identification practices are required (e.g. whether more limited collection or greater utility of pseudonymous or anonymous functions need to be promoted). This may also include the need to provide better guidance to users or service providers.

10 Conclusion

TAS³ improves on traditional 'Privacy by Design' approaches by going beyond consideration of just technology in the design phase. The consideration and coordination of privacy issues across technology, policy, business and legal elements during the design stages creates a more seamless and mutually supportive method of privacy compliance. Technology is also better used to support compliance and oversight. Legal instruments and organizational policies are better used to support the technology and enforce the obligations of the service providers. This more holistic approach is also fundamental to design the type of accountable systems that we will need to deal with in today's information society. TAS³ plays a valuable role in testing the capacity of such collaborative development, design and implementation.

TAS³ also improves existing approaches to user-centricity by combing both credential and relationship management approaches. This provides users with greater functionality through enhanced control options. These combined approaches are supported at both the architecture and policy/contract level to create a user-centric ecosystem, as opposed to just better controls within a particular application. This ecosystem approach is important as today's users operate in a world of global information flows, complex value chains and information intensive technologies.

Today's global information society also poses increasing challenges to the application of privacy laws that were developed before the true advent of the Internet. Applying existing notice and consent models is more challenging in an age of ubiquitous information processing. A number of data protection authorities, and other stakeholders, are exploring models of accountability, which can supplement and extend the privacy principles inherent in the Directive. These accountability frameworks will require systems developed to meet their inherent technical and governance needs. TAS³ is a first attempt at the development of such an accountable system.

11 Annexes

11.1 Annex I – Core of PCI DDS

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data
Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

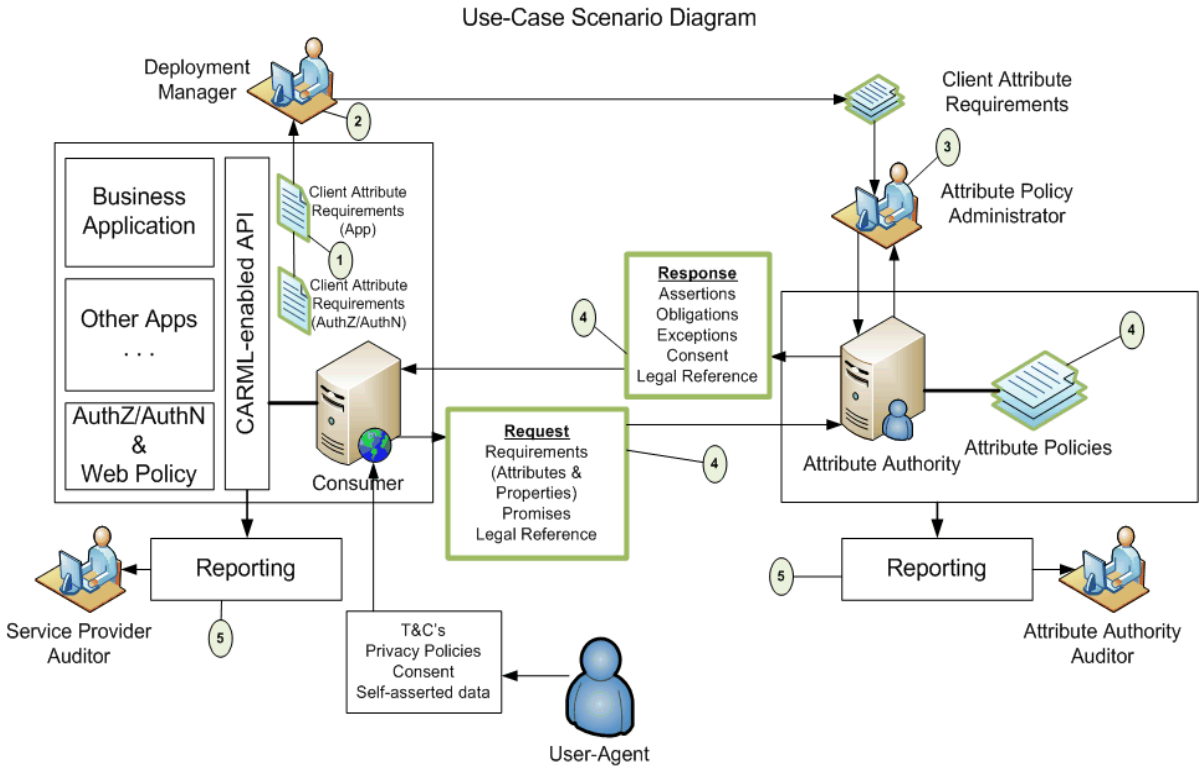
Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

11.2 Annex II – Use-case scenario diagram



In the diagram, above, the relationships between the deployed application environment, the attribute authority, and the end-user are shown:

1. Developer – the developer declares the attribute requirements of the application.

2. Application Deployment Manager – determines how attributes will flow to/from the application, what information is gathered directly from the user under what Ts and Cs, and what information will come from back-end systems and federated partners.

3. Identity Services Manager/Attribute Authority Manager – Attribute authorities are contacted for permission to use information by providing an appropriate declaration. If the Attribute Policy Administrator approves, then the attribute policy for the Attribute Authority can be revised to enable access by the client business application.

4. Client application – Access identity information sources using CARML declarations and AAPML policy enforced providers.

5. Audit Reporting – Auditors on both sides audit the consumption and publication of identity-related information.

Source: Liberty Alliance: An Overview of Id Governance Framework v1.0

www.projectliberty.org/liberty/content/download/3500/23156/file/**overview-id-governance-framework-v1.0**.pdf

11.3 Annex III - Definitions

Article 2 Definitions (Directive 95/46/EC)[94]

For the purposes of this Directive:

(a) 'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b)'processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

[94] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h)'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

UK Data Protection Act Definitions

Data Controller

A Data Controller either alone or jointly with others determines the purposes for which data is to be used. If you wish to use data for a new purpose you should seek guidance from the Head of Information Compliance & Policy.

Data Processor

Any person or organization (other than an employee of the data controller) who processes the data on behalf of the data controller. An example of this might be a payroll bureau.

Data Subject

The living individual to whom the data relates who is therefore the subject of personal data.

Personal Data

Data relating to a living individual who can be identified from the information, or any other data likely to come into the possession of the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing

The collecting, amending, augmenting, deleting or re-arranging of the data or extracting information by means of reference to the data subject to whom they will/may be disclosing. Basically anything that can be done with data!

Sensitive Data

The Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:

- the racial or ethnic origin of the data subject,
- their political opinions,

- their religious beliefs or other beliefs of a similar nature,
- whether they are a member of a trade union,
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Where such data is being processed not only must the controller meet the requirements of the Principles and Schedule 2, but also processing is prohibited unless at least one of the conditions in Schedule 3 can be satisfied. The explicit consent of the individual will usually have to be obtained before sensitive data can be processed unless the controller can show that the processing is necessary based on one of the criteria laid out in Schedule 3 of the Act.

Subject Access Request

Every living individual has the right of access to personal data held about them by City University and to be informed whether personal data of which that individual is the data subject are being processed. This is known as a SAR (Subject Access Request)

Third Party

Any person other than the data subject, the data controller, any data processor or other person authorized to process data for the data controller or data processor.

Source: City University of London – Data Protection Act Definitions - http://www.city.ac.uk/ic/dataprotection/dpadefinitions.html

11.4 Annex IV – WP 6 Requirements list

The legal requirements can be broken out into three main sections, namely: intake processes, legal requirements and contractual framework requirements.

Intake Processes (enrolment): All participants will need to be vetted and contractually enrolled in the system (intake processes) so that their obligations are clarified and made binding on the participating entities (individuals and organizations).

Individuals will need to be identified and registered in the system and provided with appropriate access rights and credentials that will allow them to use the system. Processes related to identification, levels of assurance, the types of external credentials and review/validation methods will be specified as part of the development of the intake process. During the intake process they must also subscribe to using the system client software as well as agree to be bound by the choices and transactions they engage in. Prior to executing any instrument or transaction, they must of course also be provided with a complete notice related to privacy in the system, their ability to exercise control as well as the compliance, redress and oversight functions.

Organizations will also need to go through an intake process, but in addition to notice, identification and validation, the ability of the service provider to use and deploy the TAS³ Architecture, their policies and their ability to comply with the requirements of TAS³ shall also be reviewed.

Legal requirements: The legal requirements of TAS³ emanate primarily from the EU Data Protection Directive and its national implementations. While these requirements apply as a matter of law to all the actors and the transactions involved, TAS³ has chosen to specify them as requirements and incorporate them into the policy and contractual framework. The recital of these legal requirements in these instruments will help achieve compliance and oversight across TAS³ by making those requirements actionable and enforceable by the parties responsible for oversight. Obviously recourse to national data protection authorities and the courts always remains possible, but we also hope to provide the data subject with more simple paths to compliance enforcement that can be accomplished within the TAS³ network (through its architecture and participants).

Contract and Policy Framework: The combination of TAS³ policies and the contractual framework creates a data governance model for TAS³. TAS³ consistent policies will reflect both the legal requirements as well as the need to respect choices of data subjects that may create even greater restrictions on the collection and/or use of data. The policies and contractual framework are being designed to both support and complement the technical infrastructure. The contractual framework operates on three different levels. The first level pertains to the infrastructure or 'ecosystem level'. This contract is signed by all users and participants and binds them to the general policies, terms and conditions related to the use of the TAS³ architecture. This contract is referred to as the 'TAS³ Framework Agreement' or the 'TAS³ Ecosystem Contract'. This contract will also

specify how and to which entity complaints and concerns should be addressed. The terms related to data subjects signing this contract will be limited to those expressed in the intake process, with an additional obligation to take reasonable steps to maintain the security of the password/credential they use to log into the system and not to engage in prohibited/fraudulent/deceptive activities on the system.

The second level of the contractual framework is at the level of the participants to the TAS³ Network. This is the level at which the respective functions and roles of entities participating to the TAS³ network are contractually addressed. These contracts contain supplemental instructions and obligations in light of the specific transactions the participant is likely to engage in. The contracts of this type are referred to as 'TAS³ Participant Contracts', which supplement the TAS³ Ecosystem Contract.
The contracts at this level may exist in two forms. For entities that are most likely to play one or a limited number of roles with clearly delineated functions, it may be possible to draft single role-based participant contracts to supplement the Ecosystem Contract. These contracts are likely to be of a more general application and could be concluded during the intake process. For participants with more dynamic or varying functions/roles, which are more context-dependent, it will not be possible to conclude all the relevant participant contracts during the intake process. Many role-based obligations will only be definable at the moment where it is clear which transaction is envisaged. This creates the need for a more dynamic contracting process. By specifying obligations based on roles and functions at the transactional level, we will be able to rapidly tailor the obligations of participants in accordance with the types of processing operations they are expected to perform. This contracting 'on-the-fly' (CotF) model will be developed based on the same concepts that underlie service oriented architectures or object-based programming. We will explore developing an automated process functions for associating predefined roles and obligations to participants based on uses of information.

The third level of the contractual framework is at the technical operational level. This is the level at obligations and restrictions are associated to personal data elements in the form of sticky policies.[95] . The Ecosystem Contract will ensure legal binding and effect to restrictions and obligations contained in those sticky policies by ensuring that participants agree to be bound to follow the instructions provided at the technical operational level. The latter is important as some legislation may still require the concept of a "writing" (written document) to give legal effect to such an instruction.

While beyond the scope of TAS³, participating organizations must develop appropriate clauses within their employment contracts and related policies to assure that employees are properly bound to organizational policies that correctly reflect these obligations.

[95] For more information concerning use of sticky policies in TAS³ see TAS³ D7.1 (Design of Identity Management, Authentication and Authorization Infrastructure) and TAS³ D2.1 (Architecture).

The following requirements have been developed from the legal and contractual framework set forth D6.1 and D6.2. Some of these requirements were initially defined in D1.2. The current list of requirements is a refinement and further elaboration of those requirements based on the increased understanding of the architecture and the deliverables of other partners. This list is not exhaustive and will continue be updated in future versions of this document. For readability purposes, we have grouped the requirements below in terms of data protection and more general operational requirements. Several requirements additionally have explanatory 'notes' associated with them to draw attention to certain specificities or additional considerations which need be taken into account during implementation.

1. Enrolment and contractual binding

- Req 6.1: Intake Process (Person). The intake process MUST include: documentation provisioning (including notice of privacy policy, disclaimers, and general terms & conditions) and agreement to be bound; validation of identity (proofing) with an appropriate level of assurance; and specification of a technical user interface.
- Req 6.2: Intake Process (Organization). The intake process MUST include: documentation provisioning (terms & conditions, privacy policies, disclaimers) and agreement to be bound; validation of identity with an appropriate level of assurance; verification of policies, contracts, infrastructure and the capacity to comply; and specification of a technical interfaces and protocols.
- Req 6.3: Contract management. All participants to the TAS³ network MUST agree to adhere to and execute the relevant TAS³ contractual documents.
    - Req 6.3.1: A versioning and archiving system MUST exist for contract terms.
    - Req 6.3.2: A versioning and archiving system MUST be in place for the informed consents given by data subjects.
    - Req 6.3.3: It MUST be easy to ascertain which terms were in force, after the fact, if an issue arises (e.g. pursuant to a complaint or detected anomaly).

- Req 6.4: Use of TAS³ Technology and Processes. All parties MUST agree to use the relevant TAS³ or TAS³ compatible, technology and processes.

- Req 6.5: Agreement to be bound. All parties MUST agree to be bound to the obligations they take on both by becoming and being part of the TAS³ network, as well as those which are the result of transactions or choices they exercise through the TAS³ Architecture.

- Req 6.6: Binding Effect of technical processes & policies. All parties MUST agree to be bound by the technical processes in the architecture, including technical policy enforcement and logging mechanisms (to the extent that they are working properly and their properties have been appropriately disclosed and consented to).

Note: The TAS³ architecture also supports sticky policies.

- Req: 6.6.1: The content of the instructions contained in (sticky or other) policies and the obligations associated with those instructions MUST be respected across the TAS³ architecture;
- Req 6.6.2: It MUST be ensured that commitment to communicated policies and privacy preferences cannot be repudiated at a later time;
- Req 6.6.3: In instances where personal data will be further processed outside the TAS³ network/architecture, the recipients of this data must commit to continued adherence to the content of associated sticky policies or other usage directives;
- Req 6.6.4: Policy information MUST be easily accessible to all relevant parties;
- Req 6.6.5 Policies MUST be drafted and communicated in a way that is appropriately tailored to and accessible by its intended audience[96];
- Req 6.6.6: The policies should be drafted to enable all parties to understand their scope of application and which resources (data, services etc.) are governed by which policies

- Req 6.7: Implementation of Required Policies. Organizational participants in the TAS³ network MUST implement TAS³ defined or compatible policies specified in the contractual framework (e.g. internal privacy and security policies) or as approved during the intake process.

- Req 6.8: The TAS³ policy framework MUST cover all aspects of data processing and the associated legal data protection requirements.

2. Assignment of roles and responsibilities

- Req 6.9: Allocation of roles and responsibilities: Responsible entities and roles MUST be defined for at least the following tasks:
  - receiving and registering consent;
  - providing notice and transparency;
  - performing the required authentications, authorizations and checks for every processing operation;
  - the maintenance of logs for the different processing operations that take place;

[96] See: UK ICO: Privacy Notices Code of Practice (2009) at pp. 11-12; http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf (for general consideration of drafting public facing documents related to privacy. These concepts are further reflected in codes of practice e.g. UK ICO Framework Code of Practice for Sharing personal information (2009 Consultation Draft at P.7): On the avoidance of legalistic language and adopting a plain-English, readable approach see http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_information_sharing_framework_draft_1008.pdf

- trusted (third) party services (e.g. attribute certification, identifier conversion etc);
- enforcement and updating of technical policies in accordance with permissions granted by data subject and legal developments;
- front-end accommodation of the rights of data subjects such as the right of access and correction;
- oversight; including regular verification of compliance, redress and point-of-contact in the event of a security breach.

3. Legitimacy of processing

- Req 6.10: Consent: Collection, use, and subsequent use, of personal data MUST be compatible with the purposes specified and MUST be with the informed consent of the data subject EXCEPT where mandated by law or through an exception recognized in law.
    - Req 6.10.1: Data subject consent legitimizing the processing MUST be freely given, informed[97], and unambiguous[98].
    - Req 6.10.2: Where required by the competent jurisdiction (e.g. in case of processing of health data), or where this is considered desirable for later evidentiary purposes, the consent of the data subject MUST be in writing (or electronic equivalent thereof).
- Req 6.11: In instances where the data subject cannot provide his consent to the processing in a valid manner (e.g. relationship of command), an alternative legally permitted ('legitimate') basis MUST be present to justify the processing.[99]
- Req 6.12: Consent Capture for New or Changed Use: If the use of information changes or if there is a new use of information there MUST be a new informed consent obtained prior to the new or changed use of information. (see also Req 6.16).[100]
- Req 6.13: The TAS³ network SHOULD provide the data subject, if so desired, with the ability to express his privacy preferences in a granular fashion (avoid "all or nothing" approach when possible; support individual privacy preferences)
- Req 6.14: The TAS³ network SHOULD consider technical policy enforcement mechanisms which can establish that there is in fact a legal basis for the processing prior to authorizing an action (e.g. by specifying them as policy conditions or through use of sticky policies)

[97] A consent may be considered informed when it satisfies all the elements listed in Req 6.44.
[98] From a technical point of view, this requires that the user "opts in" to the processing of personal data.
[99] See articles 7-8 of the Data Protection Directive.
[100] In instances where the subsequent processing cannot be based on the consent of the data subject, an alternative legally permitted ('legitimate') basis must be present to justify the subsequent processing (see Req 6.11).

4. Finality

- Req 6.15: Purpose specification. The purpose(s) for collection and subsequent processing of personal data MUST be clearly specified.

  Note: the purpose(s) of processing MUST be identified in advance (prior to initial collection, transfer …).

- Req 6.16: Purpose binding/limitation: If the use of information changes or if there is a new use of information which cannot objectively be considered as compatible with the originally specified purpose there MUST be a new consent obtained prior to the new or changed use of information (unless this processing is explicitly required or permitted by law).[101]

- Req 6.17: Each participant of the TAS³ network MUST have a privacy policy that articulates restrictions and obligations with regards to subsequent use of the personal data it has under its control.

- Req 6.18: When personal data is forwarded from one TAS³ participant to another (or from a participant to a non-participant), it MUST be determined under which policies (in particular: under which restrictions and obligations) this data is being passed on.[102]

    - Req 6.18.1: Such data handling policies MUST be compatible with the TAS³ governance framework;

    - Req 6.18.2: The data recipient MUST be legally bound to restrict itself to authorized usage and to execute the specified obligations specified in these data handling policies (see also Reqs 6.5-6.6);

    - Req 6.18.3: The data subject SHOULD be provided with additional and explicit information if the if a requestor/future recipient of information is not a part of the TAS³ network.

- Req 6.19: Technical policy enforcement mechanisms SHOULD be able to take into account the specified purpose when evaluating a processing request (e.g. through sticky policies and/or policy conditions).

- Req 6.20: In order to assure that there is a legitimate basis for processing, and to assist in compliance verification functions, there MUST be appropriate logging of asserted purposes and the ability to audit how the information was used against the purpose for which it was collected (see also Reqs 6.63-6.65).

  Note: Seeing as such information (the purpose for which a processing can be authorized / has taken place) can be highly-sensitive in and of itself, careful

[101] In instances where the subsequent processing cannot be based on the consent of the data subject, an alternative legally permitted ('legitimate') basis must be present to justify the subsequent processing (see also Req 6.11).
[102] This will typically only be a subset of the actions the forwarding entity is authorized to perform.

consideration MUST be given to deciding which entity shall be trusted to register and verify the asserted/permitted purposes.

5. Data minimization

- Req 6.21: The collection and further processing of personal data MUST be relevant and non-excessive in relation to the specified purposes (see Req 6.15).

  Note: the processed data must also be adequate to achieve the specified purpose.

- Req 6.22: Collection Limitation: The TAS³ network and related processes MUST install appropriate limits on personal data collection to what is needed for legitimate, identified and notified business purpose. The system must be supplemented by explicit policies that limit employee access to data based on business need.

- Req 6.23: Response to attribute requests: Technical policy enforcement mechanisms MUST have the ability to respond to data requests with only that information that the requesting entity is authorized to receive (sufficient level of granularity).

- Req 6.24: Selective attribute/personal data disclosure during authentication: Authentication protocols MUST be designed in a way which ensures that no more attributes/personal data than needed for the processing are verified or propagated (e.g. avoid unnecessary leaking of identifiers).

    - Req 6.24.1: Mechanisms SHOULD be in place to enable the user to choose which identity providers and/or attributes shall be used for a particular service, subject to applicable policy (e.g. minimum level of assurance, prerequisite attributes for authorization decision etc.).

- Req 6.25: Storage limitation: Procedures MUST be in place to ensure destruction or anonymization of personal data once the purpose for which it was collected and/or further processed has been completed

    - Req 6.25.1: Prior to initiating any processing operation upon personal data, the storage duration of each data element MUST be specified, either individually or by category, for every entity that is involved in the processing. This SHOULD be done as part of the service/process definition.

    - Req 6.25.2: Data Management. Data MUST be managed according to a data life cycle which describes its management from collection to deletion, and all processes in between, including which events trigger which processes.

- Req 6.25.3: The TAS³ network SHOULD support technical obligations languages which allow data providers to specify the time-span after which deletion is mandatory.

Note: determining appropriate storage duration MUST also take into account the need for accountability at a later time, as well as legally prescribed retention periods. In case the data only needs to be retained for a subset of the initially specified purposes, appropriate measures MUST be taken to limit the further processing to these (more limited subset of) purposes (e.g. encrypted archiving).

6. Data accuracy

- Req 6.26: Designation of authoritative sources: In order to ensure data accuracy to the fullest extent possible, an inventory MUST be maintained that describes which entities are authorized to act as data providers (authoritative source) for which data sets.

- Req 6.27.: Verification procedures MUST be in place to ensure the trustworthiness of each attribute with a level of assurance proportionate to the interests at stake.

    - Req 6.27.1: Where appropriate, review and update procedures MUST be in place for personal data which is being kept for an extended period of time.

- Req 6.28: Procedures MUST be in place on how to report and deal with suspected inaccuracies.

    - Req 6.28.1: Data subjects MUST have the ability to check the accuracy and quality of the data, and to report suspected inaccuracies. (see Reqs 6.51, 6.53, 6.55 and 6.61);

    - Req 6.28.2: In the event of indirect collection, prior to further processing the accuracy of the data SHOULD be verified with the data subject where this is both possible and appropriate;

    - Req 6.28.3: In case of amendment, notification MUST be provided to relevant entities (e.g. entities to whom data has been forwarded / who have accessed the data and continue to rely on it) (see also Req 6.58)

- Req 6.29: Where further verification or assurance of data quality is still needed, there MUST be a clear indication of the need for further verification when appropriate.

    - Req 6.29.1: Indication of level of confidence: each element of personal data has a 'level of confidence' associated with it (e.g. self-asserted, verified with authoritative source by trusted data manager, inaccuracy

reported etc) and this level of confidence should be reflected in its meta-data where appropriate.

- Req 6.30: The integrity of data maintained in authoritative sources MUST be appropriately guaranteed.
    - Req 6.30.1: Modification rights MUST be restricted to authorized entities on a 'need-to-modify' basis.
- Req 6.31: Data to and from authoritative sources SHOULD be authenticated through use of appropriate data origin authentication protocols to ensure authenticity and integrity.
- Req 6.32: Relying Parties and other data recipients MUST commit to only process personal data further if there is sufficient certainty as to its origin and integrity (i.e. upon verification that it emanates from the trusted source and has not been subject to unauthorized manipulation).
    - Req 6.32.1: Policies MUST be in place which specify how a 'sufficient level of certainty' as to the origin and integrity of personal information is established.

7. Confidentiality and security of processing

- Req 6.33: Confidentiality. Appropriate organizational and technical security measures MUST be in place to ensure the confidentiality of personal data.
- Req 6.34: Security. Appropriate technical and organizational measures against unauthorized/unlawful/accidental access; modification, disclosure, destruction, loss or damage to personal data MUST be in place.
- Req 6.35: An organizational framework for information security management (describing both organizational and technical measures) MUST be in place.
- Req 6.36: Identity and credential life cycle management. Policies and measures to ensure appropriate identification and authentication of entities attempting to perform a particular action MUST be in place.
    - Req 6.36.1: Identities and credentials MUST be managed in way that they continuously provide a level of assurance proportionate to the interests at stake;
    - Req 6.36.2: Common authentication approaches and rules MUST be defined and enforced;
    - Req 6.36.3: Adequate policies specifying minimum levels of entity authentication assurance in a manner that is proportionate to the interests at stake MUST be in place;
    - Req 6.36.4: Adequate procedures to ensure proper verification of relevant attributes of requesting/asserting entities (e.g. a pre-requisite

professional qualification) MUST be in place (e.g. through use of authoritative sources as an integrated component in user- and access management).

- Req 6.37: Authorization. Technical policy enforcement mechanisms MUST support a sufficient level of granularity with regards to the access and further processing rights (privileges) of each requesting entity. To this end at least the following measures MUST be taken:

    - Req 6.37.1: A list and directory of resources, potential data recipients and applications MUST be made.

    - Req 6.37.2: Personal data contained in data repositories MUST be categorized according to a classification system that recognizes type and sensitivity of data.

    - Req 6.37.4: Roles and privileges of each entity MUST be defined based on legitimate organizational needs (in other words, on a "need-to-process" basis).

    - Req 6.37.5: For each object that qualifies as personal data a list of valid recipients MUST be defined or definable immediately upon request at any point in time;

    - Req 6.37.6: Acceptable purposes for access to data categories MUST be defined, emergency procedures for access beyond those purposes SHOULD also be defined.

    - Req 6.37.7: Authorization profiles for resources MUST be defined and enforced; indicating which resource is accessible to which type of entity/application in which capacity, in what situation and for what period.

    - Req 6.37.10: Adequate measures and procedures MUST be in place to properly address security breaches, including notification of relevant entities (e.g. audit & oversight committee)

    - Req 6.37.11: Adequate measures and procedures MUST be in place to support enforcement of authorization policies at both central and local levels.

- Req 6.38: Use of cryptography. TAS³ MUST support the use of cryptography to ensure confidentiality, authenticity and integrity of personal data where appropriate.
  Note: this requirement pertains both to transmission (channel security) and storage

- Req 6.39: Avoid unnecessary linkability. TAS³ SHOULD support advanced pseudonym management to limit the level of linkability or correlation among personal data where appropriate.

- Req 6.40: Physical access restriction: Physical access to terminals and other resources MUST be restricted where appropriate.

- Req 6.41: Each participant MUST adopt internal privacy policies documenting security measures (specifying inter alia the persons responsible within the organization (security officers), what to do in the event of a security breach etc.).[103]

- Req 6.42: Confidentiality agreements. Natural persons who are employed by (or otherwise perform services for) TAS³ participants MUST be bound by a contractual duty to respect the confidentiality of data when this is required by law.[104] TAS³ SHOULD consider instituting such an obligation towards all TAS³ participants.

The list of organisational and technical measures described here is by no means exhaustive. Additional examples of potential obligations pursuant to the requirements of confidentiality and security are listed below the requirements.*

8. Transparency and notice

- Req 6.43: Whenever personal data shall be processed, the following MUST be specified: the identity of the controller, what data is collected and how, why it is being collected (purpose of the processing), how it will be used, who it might be shared with, and how it will be managed.[105]

8.1 *Direct collection*

- Req 6.44: Notice requirements where data is collected from data subject herself (direct collection):
    - Req 6.44.1: In case of direct collection, the data subject MUST be provided with the following information (except where he already has it):
        - the identity of the controller (and, if applicable, of his representative);
        - the purposes of the processing for which the data are intended;
    - Req 6.44.2: The data subject SHOULD also be informed of:

[103] Such policies must of course be compatible with the TAS³ governance framework (see Req 6.7).
[104] E.g. in certain jurisdictions such agreements are required when such employees or contractors are charged with handling of sensitive data such as health data.
[105] The data subject MUST in principle be notified of the elements listed in Req 6.43 prior to initiating any (entirely new or 'incompatible') processing operation involving personal data (or at least have access to this information upon request – see Req 6.53). The instances and modalities of the notice obligations are described in more detail in subsections 8.1-8-2. Subsection 8-3 provides some additional guidance towards the implementation of these requirements in TAS³.

- the recipients or categories of recipients of the data;
- whether replies to questions he is asked are obligatory or voluntary, as well as the possible consequences of failure to reply;
- the existence of the right of access to and the right to rectify the data concerning her.

- Req 6.44.3: The data subject MUST be provided with the information listed in Req 6.44.2 when this is necessary to guarantee fair processing in respect of the data subject, when considering the specific circumstances in which the data are collected.

8.2 *Indirect collection*

- Req 6.45: Notice requirements where data is not obtained directly from data subject herself (indirect collection):
  - Req 6.45.1: In case of indirect collection, the data subject MUST**, at the moment of undertaking, or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, be provided with the following information:
    - the identity of the controller and of his representative, if any;
    - the purposes of the processing;
  - Req 6.45.2: The data subject SHOULD also always be informed of:
    - the categories of data concerned;
    - the recipients or categories of recipients;
    - the existence of the right of access to and the right to rectify the data concerning her
  - Req 6.45.3: The data subject MUST be provided with the information listed in Req 6.28.2 when this is necessary to guarantee fair processing towards the data subject (taking into account the specific circumstances in which the data are collected) or when this is required by the applicable national legislation.

** Note: Requirements 6.45.1-3 MAY in principle be discarded where:

- where it is certain that the data subject already has such information;
- where the processing takes place for statistical purposes or for the purposes of historical or scientific research;
- the provision of such information proves impossible or would involve a disproportionate effort; or
- disclosure is expressly mandated by law.

8.3 *Implementation*

- Req 6.46: All the information elements listed in Reqs 6.44-6.45 MUST be made readily available to (both actual and potential) data subjects in the form of a privacy policy (or policies), which is (are) both easily accessible and easy to understand.

- Req 6.46: Layered approach._In order to limit complexity, the fulfilment of Reqs 6.44-6.45 need not necessarily take the form of a single document.[106] TAS³ SHOULD consider adopting a 'layered' approach for notice when appropriate.
    - Req 6.46.1: This approach SHALL NOT contain more than three layers of information (short – condensed – full)
    - Req 6.46.2: The sum total of these layered notices MUST meet the notice requirements imposed by the applicable national legislation.
    - Req 6.46.3: It MUST be easy to ascertain which data processing operations are governed by which policies.

- Req 6.47: Privacy policy for TAS³ portal (full notice). The privacy policy notice provided on the TAS³ portal SHALL not only cover the processing operations performed by the TAS³ infrastructure itself, but MUST also include a general notice with regard to the operations of entities participating to the TAS³ network as service providers.
    - Req 6.47.1: In addition to the elements in Reqs 6.44-6.45, this notice MUST also contain a point of contact for questions and information and redress mechanisms
    - Req 6.47.2: This general privacy policy SHOULD reference and link the privacy policies maintained by TAS³ participants (see Req 6.48) when appropriate.

- Req 6.48: Each entity participating in the TAS³ network as a service provider MUST also provide notice of its own privacy policy (policies), which provides further details specific as to its particular processing operations.
    - Req 6.48.1: In addition to the elements in Reqs 6.44-6.45, this notice MUST also contain a point of contact for questions and information on redress mechanisms
    - Req 6.48.2: These privacy policies SHOULD also cross-reference the TAS³ infrastructure privacy policy where appropriate.

[106] See Article 29 Data Protection Working Party, 'Opinion on More Harmonized Information Provisions', WP100, 25 November 2004, p. 8-9.

- Req 6.49: Consent to notices. The consent of the data subject MUST (as a rule[107]) be obtained in relation to privacy policies listed in 6.47-48 prior to any processing of his personal data, by either TAS³ Infrastructure Members or one of the participating TAS³ entities (see Req 6.10).
    - Req 6.49.1: A versioning and archiving system MUST be in place for the informed consents given by data subjects to enable later verification that appropriate notice was given (see also Req 6.3)

- Req 6.50: If any entity within the TAS³ network intends to process personal data for an additional purpose (i.e. a purpose which has not yet been previously specified and communicated to the data subject), a subsequent notice MUST be provided, and the data subject MUST be given the ability to either accept or reject the envisaged processing (see Req 6.12).[108]

9. Data subject rights of access, rectification, blocking and erasure

- Req 6.51: Access request process/Accuracy: a process MUST be in place which enables users to request access to (and possibly amend or correct) personal data relating to them which has or is being processed within the TAS³ network.[109]

- Req 6.52: Blocking and erasure: a process MUST be in place which enables blocking or erasure of specific data elements upon request of the data subject, unless the processing is specifically mandated by law.

9.1 *Right of access*

- Req 6.53: Upon request, the data subject MUST be provided with confirmation, as to whether or not data relating to a particular data subject are being processed, and information at least as to:
    - the purposes of the processing, the categories of data concerned, and the recipients or categories of to whom the data are (have been) disclosed;
    - the data undergoing processing and of all available information as to its source;
    - the logic involved in the processing of data particularly where automated decisions are involved.

---

[107] In instances where the data subject cannot provide his consent to the processing in a valid manner (e.g. relationship of command), an alternative legally permitted basis must be in place (see Req 6.11). This situation does not remove to obligation to inform the data subject of such processing (see Reqs 6.43 et seq.)

[108] Req 6.50 does not apply where the processing is based on a legally admissible basis other than consent AND where such notice is impossible or would involve a disproportionate effort. However, such instances of overriding legitimate interest MUST at least be generically outlined in the TAS³ privacy policy notice(s) mentioned in Reqs 6.47-48.

[109] This also helps assure the accuracy and integrity of the data, which MUST be maintained in a manner appropriate to the specified purposes (see Reqs 6.26 et seq.).

- Req 6.54: The confirmation and information listed in Req 6.53 MUST be provided without constraint or excessive delays or expense.

9.2 *Rectification, blocking and erasure*

- Req 6.55: Data subject requests to rectify, block, or erase data MUST be accommodated at all times EXCEPT where an overriding legitimate interest exists.
    - Req 6.55.1: Such overriding interest SHOULD be specified in the TAS³ privacy policy notice(s).
    - Req 6.55.2: Data subject requests to rectify, block or erase data MUST in any event be accommodated in case the processing infringes upon the applicable national data protection legislation.
    - Req 6.55.3: In case of denial, the reason for denial MUST be communicated to the data subject.
- Req 6.56: The TAS³ privacy policy MUST specify:
    - to which entity in particular data subjects should address their request for access, rectification, blocking or erasure in which instance;
    - which entity shall decide these requests;
    - valid reasons for denying the request;
    - the time-frame in which this request will be processed;
- Req 6.57: A procedure SHOULD be in place to adequately deal with the situation in which a data subject submits his/her request to a TAS³ actor which is not competent to decide that particular request.

9.3 *Notification to third parties*

- Req 6.58: A process MUST be in place that provides notification to third parties to whom the data have been disclosed in case of corrections, erasure of blocking of processing of personal data pursuant to a request by the data subject.

9.4 *Implementation*

- Req 6.59: The TAS³ user interface ('dashboard') SHOULD make all the information listed in Reqs 6.53 readily available to data subjects in a user-friendly way.

- Req 6.60: Where appropriate, the TAS³ Dashboard SHOULD also provide data subjects with more detailed information as to the processing operations performed upon their personal data (e.g. at what time individual processing operations took place, under which pretext etc.).

- Req 6.61: The TAS³ Dashboard SHOULD provide an interface which enables exercise of the data subject rights listed in Reqs 6.55 (or at least direct the user as to how those rights may be exercised).

- Req 6.62: The TAS³ Dashboard SHOULD support automatic notifications to relevant parties in case of corrections, erasure of blocking of processing of personal data pursuant to a request by the data subject

10. Accountability and compliance verification

10.1 *Logging*[110]

- Req 6.63: Processing operations involving personal data MUST be logged with a sufficient level of detail.

- Req 6.64: The level of detail of log files MUST be sufficient as to enable compliance verification and oversight of processing operations with the governing policies

    - Req 6.64.1: Log files MUST detail which entity performed which action upon which resource, and at what time;

    - Req 6.64.2: Where appropriate, log files SHOULD also record for which purpose (under which pretext the action took place/was authorized);

    - Req 6.64.3: Log files MUST contain explicit information as to the recipients to whom personal data has been transferred.

    Note: Separation of duties should be considered to avoid situations where a single entity might have the ability to profile all the activities of end-users.

- Req 6.65: Reliability: Appropriate measures MUST in place to ensure the authenticity, accuracy, integrity and completeness of the logs.

[110] The logging of actions performed by entities within the TAS³ network will often also amount to processing of personal data. Where this is the case, such logging must also take into the requirements listed in this section 6.

- Req 6.66: Transparency. The fact that processing operations are logged MUST be transparent towards users through appropriate notification (see Reqs 6.43 et seq).

- Req 6.67: Proportionality: Logging MUST organized in a proportionate manner (e.g. storage in a pseudonymized or de-identified format, separation of duties).

- Req 6.68: Confidentiality: Appropriate measures MUST be in place to ensure the confidentiality of the logs

    - Req 6.68.1: Privileges to access nominative log information SHOULD in principle only authorize selective access (no 'free search');

    - Req 6.68.2: In case of non-targeted compliance verification (e.g. detection of anomalies through dedicated algorithms), the log data MUST first be de-identified/pseudonymized. Only after an anomaly has been detected may the log information be re-identified.

10.2 *Audit & oversight*

- Req 6.69: The proper implementation and functioning of all technical mechanisms and organisational measures MUST be documented and audited on a regular basis.

- Req 6.70: Definition of roles & responsibilities (see Req 6.8) MUST also include assignment of tasks with regards to audit and oversight.

- Req 6.71: Each participant MUST be bound to provide co-operation to entities in the TAS³ network charged with oversight & audit.

10.3 *Other accountability mechanisms*

- Req 6.72: Both within the TAS³ network and within each participating entity internal responsibility and accountability mechanisms MUST be adopted (e.g. designating 'owners' for both equipment and processing operations where personal data is involved).

- Req 6.73: Technical non-repudiation mechanisms MUST be supported when appropriate. For example:

    - Req 6.73.1: When forwarding personal data, it MUST be ensured that the sender is not able to later deny having forwarded it;

    - Req 6.73.2: It MUST be ensured that the commitment to communicated policies and privacy preferences cannot later be repudiated at a later time.

- Req 6.74: Automated notifications MUST be instituted for extraordinary processing operations (e.g. break-the-glass), and procedures MUST be in place to further follow up such notifications (e.g. through audit & oversight committee).
    - Req 6.74: Automated notifications SHOULD also be considered for certain types of processing operations (e.g. access to particularly sensitive data)

- Req 6.75: Procedures MUST be in place to ensure that when requested it is possible to indicate the source of the personal data that is being processed, as well as what the reason for processing has been.

- Req 6.76: Outsourcing – reliance upon other entities for personal data handling: Where members/participants of the TAS³ network decide to pass any personal data to entities outside their own organisation for them to process it on their behalf, they MUST ensure that such recipients only process this data in a lawful manner and in accordance with the policies of the TAS³ network. Members/participants must also ensure that the recipients adhere to all of the commitments they have themselves made towards the data subject (e.g. with regards to storage duration, finality etc.)

9.4 *Complaint handling*

- Req 6.77: Complaint capture system: Potential abuses to the system or concerns of either users or organizations MUST be captured.

    - Req 6.77.1: The complaint capture system SHOULD include a feedback mechanism which enables users to both
        - provide information to reputation engines or other trust entities that may be evaluating service providers, and to
        - initiate procedures for privilege revocation as a consequence of intentional or uncured breach of terms, and corresponding redress.

    - Req 6.77.1: Appropriate levels of proof are required to justify the consequences listed in Req 6.77.2 and complaints should therefore be corroborated on the basis of logs and other relevant documentation

- Req 6.78: Redress/oversight Processes: Once a compliant is captured, redress MUST be possible. In addition, an oversight process MUST be in place and SHOULD be able to proactively detect non-compliance.

11. Notification & prior checking

- Req 6.79: Where required by the applicable law, the TAS³ network and/or its participants MUST ensure prior notification and/or prior checking with national data protection authorities

* Sample Service Provider Obligations: While actual contract instruments will need to be tailored to the role of the service provider, the following list measures is indicative of the types of controls which SPs may be obligated to implement:

- Use of up-to-date Anti-virus/ Spyware/ Malware detection systems
- Spam filters (may need to define settings to assure that legitimate mail is not suppressed)
- Penetration testing (may only be appropriate for largest players)[i]
- Encryption
  - In transit
  - At rest
- Security policies
  - Physical
  - Logical
  - Administrative
  - Separation of Duties
- Privacy policy
  - W/specific obligation to honour preferences and negotiated obligations of end-users
  - Notice
- Complaint handling policies / mechanism
- Compliance processes/officer
- Contact points
- Internet Access and Use Policies
- Training
- Code of ethics
- HR Policies (related to vetting of employees that have access to personal to the extent permitted by law)
- Service Level Agreements
- Breach Notification
- Disaster recovery / Business continuity plans/exercises
- Audit/oversight
- Exceptions and Emergencies handling policies
- Government/Law Enforcement obligations/request for information policies
- Third party agreements' obligations/requirements clauses

11.5 Annex V – Defining elements of user-centricity in TAS³

This annex provides a first iteration of the defining elements of user-centricity in TAS³. These elements have been identified based on existing deliverables, email discussions and meeting interaction. The subsequent sections list these elements and provide references to the deliverables that cover (or are expected to cover) these aspects of user-centricity. This list will be continuously refined throughout further development of the project.

11.5.1 The user's ability to express privacy preferences

Within TAS³ every data subject user will be provided with the opportunity to express his or her own privacy preferences with regards to at least the following aspects of the processing operations that take place within the TAS³ network:

- the categories of recipients of his personal data. The interface provided to the user shall be sufficiently granular to allow him to both identify categories of recipients, and also to exclude particular entities as potential recipients (e.g. to deny a particular physician future access to his/her PHR);

- what their processing capabilities shall be (read, write, edit, delete, ...);

- for which context/purpose (e.g. yes where pursuant to self-initiated job application but not for headhunting purposes; or yes when being referred to this doctor for treatment, etc);

- to formulate constraints (e.g. specify the time-period in which the processing operation is allowed to take place);

- whether or not an operation is to be dependent on specific obligations (e.g. delete after two weeks).

The user's privacy preferences will be translated operationally within the TAS³ network in mainly three ways:

1. Either through a constrained delegation process (see deliverables D2.1, D7.1, D3.1);
2. Under a policy-based approach ('policy wizard') (see deliverable D4.2);
3. Or a combination of both 1 and 2.

In each of these instances the interface for the user will be the so-called 'dashboard' (see D2.1). Under all three approaches, the user's privacy preferences will be translated into so-called "sticky policies", which shall be attached to the data to ensure that all data recipients along the value chain are aware of usage restrictions (and to ensure that they are subsequently enforced).

In order to ensure proper enforcement, the consent by the data subject shall operate as a default requirement (policy condition) for any authorization decision by Policy Decision Points (PDPs) whenever appropriate. Other consent directives (e.g. restrictions with regards to subsequent use) shall be enforced by securely associating these instructions with the data as sticky policies.

Note 1: The user's expression of privacy preferences of course needs to take place within certain parameters. These parameters shall be clearly described in the initial privacy notice provided to the data subject during the intake/enrolment process. In particular, the user shall be notified of those aspects that he MUST subscribe to, such as processing operations, which may take place pursuant to legal obligations incumbent upon the user or the TAS³ network, or further processing for statistical purposes.

Note 2: For the employability scenario there may be restrictions as to when consent may act as a legal basis to legitimize the processing (due to imbalance of power between employee – employer / prospective employee). The relevant opinions of the Article 29 Working Party[111] will be taken into account to ensure that consent only acts as a legitimate basis within the meaning of articles 7 et seq. of the Directive when the data subject can truly give his consent 'freely' (article 2 (h) of the Directive).

While pre-authorization is a possibility for relatively simple processes, more complex processes may require additional consent capture. After all, the user's general privacy preferences are intended to serve multiple purposes, and therefore cannot adapt to all situations or remove the need for additional consent in case of new or unanticipated uses of information. In order to accommodate the need for subsequent consent capture, a 'call-back' process shall be in place that alerts the individual to an unanticipated situation or 'out-of-policy' request for use of or access to information (see D2.1). In other words, for most processes the user will exercise control prior to moment that a service provider requests to undertake processing (pre-authorization), for others the will have to authorize the transaction at the moment that it is requested (user call-back).

11.5.2 The user's ability to manage his own partial identities

In addition to deciding which attributes he discloses to which service provider (and under which conditions), the user will also have the opportunity to choose which digital identity (identity provider or other authoritative source for attribute information) he uses to provide these attributes.

In this regard the TAS³ is approach is somewhat similar to the Microsoft Cardspace model, however, the TAS³ approach is more advanced for mainly two reasons. First, the user has the ability to become actively involved in the management of the identifiers/ pseudonyms associated with his respective digital

[111] See in particular Article 29 Working Party, 'Opinion 8/2001 on the processing of personal data in the employment context', WP48, 13 September 2001 and 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995', WP 114, 25 November 2005; available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

identities, and the correlations between them. Additionally, the TAS³ approach provides for an important functionality currently not provided by Cardspace, namely the ability to aggregate attributes across different partial identities to respond to a single request from a service provider, without compromising the privacy of the data subject with regards to the identifiers associated with these different partial identities.

Another advantage provided by TAS³ is the governance framework. The contract framework coupled with the required polices, create an ecosystem-wide binding of obligations. Most systems can only bind a limited number of parties to a transaction and only for a limited number of transactions.

See deliverables D2.1 (high-level), D4.2 D7.1 and upcoming deliverables of WP6.

11.5.3 The user's ability to express trust preferences and provide feedback

The user's ability to express trust preferences in TAS³ is accommodated by allowing the user to specify the 'trust rating' or 'trust score' that is required for entities in order for them to be involved in processing operations involving his personal data.

Example: A user may specify that only head-hunters with a sufficiently high trust rating are eligible to access his employability e-Portfolio. This condition then applies cumulatively along with the user's specified privacy preferences. So head-hunter X may theoretically have been authorized to access the user's e-Portfolio as far as the privacy preferences were concerned (because the user has specified that his e-Portfolio may be accessed by head-hunters for placement purposes), but fails to meet the required trust rating so is still denied access.

The user will also be provided with some form of feedback mechanism, in which he can share experiences with regard to particular service providers, which may in turn affect the overall 'trust rating' of the service provider in question.

See deliverable D5.4 (expression of trust preferences into policies and user feedback), D2.1 (subrole of auditor); upcoming deliverables in WP 6 will include the contract related to reputation based service providers and any oversight processes/policies to help assure correctness and fairness.

11.5.4 Enhanced transparency

TAS³ shall ensure that, as a rule, no operation upon personal data will be authorized within the TAS³ network without the prior consent of the data subject.

As described in section of 3.2 of D6.2, notice and consent typically only provide 'ex ante' transparency towards the data subject. The data subject usually has no or only limited means of verifying whether or not the data recipient has adhered to the asserted or negotiated policies.

TAS³ will enhance transparency towards the data subject by providing him with opportunity to verify after the fact which actions upon his personal data have taken place. Due to the advanced level of security and accountability mechanisms applied throughout the TAS³ network, the user will be able to obtain a much higher degree of assurance that his privacy preferences have in fact been adhered to.

See deliverable D2.1 (dashboard)

11.6 Annex VI - Self Assessment Questionnaire

The purpose of this self-assessment questionnaire is to provide information on the ability of your organization to effectively participate in a privacy and security architecture that provides users with a user-centric, end-to-end trust enabled infrastructure. The following questionnaire will go through general questions about organizational policies and practices that are tailored to privacy requirements. Each section is introduced with a brief description of the privacy or security principles followed by questions about your organizations policies and practices related to privacy and security.

A. Notice (Questions 1-4)

The questions in this section are directed towards:

(a) ensuring that individuals understand your policies regarding personal information that is collected about them, to whom it may be transferred and for what purpose it may to be used; AND

(b) ensuring that, subject to the qualifications listed in part II of this section, individuals know when personal information is collected about them, to whom it may be transferred and for what purpose it may be used.

I. General

1. Do you have clear and easily accessible statements about your practices and policies that govern the processing personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.

_____ Y _____ N

a) Does this privacy statement describe how your organization collects personal information?

_____ Y _____ N

b) Does this privacy statement describe the purpose(s) for which personal information is collected?

_____ Y _____ N

c) Does this privacy statement inform individuals as to whether and/for what purpose you make personal information available to third parties?

_____ Y _____ N

d) Does this privacy statement disclose the name of your company and location, including information on how to contact you about your practices and handling of personal information upon collection? Where YES describe below.

_____ Y _____ N

e) Does this privacy statement provide information regarding the use of their personal information?

_____ Y _____ N

f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?

_____ Y _____ N

2. Subject to the qualifications listed below, at the time of collection of personal information, (whether directly or through the use of third parties acting on your behalf) do you provide notice that such information is being collected?

_____ Y _____ N

3. Subject to the qualifications listed below, at the time of collection of personal information, (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?

_____ Y _____ N

4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?

_____ Y _____ N

II. Qualifications

- **Disclosure to a government institution which has made a request for the information with lawful authority:** Personal data controllers may not need to provide prior notice of actual disclosure to law enforcement agencies subject to lawful forms of process.

- **For legitimate investigation purposes:** Personal data controllers may not need to provide prior notice of actual disclosure or other processing when the following conditions are met:
  - providing notice would compromise the availability or accuracy of the information; and
  - the collection, use and disclosure are reasonable for purposes relating to investigating a violation of a code of conduct, breach of contract or a contravention of domestic law.

- **Action in the event of an emergency**: Personal data controllers may not need to provide prior notice in emergency situations that threaten the life, health or security of an individual.

B. Collection Limitation (Questions 5-7)

The questions in this section are directed towards ensuring that collection of information is limited to what is strictly required to realize the stated purposes for which it is collected. In all instances, collection methods must be lawful and fair.

5. How do you obtain personal information:

   a) Directly from the individual?

_____ Y _____ N

b) From third parties collecting on your behalf?

_____ _____
Y N

c) Other. If YES, describe.

_____ _____
Y N

6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected?

_____ _____
Y N

7. Do you collect personal information (directly or indirectly) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.

_____ _____
Y N

C. Uses of Personal Information (Questions 8-13)

The questions in this section are directed toward ensuring that the use of personal information is limited to fulfilling the purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. In TAS^3 use questions also have a technical dimension as certain limitations on use may be communicated and enforced via "sticky policies". Once the information has been received, subsequent uses of the information by organizations must be consistent with any limitations on use set forth in either the transactional policies or other applicable TAS^3 policies or contractual obligations.

8. Do you limit the use of the personal information you collect (directly or indirectly) as articulated in TAS^3 policies or requirements and as identified in your privacy statement and/or in the notice provided at the time of collection to those

purposes for which the information was collected or for or other compatible or related purposes? Provide a description in the space below,

_____ Y _____ N

9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.

   a) Based on express consent of the individual?

   b) Compelled by applicable laws?

10. Do you disclose personal information you collect (directly or indirectly) to other personal information controllers? If YES, describe.

_____ Y _____ N

11. Do you transfer personal information to personal information processors? If YES, describe.

_____ Y _____ N

12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? Describe below.

_____ Y _____ N

13. If you answered NO to question 12, or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?

   a) Based on express consent of the individual?

   b) Necessary to provide a service or product requested by the individual?

   c) Compelled or expressly authorized by applicable laws?

D. Choice (Questions 14-20)

The questions in this section are directed towards ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information.

I. General

14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.

_____ Y _____ N

15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.

_____ Y _____ N

16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.

_____ Y _____ N

17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and noticeable manner?

_____ Y _____ N

18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?

_____ Y _____ N

19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of

their personal information, are these choices easily accessible and affordable? Where YES, describe.

_____ Y _____ N

20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.

II. Qualifications to the Provision of Choice Mechanisms

The following are situations in which the application of the Choice Principle may not be necessary or practical.

1. **Third-Party Receipt**: Where personal information is received from a third party, the recipient personal data controller may not be able to provide directly provide the concerned individuals with a mechanism for individuals to exercise choice in relation to this collection. However, the third party who has been engaged by the personal data controller to collect personal information on its behalf, the recipient personal data controller should instruct the collector to provide such choice when collecting the personal information (or additional notice prior to transmitting the data insofar as it concerned data previously collected for a different purpose).

2. **Disclosure to a government institution which has made a request for the information with lawful authority**: Personal Information controllers may not be able to provide a mechanism for individuals to exercise choice in relation to disclosure to law enforcement agencies pursuant lawful forms of process.

3. **For legitimate investigation purposes**: Personal Information controllers may not be able to provide a mechanism for individuals to exercise choice when providing a mechanism for individuals to exercise choice would compromise the availability or accuracy of the personal information and its collection, use and disclosure are reasonable for purposes relating to investigating a violation of a code of conduct, breach of contract or a contravention of domestic law.

4. **Action in the event of an emergency**: Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in emergency situations that threaten the life, health or security of an individual.

E. Integrity of Personal Information (Questions 21-26)

The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.

21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.

_____ Y _____ N

22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.

_____ Y _____ N

23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.

_____ Y _____ N

24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.

25. Do you require personal information processors, agents, or other service providers to who act on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?

_____ Y _____ N

F. Security Safeguards (Questions 26-35)

The questions in this section are directed towards ensuring that when individuals entrust their information to an organization, their information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification or disclosure of information or other misuses.

26. Have you implemented an information security policy?

_____ _____
Y N

27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?

28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.

29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).

30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:

    a) Employee training and management or other organizational safeguards?

    _____ _____
    Y N

    b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?

    _____ _____
    Y N

    c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?

    _____ _____
    Y N

    d) Physical security?

    _____ _____
    Y N

31. Have you implemented a policy for secure disposal of personal information?

_____ _____
Y N

32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?

_____ _____
Y N

33. Do you have processes in place to test the effectiveness of the safeguards referred to above in questions 32? Describe below.

_____ _____
Y N

34. Do you use third-party certifications or other risk assessments? Describe below.

35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:

    a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?

    _____ _____
    Y N

    b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of your organization's personal information?

    _____ _____
    Y N

    c) Take immediate steps to correct/address the security failure which caused the privacy or security breach?

    _____ _____
    Y N

G. Access and Correction (Questions 36-38)

The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures by which the ability to access and correct information is provided may differ depending on the nature of the information and other interests. For this reason, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

I. General

36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.

_____ Y _____ N

37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your organization's policies/procedures for receiving and handling access requests below. Where NO, proceed to question 38

_____ Y _____ N

a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.

_____ Y _____ N

b) Do you provide access within a reasonable timeframe following an individual's request for access? If YES, please describe.

_____ Y _____ N

c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.

_____ _____
Y N

d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?

_____ _____
Y N

e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.

_____ _____
Y N

38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your organization's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e).

_____ _____
Y N

a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.

_____ _____
Y N

b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?

_____ _____
Y N

c) Do you make such corrections or deletions within a reasonable timeframe following an individual's request for correction or deletion?

_____ _____
Y N

d) Do you provide a copy of the corrected personal information or provide confirmation that the data has been corrected or deleted to the individual?

_____ _____
Y N

e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?

_____ _____
Y N

II. Qualifications to the Provision of Access and Correction

Although organizations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organizations to deny access requests. Please identify which, if any, of these situations apply, and specify their application to you, with reference to your responses provided to the previous questions, in the space provided.

i. **Disproportionate Burden:** Personal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.

ii. **Protection of Confidential Information:** Personal information controllers do not need to provide access and correction where the information cannot be disclosed due to legal or security reasons or to protect confidential commercial information (i.e. information that you have taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against your business interest causing significant financial loss). Where confidential commercial information can be readily separated from other information subject to an access request, you should redact the confidential commercial information and make available the non-confidential commercial information to the extent that such information constitutes personal information of the individual concerned. Other situations would include those where disclosure of information would benefit a competitor in the market place, such as a particular computer or modelling program. Furthermore, a denial of access may also be considered acceptable in situations where, for example providing the information would constitute a violation of laws or would compromise security.

iii. **Third Party Risk:** Personal information controllers do not need to provide access and correction where the information privacy of persons other than the individual would be violated.

H. Accountability (Questions 38-50)

The questions in this section are directed towards ensuring that you are accountable for complying with measures that give effect to the Principles stated above. Additionally, when transferring information, you should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

I. General

38. What measures does your organization take to ensure compliance with the EU Data Protection Principles? Please check all that apply and describe below.

    - Internal guidelines or policies _____
    - Contracts _____
    - Compliance with applicable industry or sector laws and regulations ____
    - Compliance with self-regulatory organization code and/or rules ____
    - Other (describe) ____

39. Has your organization appointed an individual(s) to be responsible for your organization's overall compliance with the Data Protection Principles?

    _____ Y _____ N

40. Does your organization have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.

    _____ Y _____ N

41. Can individuals expect to receive a timely response to their complaints?

    _____ Y _____ N

42. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.

    _____ Y _____ N

43. Do you have procedures in place for training employees on how to respond to privacy-related complaints? If YES, describe.

_____ Y _____ N

44. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?

_____ Y _____ N

II. Maintaining Accountability When Personal Information is Transferred

45. Do you have agreements in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met?

_____ Y _____ N

46. Do these agreements generally require that personal information processors, agents, contractors or other service providers:

- Abide by your EU-compliant privacy policies and practices as stated in your Privacy Statement? _____
- Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____
- Follow-instructions provided by you relating to the manner in which your personal information must be handled? _____
- Impose restrictions on subcontracting unless with your consent? _____
- Other (describe) _____

47. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.

_____ Y _____ N

48. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.

_____ _____
Y N

49. Do you disclose personal information to other personal information controllers in situations where due diligence and mechanisms to ensure compliance with your Privacy policy by the recipient as described above is impractical or impossible?

_____ _____
Y N

50. If YES, please describe the disclosures and state whether you use other means, such as obtaining the individual's consent prior to the disclosure? Where applicable, describe the form in which the consent is obtained from individuals, when it is obtained, the mechanism used to seek the individual's consent and honour the individual's choice, and provide copy of the applicable template consent form below.

Amendment History

Version	Date	Author	Description/Comments
0.1	28-11-2008	Joseph Alhadeff	First draft
0.2	12-12-2008	Joseph Alhadeff	Draft
0.9	05-01-2009	Joseph Alhadeff	Comments of reviewers incorporated
1.0	05-01-2009	Theo Hensen	Deliverable in TAS³ template
1.1	23-05-2009	Brendan Van Alsenoy	Revisions/extensions - introduction of annexes wrt requirements and defining elements of user-centricity in TAS³
1.2	24-05-2009	Joseph Alhadeff	Revisions/extensions – addressed issues raised in 1.1; expanded executive summary, introduction, conclusion, and cross-referenced several other EU research projects.
1.3	24-05-2009	Brendan Van Alsenoy	Revisions/extensions – in particular introduction of text wrt issue of determining controllers vs. processors and e-discovery issue
1.4	24-05-2009	Joseph Alhadeff	Review of edits, cleanup
1.5	25-05-2009	Brendan Van Alsenoy	Minor edits/revisions
1.6	25-05-2009	Joseph Alhadeff	Clean up
1.7	26-05-2009	Brendan Van Alsenoy	Review
1.8	27-05-2009	Joseph Alhadeff	Final review
1.9	28-05-2009	Brendan Van Alsenoy	Final review
2.0	28-05-2009		Release
2.1	11-12-2009	Brendan Van Alsenoy	Integration in new template Incorporation updated WP6 requirements list
2.2	16-12-2009	Joseph Alhadeff	Incorporation of Intake Questionnaire
2.3	18-12-2009	Brendan Van Alsenoy	Incorporation of controller v. processor extension
2.4	18-12-2009	Joseph Alhadeff	Incorporation outline intake process (hallmarks, self-assessment, gap analysis)
2.5	20-12-2009	Brendan Van Alsenoy	Revisions/Comments
2.6	22-12-2009	Joseph Alhadeff	Revisions/Comments
2.7	23-12-2009	Brendan Van Alsenoy	Revisions/Comments
2.8	26-12-2009	Joseph Alhadeff	Minor revisions
2.9	28-12-2009	Brendan Van Alsenoy	Minor revisions
3.0	29-12-2009		Release