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, 2010
Version:	3.6

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

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.

PART I
DEVELOPPING THE CONTRACTUAL FRAMEWORK

1 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.

2 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.

2.1 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 TAS³ 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. TAS³ enables information to be functional and accessible within a user-centric framework.

2.2 Accountability and accountable systems

As was detailed in TAS³ 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]:

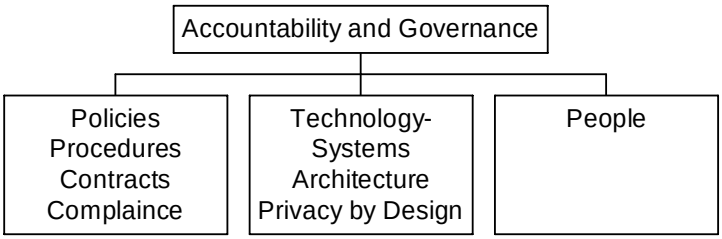


Figure 1
Accountability and Governance Model Proposed by Commissioner Thomas

Commissioner Thomas correctly highlighted the multiple elements needed to address accountability. These elements are essentially the same elements that are incorporated in the TAS[3] 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 privacy concerns in a recent Sun White Paper of Engineering for Data Protection and Accountability: [5]

[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.
[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.

> *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.

2.3 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.

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

[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

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 • Make decisions as to which credentials to use and when to re-identify	Expands user options related to risk mitigation and disclosure
User can define privacy preferences related to:	Privacy controls accessible through usable interface, which may include a

[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

• Categories of Recipients • Processing permissions • Purpose • Time of availability • Additional controls; depending on the type of service	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

3 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.

3.1 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.

3.2 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.

3.3 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.

4 Organizational models

4.1 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.

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.

[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).

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.

4.2 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.

4.2.1 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 trust 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/

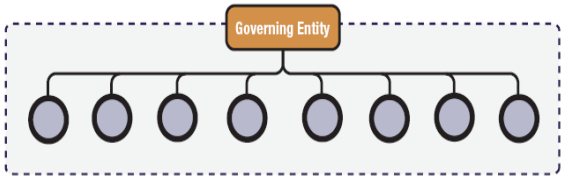
[11] www.projectliberty.org/liberty/content/download/3500/23156/file/overview-id-governance-framework-v1.0.pdf. – See Annex 2 for a mapping dataflows/functions.

[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

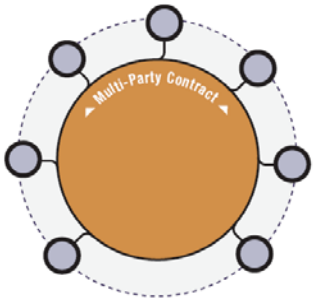
In the collaborative model, a group of founding members or member forms an entity that establishes the rules for the operation and governance of the ecosystem, as well as overseeing day-to-day control of the system.



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

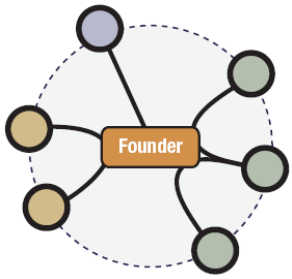


Figure 3: Liberty Alliance Federation Organizing Models[14]

4.2.2 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.

4.3 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.

5 Developing a Contractual Framework

5.1 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, we have focused on issues and perspectives of EU Jurisdiction.

5.2 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.

5.2.1 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.

5.2.2 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?

5.3 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.

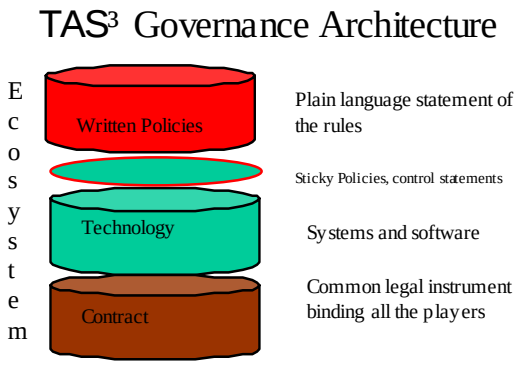


Figure 4 – TAS³ governance architecture

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

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

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.

5.4 Defining the "Who"

5.4.1 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,

[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

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 TAS³ 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 TAS³, 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 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.

[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.

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]

5.4.2 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 roles 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.

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 are dividing their respective responsibilities in a way, which does 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. 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

[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.

[24] Ibid, p. 72.

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.[26] 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.

Until recently, only limited authoritative guidance was available to help practitioners deal with the increasingly difficult task of applying these concepts in practice. In February of 2010, the Article 29 Data Protection Working Party issued an Opinion (1/2010) containing a comprehensive analysis of both the controller and processor concepts.[27] In the following subsections we shall provide a summary of the main findings of Opinion 1/2010 which are relevant to our current analysis, followed by an assessment of their implications for the TAS[3] contractual framework. By way of conclusion we will outline certain issues that are likely to persist despite the clarifications made by the Working Party. [28]

---

[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, 2009, vol. 2, p. 68-69, available at http://www.springerlink.com/content/u11161037506t68n/?p=352e04236b974655a1271b94c857ff67&pi=32.

[26] This 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.

[27] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller and "processor"', WP169, 16 February 2010, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf. Hereafter referred to as "Opinion 1/2010". The Working Party had been called upon to deal with the question of legal 'control' several times in the past, but the guidance provided in these opinions was often closely tied to the specific issues at hand. See e.g. 'Working Document on on-line authentication services', WP68, 29 January 2003 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp68_en.pdf); 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)', WP128, 22 November 2006 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf); 'Opinion 7/2007 on data protection issues related to the Internal Market Information System (IMI)', WP140, 20 September 2007 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp140_en.pdf); 'Opinion 5/2009 on online social networking', WP163, 12 June 2009 (available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf). The cited urls were last accessed on 20 November 2010.

[28] The remainder of this section (with the exception of section 6.4.2.4) is comprised primarily of extracts of the forthcoming publication: B. Van Alsenoy, 'Allocating responsibility among controllers, processors "and everything in between": a preliminary analysis of structural issues underlying the definition of roles and responsibilities in

5.4.2.1 Essential components of the controller concept

A controller is defined by art. 2, e of the Directive as '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 […]'. There are in essence two components in the definition of a controller which set controllers and processors apart from one and other. In first instance, there is the reference to the controller's exercise of a 'determinative influence' over the processing. The second component refers to the object of the controller's influence, namely the 'purposes and means' of the processing. The definition of a controller also contains a third component, which makes clear that control might be exercised by more than one entity. Each of these components shall be elaborated further over the following paragraphs.

a) A determinative influence …

The first essential component of the controller concept, namely the determinative influence of the controller, refers to an *exercise of decision-making power* ('control') regarding the processing. Herein lies the first indication that the concept of a controller is a *functional* concept: rather than allocating responsibility on the basis of formal criteria, it aims to allocate responsibilities where the factual influence is.[29] The ability to influence the processing may stem from a variety of circumstances. The Working Party has developed a typology to assist practitioners in ascertaining which entity acts as a 'determining body'. According to the Working Party, the circumstances giving rise to legal control can be classified into three main categories, namely[30]:

1. Control stemming from *explicit legal competence* (e.g. when controller or the specific criteria for its nomination are designated by national law);

2. Control stemming from *implicit competence*, whereby by an analysis of the traditional roles associated with a certain actor will assist in identifying the controller (e.g. an employer in relation to data on his employees, the publisher in relation to data on subscribers); or

3. Control stemming from *factual influence*, whereby the qualification of controller is attributed on the basis of an assessment of factual circumstances, which warrant the conclusion that this party exercises a 'dominant role' with respect to the processing.

b) … over the 'purposes and means' of the processing …

A common element among the aforementioned categories is the power or responsibility to decide what processing is carried out and how it is carried out.[31] In other words, the concept of a controller implies an exercise of decision-making

---

Directive 95/46/EC', submitted to Computer Law and Security Review, expected publication date May 2011.

[29] Opinion 1/2010, *l.c.*, 9.

[30] Opinion 1/2010, *l.c.*, 10-12.

[31] See also D. Bainbridge, , *EC Data Protection Directive*, London, Butterworths, 1996, 45.

power as to whether and how the processing will take place. This brings us to the second essential component of the controller concept, i.e. the 'purposes and means' component. This component of the definition of controller has been paraphrased as referring to the 'why' and the 'how' of a given processing operation.[32] The Directive requires that an entity's influence and decision-making power is instrumental in both the *initiation* (why) and the *modalities* (how) of the processing in order to be considered a controller.

Of these two elements, the Working Party seems to place greater weight on the controller's determination of purpose than upon his determination of means.[33] It views the determination of purpose(s) as something that is reserved to the controller: whoever decides the purpose acts as a controller.[34] As far as the determination of the 'means' of the processing is concerned, the Working Party feels that the Directive supports a certain degree of flexibility. Specifically, it accepts that the controller leaves its processor(s) a certain 'margin of manoeuvre' in specifying how the processing shall be organized.[35] In other words, while the determination of purpose 'automatically' triggers the qualification of controller, this would not necessarily the case where an entity only influences the means of the processing.[36] Whether or not an entity's determination of means gives rise to a qualification as (co-)controller would in turn depend on the assessment of whether or not this determination relates to the 'essential' or 'non-essential' means of the processing.[37] Essential means, according to the Working Party, are those elements which are traditionally and inherently reserved to the determination of the controller, such as "which data shall be processed?", "for how long shall they be processed?", "who shall have access to them?". Non-essential means appear to concern more practical aspects of implementation, such as the choice for a particular type of hard- or software. [38] Under this approach, the Working Party considers it possible that the technical and organizational means of the processing are determined exclusively by the data processor.[39]

---

[32] Opinion 1/2010, *l.c.*, 13.

[33] See also P. Van Eecke and M. Truyens, 'Privacy and social networks', *Computer, Law & Security Review*, Vol. 26, n° 5, September 2010, 539. The tendency to emphasize the purpose over the means of the processing can also be found in earlier doctrine (see e.g. D. De Bot, *Verwerking van persoonsgegevens*, 2001, Antwerpen, Kluwer, 46) and in guidance issued by regulatory authorities (see e.g. Office of the Information Commissioner, 'Data Protection Act 1998 – Legal Guidance', Version 1, not dated, 16, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf) (last accessed 26 November 2010). Bainbridge has even raised the question as to whether it might have been better to identify the controller based on who determines the purposes alone (See Bainbridge, *o.c.*, 128.). This tendency appears to have been brought about by considerations of pragmatisms; in particular to address the fact that entities that process personal data 'on behalf' of other entities often substantially influence the means of the processing..

[34] Opinion 1/2010, *l.c.*, 15.

[35] Opinion 1/2010, *l.c.*, 13-14.

[36] Opinion 1/2010, *l.c.*, 14.

[37] Opinion 1/2010, *l.c.*, 14. See also e.g. Opinion 1/2010, *l.c.*, 25.

[38] Opinion 1/2010, *l.c.*, 14.

[39] See Opinion 1/2010, *l.c.*, 14. In cases where there is a clear definition of purposes, but little or no guidance concerning the technical and organizational means to be used, the Working Party states that "the means should represent a reasonable way of achieving the purpose(s) and the data controller should be fully informed about the means used." (*Ibid*, 14.) Whether this normative statement is simply

c) … which is exercised 'alone or jointly with others'

The Directive implicitly acknowledges that the purposes and means of the processing might be determined by more than one legal entity. Specifically, article 2 (d) alludes to this fact by stating that the controller is the entity that 'alone or jointly with others' determines the purposes and means of the processing.[40]

According to the Working Party, the word 'jointly' should be interpreted as meaning 'together with' or 'not alone'. It also added that there are many different forms and combinations in which such 'joint control' might be manifest.[41] Due to the wide range of possible ways in which joint control might be exercised, the Article 29 Working Party chose not to develop an additional typology.[42] Instead, it concluded that for these situations the assessment of joint control should 'mirror' the assessment of a single control.[43]

It follows from the previous subsection that co-decision as to the means of the processing does not necessarily imply that an entity is a co-controller. For an entity to be considered a co-controller, the Working Party considers it necessary that it has a sufficiently relevant role in determining either the purposes or the essential means of processing.[44] Where co-control does exist, the breadth of influence a particular entity may vary considerably. In respect to this 'granularity of co-control', the Working Party observed that *'in the context of joint control the participation of the parties in the joint determination may take different forms and does not need to be equally shared'*.[45] As a result, many different forms of co-control are imaginable, based on the different degrees in which collaborating entities jointly determine the purposes and means of processing operations.[46]

It is worth underlining that a collaboration among organizations, whereby each organization exercises a determinative influence towards certain processing operations, does not necessarily give rise to joint control. For instance, the control of each entity might relate to entirely distinct processing operations. Similarly, an exchange of personal data among entities which does not involve shared

based on the Working Party's personal opinion as to what would be the most desirable state, or can be derived directly from the current concept of processor is unclear.

[40] 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 Review*, Vol. 23, n° 5, 2007, 419.

[41] Opinion 1/2010, *l.c.*, 18.

[42] While the Working Party did not explicitly develop a typology of the different forms co-control, it did proceed to provide a description of a number of examples to illustrate the fact that 'joint control' can take on many different of forms. See Opinion 1/2010, *l.c.*, 18-24.

[43] Opinion 1/2010, *l.c.*, 18.

[44] See Opinion 1/2010, *l.c.*, 25.

[45] Opinion 1/2010, *l.c.*, 19.

[46] Opinion 1/2010, *l.c.*, 18. Olsen and Mahler have developed an interesting visual representation of the different degrees of collaboration among (co-)controllers. See T. Olsen and T. Mahler, 'Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II', *l.c.*, 419-420.

purposes or means will likely be seen only as a transfer of data between separate controllers.[47]

5.4.2.2 Essential components of the processor concept

In practice controllers often decide not to perform all the envisaged processing operations by themselves, but instead choose to have some or all of these operations carried out by a different entity. This decision may stem from a variety of reasons: lack of technical expertise, lack of manpower, lack of infrastructure, insufficient return on investment if it were to perform all operations himself, etc. When an entity other than the controller (or its employee) carries out processing operations 'on behalf of' a controller, this organization shall be deemed a processor rather than a controller.

By definition, the existence of a processor depends on a decision taken by a controller to have certain processing performed by an external organization.[48] According to the Working Party the two basic conditions for qualifying as a processor are, on the one hand, being a separate legal entity and, on the other hand, processing personal data on behalf of a controller.[49]

The substantive component of the processor definition is that a processor acts 'on behalf' of a controller. The Working Party has approximated this wording with the legal concept of delegation. The term 'delegation' can be used to refer to a variety of actions. In the legal sense, delegation is often used to refer to figures of legal representation, such as agency. In the case of agency, one party (the principal) bestows upon another party (the agent), the authority to undertake one or more legal actions on the principal's behalf.[50] The legal effects of these actions shall, as a rule, be attributed directly to the principal (provided the agent acts within the scope of his authority).[51] The term delegation is sometimes also used to refer to the situation whereby one entity confers to another entity the power to perform one or more actions of a non-legal nature (so-called 'material' acts) on its behalf. Here it appears as if the Working Party is using the term delegation primarily in the latter sense, seeing as the type of services typically associated with processors consist in performing technical operations.[52]

---

[47] Opinion 1/2010, *l.c.*, 19. Olsen and Mahler have qualified such modes of collaboration as being one among 'collaborating single controllers'. See T. Olsen and T. Mahler, 'Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II', *l.c.*, 419.

[48] Opinion 1/2010, *l.c.*, 25.

[49] Opinion 1/2010, *l.c.*, 25. Bainbridge has questioned whether a distinct legal personality is an essential component of the processor concept. See D. Bainbridge, *o.c.*, 118.

[50] See O. Lando and H. Beale (eds.), 'Principles of European Contract Law – Parts I and II', prepared by the Commission on European Contract Law, Kluwer Law International, The Hague (Netherlands), 2000, p. 197 et seq. The full text of the Principles of European Contract Law is also available at http://frontpage.cbs.dk/law/commission_on_european_contract_law/PECL%20engelsk/engelsk_partI_og_II.htm (last accessed 28 November 2008).

[51] Even where the agent exceeds his authority, his actions might still be attributed to the principal under the theory of apparent authority. For more information see also B. Van Alsenoy, D. De Cock, K. Simoens, J. Dumortier and B. Preneel, 'Delegation and digital mandates: Legal requirements and security objectives', *Computer, Law and Security Review*, Vol. 25, n° 5, September 2009, 415-420.

[52] Note that a processor might also perform legal acts on behalf of a controller, e.g. in case of further subcontracting pursuant to the instructions of the controller; or where the processor also operates the front-office for consent registration and acceptance of the terms of use of a particular service.

The processor-delegate analogy appears to be founded on a number of considerations. In first instance, a processor is called upon to 'implement the instructions given by the controller' (see art. 16 of the Directive).[53] Secondly, the consequences of the processor's actions are in principle attributed to the controller; provided that the processor merely follows the latter's instructions. Finally, the delegation concept? also permits the delegate (processor) to exercise a certain amount of discretion on how to best serve the principal's (controller's) interests.[54]

5.4.2.3 Distributed operational and legal control

When processing of personal data involves multiple service providers, each actor plays a certain part. The nature of their relationship towards one another under data protection law can take on several different forms: a controller-processor relationship, a controller-to-controller relationship, a relationship of joint control, etc. Regardless of the legal qualification of their respective roles, the distribution of *operational* control over the data processing that is assumed by the respective actors can differ considerably. In fact, an indefinite number of combinations are imaginable. For instance, it could be that the entity that legally qualifies as the controller does not store any of the information himself, but relies entirely on a hosting service outside its organization that makes it available upon his request. It is also possible that it has direct access to the information, but that the enforcement of authorization policies and privilege management is organized by yet another entity. Thus the Directive has introduced the possibility of 'dualism' between control from a legal perspective (which brings about the responsibilities of a 'controller') on the one hand, and control from a practical ('operational') perspective on the other hand (the ability to enforce access control policies, the ability to delete, etc.). It is possible that in practice both notions of control coincide, but it also possible that there is only a partial overlap; or even that a dichotomy exists between them. As a result certain obligations incumbent upon the controller may in practice more easily be observed by an entity which does not qualify as the controller (or at least not as the sole controller) for the data processing.

The Working Party has acknowledged this reality and emphasized that even where the controller's obligations may in practice be more easily fulfilled by other parties (e.g., if those parties have a more direct relationship with the data subject), it is the controller that remains 'ultimately responsible for its obligations and liable for any breach to them'.[55] As a consequence, access to data does not necessarily bring about legal control, whereas having access to data also is not an essential condition to be a controller.[56]

[53] Opinion 1/2010, *l.c.*, 25.
[54] See Opinion 1/2010, *l.c.*, 25.
[55] Opinion 1/2010, *l.c.*, 22
[56] Opinion 1/2010, *l.c.*, 22. See also D. Bainbridge, *o.c.*, 45-46 and T. Olsen and T. Mahler, 'Identity management and data protection law: Risk, responsibility and compliance in 'Circles of Trust' – Part II', *l.c.*, 419.

Where multiple parties do jointly exercise control, the Working Party has stated that these entities have a certain degree of flexibility when allocating responsibility amongst each other, as long as they ensure full compliance.[57] More specifically, the bottom line should be that

> *'[…] even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties'.*[58]

As far as the distribution of liability exposure is concerned, the Working Party has indicated that joint control does not always entail joint and several liability.[59] Given the fact that there are many possible modes of collaboration, it is equally possible that the various collaborating controllers are responsible (and thus liable) for the processing of personal data 'at different stages and to different degrees'.[60] According to the Working Party, joint and several liability for all parties involved 'should only be considered as a means of eliminating uncertainties, and therefore assumed only insofar as an alternative, clear and equally effective allocation of obligations and responsibilities has not been established by the parties involved or does not clearly stem from factual circumstances'.[61]

5.4.2.4 Implications for the TAS³ contractual framework

In Opinion 1/2010, the Working Party (re)emphasized the need for collaborating organizations to clearly allocate their mutual responsibilities under data protection law. As a result, the TAS³ contractual framework will need to consider how each entity involved in the implementation of TAS³ will acquit itself of the obligations associated with its role. While there is a certain degree of flexibility in the distribution of obligations and responsibilities[62], each actor's role must still be accounted for (in the sense that each actor's obligations under data protection law must be taken into account).

In section 5 of this Deliverable we have elaborated upon the different types of organizational models under which TAS³ might be implemented (cf. *supra*). During this discussion we distinguished among two main organizational models: a centralized and a distributed model.[63] How the service providers choose to structure their collaboration, together with the operational role of each actor, will

[57] Opinion 1/2010, *l.c.*, 24.
[58] Opinion 1/2010, *l.c.*, 22.
[59] Opinion 1/2010, *l.c.*, 22.
[60] Opinion 1/2010, *l.c.*, 22.
[61] Opinion 1/2010, *l.c.*, 24.
[62] Opinion 1/2010, *l.c.*, 25.
[63] We also indicated that the entirely centralized (all functions and control in one entity) and entirely distributed (no centralized functions or control whatsoever) models merely exist as the two end points of a continuum. It is highly unlikely, if not impossible, that either extreme could be implemented.

be of great importance when determining the legal qualification of each entity.[64] In order to facilitate the determination of which entity acts as a controller and which entity merely acts as a processor, we have developed an number of presumptions[65]:

- every service provider participating in a TAS³ implementation acts as a controller for the data that they process about the consumers of their services;
- each entity shall be considered a controller with respect to data processing activities, undertaken for its own account, unless it can be clearly demonstrated that it performs these operations on behalf of another entity;
- any centralization of decision-making concerning the modalities of data processing may implicate this central entity as a controller or co-controller, particularly where its decision-making power extends to either the purpose or the 'essential means' of the processing.

These presumptions will merely act as guiding principles in the further development of the contractual framework. Once a reference implementation model has been established, these assumptions will need to be tested in order to verify whether these provisional qualifications match with the actual role of each actor.

5.4.2.5 Conclusion and outlook

In Opinion 1/2010, the Article 29 Working Party has clarified many issues surrounding the controller and processor concepts. Most notably it has developed what was previously perhaps a binary analysis of controller or processor into a multifactor evaluation. Nevertheless, when applying the current definitions in practice there is still much room for discussion, and as a result, legal uncertainty.

Perhaps the main reason for this uncertainty resides in the criteria the Directive uses to establish control in the legal sense. 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 of the assessor. 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.

---

[64] For instance, whether or not a central body is authorized to dictate any of the processing modalities is likely to implicate this entity as co-controller for data protection operations where its decision-making authority extends to 'essential' elements of the processing.

[65] These presumptions have been developed on the basis of our reading of Opinion 1/2010, in conjunction with our analysis case studies which was performed for the second iteration of this deliverable (see pp. 33-44). Particular consideration was given to the Liberty Alliance and IMI models, as both these models are considered plausible implementation models for TAS³.

Nor does it mention how the structure of their collaboration might affect their respective obligations.[66]

A second reason why it is becoming increasingly difficult to apply the controller and processor concepts in practice is because these concepts were conceived with very specific data processing models in mind.[67] Those models lent themselves to a much more 'monolithic' and 'static' conception of control, which was in turn translated in the definition of actors and roles. Contemporary data processing models often involve a plurality of actors, which each influence 'the processing' to a greater or lesser extent. Due to these developments both doctrine and the Article 29 Working Party have adopted a more granular and flexible notion of control. This approach creates tension with some of the other objectives underlying the Directive, such as providing transparency towards data subjects. In addition, this approach is likely to cause difficulties when resolving questions of international private law, and may prove to undermine the efficacy of redress mechanisms.

In Opinion 1/2010, Article 29 Working Party has affirmed that the actors involved in data processing enjoy a certain degree of flexibility when allocating responsibilities among one and other. Be that as it may, the actual qualification of the role of an actor under data protection law cannot be established on the basis of contract alone. Applying the current controller and processor concepts will remain challenging, particularly when applying it to contexts such as TAS³ where the modalities of processing are influenced, at least indirectly, by the broader contractual framework within which they operate.

5.5 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 TAS³ trust infrastructure (anchor/founder) because the contractual framework in this situation is the most complete of the three possible architecture scenarios.[68]

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

[66] 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.

[67] See also 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; C. Reed, 'The Law of Unintended Consequences – Embedded Business Models in IT Regulation', *Journal of Information Law and Technology*, 2007, vol. 2, 8-9, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/reed/reed.pdf (last accessed 4 December 2010).

[68] Cf. section 4.5.

is captured in the OECD Guidelines for the Security of Information Systems and Networks[69] principle on responsibility:

> ***All participants are responsible for the security of information systems and networks.***
> *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 TAS[3] 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.

[69] http://www.oecd.org/dataoecd/16/22/15582260.pdf

5.5.1 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.

5.5.2 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.

5.5.3 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.

5.5.3.1 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.[70] 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)[71] provides a useful summary

[70] See TAS³ D6.1 at section 5.

[71] 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-

overview of the interrelation among the techical, business, legal and policy, components of TAS³.

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	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

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.

organization so that its members are only able process personal data in accordance to 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	authentication: additional measures to avoid unnecessary linkability, pseudonym 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	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)

integrity protected where appropriate 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)

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	4. Additional measures to avoid 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 4. The source of personal data and logic of processing shall be communicated when	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)

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.[72]

5.5.3.2 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.

The Article 29 Data Protection Working Party (WP 29) has developed guidance for how to comply with E-discovery requests[73]. This guidance was developed to

[72] 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.

[73] 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.

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 gather the necessary evidence
Security The requirements of security apply to	• This requirement, that court services also treat information

the court service, not just the organization complying	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[74] 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 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.

[74] 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.

6 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.

6.1 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.

6.2 End-user rights and obligations

6.2.1 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.[75] 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.

6.2.2 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.

[75] 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[76] 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

[76] 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.

7 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 (i.e. transactional) 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 the intake process for the individual end-users of TAS³ services (i.e. data subjects).

7.1 TAS³ intake process for organizations

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 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

7.1.1 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.

7.1.2 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 in relations to privacy, security and technical capacity.

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.

7.1.3 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.[77]

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.[78] 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.

One of the benefits of the Gap Analysis is to provide flexibility of implementation. With the potential breadth of roles, sizes, specialization and capacity among service providers it is very hard to presume that one size could fit all. Nothing in the Gap Analysis process, should however be understood to be a lessening of the legal requirements of compliance or the level of TAS³ standards. In fact the least flexibility exists in relation to technical capacity to participate in TAS³ as the technical requirements must be common across all service providers.

7.1.4 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.

7.1.4.1 Binding Service Providers to Policies

As has been discussed previously, one of the benefits of TAS³ is the collaborative and mutually supportive contract, policy and technology architecture. The main policies of TAS³ consist of Notice of Privacy Practices (NPP) and the TAS³ Minimum Security policy requirement and TAS³ technical security requirements.

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

[78] '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.

The policy documents are supplemented by supporting guidance, checklists and questionnaires. These supporting documents provide an effective mechanism form prospective service providers to describe and document their capacity to comply with the requirements outlined. We are further exploring how non confidential aspects of this information may be made available to the emerging reputations, and to the extent possible, a high level summary for individual end users[79].

The terms of the Ecosystem Contract will require service providers to meet the minimum requirements of TAS³ both in the operation of the specific service as well as related to the maintenance of expected minimum practices across the organization. These TAS³ requirements do not represent any intention for TAS³ to manage the non-TAS³ operations of participating service providers. The requirements represent a collective understanding of the need for greater commitment to both privacy and security in an attempt to develop a Trust Network based on solid fundamentals. A participating organization does not benefit the collective trust if it can only secure information while transacting in the TAS³ defined architecture, while not being able to properly protect credentials or other information they may be required to maintain related to transactions.

Furthermore, these polices are based on recognized international norms – for privacy, the EU Directive 95/46/EC and for Security ISO 27001 et seq.

Lastly, there is also a set of requirements related to the technical capacity to participate in TAS³. As was highlighted above, the evaluation of technical capacity is less a self-assessment with alternative means of compliance and more of a detailed evaluation of your technical capacity to participate.

In reviewing the three evaluations one will notice that they are closely related and in some case overlapping in what they ask. This is unavoidable due to the close relationship of the topics and also useful in that it allows for better evaluation of your grasp of importance nuances among the topics. For example, a security professional may consider a broader scope of access control permissible if they are not used to implementing concepts of data minimization. While no process is perfect, this intake process was developed with the hope of not only gauging the capacity of prospective service providers to comply and participate, but also in helping to further understanding of how TAS³ can help to optimize the configuration and implementation of privacy and security to enhance both trust and usability. Such an optimization would also lead to enhanced sharing and use of information for beneficial purposes because of that enhanced confidence.

7.1.4.2 Privacy

A questionnaire has been developed as part of the TAS³ service provider intake process. That questionnaire helps TAS³ consider the capacity of the organization

[79] While these are being considered, they are beyond the scope of the current deliverables. To the extent possible some of the requirements for such work will be specified.

to comply with both TAS³ privacy requirements and general legal requirements of data protection.

The NPP is the TAS3 public notice of privacy practices and has been drafted to work in conjunction with the End User license Agreement and may be found in annex IX. Because TAS³ is not a static environment and policies must be tailored to and supportive of specific transactions and because not all service providers can support all preferences. We have provided for Supplemental Notices of Privacy Practices (SNPP) where service providers can highlight special requirements or limitations related to processing that are not covered by the NPP. In order to increase usability, SNPPs will be available on the service provider website and highlighted at the time of transaction. SNPPs will also be centrally linked from the NPP site should a user wish to review these Notices and to facilitate comparison. Lastly, the NPP is supported by a matrix which provides users with greater transparency across collection and use of information in relation to TAS³ functions while also calling out issues of special concern and the available TAS³ controls.

The NPP also plays a role in the Intake Process as prospective Service providers have to ensure that their organizations can support the practices outlined in the NPP, both in terms of their participation in TAS³ transactions and more broadly in their operations as they may maintain information related to TAS³ transactions in general corporate systems.

7.1.4.3 Security

The security policy architecture of TAS³ is complex because not all operations of a service provider may be related to TAS³. Furthermore, it is possible that a service provider may play different roles depending on the nature of the transaction, and as such may support various level of assurance related to those transactions. Lastly, we have to consider the breadth of potential participants and the varying levels of technical capacity in how we address these requirements. This applies to both ends of the spectrum. For larger or more technically literate and security experienced organizations, they may just need to demonstrate how their existing policies and certification meet the specified requirements. For those smaller less security and technology experienced organizations (for examples medical practitioners in their offices) we will try to provide clear sets of obligations supported by draft policies.

There should be no mistake, however, that lack of security is not acceptable and no flexibility in acceptable policy description will lessen the specific requirements of technical and legal participation in TAS³.

The Security evaluation may be found in annex VII. It consists of a package of material related to the overall organizational minimum requirements of security. This also includes a self description of capacity to provide the basis or organizational security, based on requirements developed by Interpol and questions related to the ISO 27001 topics. We believe that the more experienced security organizations with dedicated staff should be able to use the questionnaires and provide existing policies to meet the requirements outlined.

For those prospective service providers with fewer technology support staff or less experience in drafting policies, the package will also include sample polices which may be used as starting points for policy development.

7.1.4.4 Technical Capacity Evaluation

As was noted above the intake process also requires the completion of a technical evaluation questionnaire which has been elaborated in the context of WP2. This questionnaire has been developed to both inform you at a greater detail level of the technical requirements of TAS3 and better enable our reviewers to determine of the prospective service provider can meet the technical requirements for participation. Organizations should provide as detailed a set of answers as possible with whatever documentation they you feel may support their responses or assertions.

7.1.5 Role of the TAS³ intake process for organizations

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:

1. the participants of the TAS³ Network have provided information on their policies 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.

7.2 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.[80]

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.[81] 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.[82] Where appropriate, we will make brief reference to how the proper implementation of a TAS[3] infrastructure can help an organization meet several of these accountability hallmarks.

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.

TAS[3] will support this first set of accountability hallmarks through the use of technology supported by a contractual framework that creates a user-centric,

[80] 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, October 2009, p.8)

[81] See Privacy Update 2009 in TAS[3] D6.1, annex 5.

[82] 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.

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.

TAS^3 provides both performance mechanisms (e.g. policy enforcement points) as well as decision support mechanisms (e.g., reputation engines. TAS^3 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.

TAS³ 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 TAS³. TAS³ 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,

7.3 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[83]. 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.

7.4 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

[83] 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.

elements cannot be varied, while the addressable elements can be met in a number of ways.[84]

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 would be enforceable by law against the organization if it misrepresented its capacity to comply[85].

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[86].

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.

---

[84] '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.

[85] 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.

7.5 TAS³ intake process for end-users

The purpose of this section is to outline the intake process for individual end-users of TAS³. The term 'end-user' as it is used here refers to the consumers of TAS³ services, not to employees or representatives of the service providers participating in a TAS³ Trust Network.[87] While the actual implementation of TAS³ may tailor to a variety of scenarios[88], this section will outline the sequence of events which ensure the necessary contractual binding of TAS³ end-users. During this discussion of the intake process, we will also highlight the legal implications of each step. Seeing as these implications are conditioned in part on the choice for a centralized or distributed implementation model, we will outline the main consequences under each model where appropriate.

As a preliminary matter, it is worth noting that every end-user intake process will involve the creation of an account with a recognized Dashboard Service Provider (DBSP). The Dashboard acts as the gateway for the end-user to TAS³ services and the creation of an account with a recognized DBSP has been deemed necessary in order to provide end-users with the functionalities TAS³ seeks to offer. The DBSP is an 'independent' service provider, in the sense that this service provider does not provide any other type of services within a given Trust Network. This has been deemed necessary in order to avoid potential conflicts of interest, and to ensure that it acts in the interest of the user at all times.

The intake process for end-users of TAS³ shall be comprised of three phases:

- Phase 1: Registration
- Phase 2: Provisioning of a Dashboard account
- Phase 3: Setting of privacy and trust preferences

7.5.1 Registration

In the first phase of the intake process, the applicant will be registered for the purposes of creating an account with a DBSP. The registration phase involves four subprocesses:

1) Interaction with a Registration Authority;

2) Verification of the identity of the applicant according to a specified or implied Level of Assurance (LoA);

3) Binding of a credential with the applicant;

4) Consent by the applicant to the TAS³ End-User and Licensing Agreement (EULA), the TAS³ Notice of Privacy Practices (NPP).

---

[87] Service providers participating in the TAS³ Network are referred to as 'TAS³ participants' or 'recognized TAS³ service providers'.

[88] See Deliverable D9.1. This Deliverable outlines several scenarios for both the employability and healthcare context. In our discussion of the intake process we have strived to make abstraction of the specific context for which intake is organized in order to identify the legal implications of each step of the intake process. However, reference will be made to context-specific consderations by means of examples as appropriate.

The modalities and implications of each of these steps will be elaborated over the following subsections.

7.5.1.1 Interaction with a Registration Authority

In order to be able to process the registration of an end-user, at least one entity must assume the role of Registration Authority (RA). In our current context, the Registration Authority can be described as a trusted entity that verifies and vouches for the identity of an applicant towards a recognized Dashboard Service Provider and the Trust Network Operator.[89] The RA can be an integral part of the DBSP, but it may also be separate entity provided that the necessary contractual arrangements are in place.

There is no definite list as to which type of entities might act as RA on behalf of a DBSP. Which entities are deemed eligible to assume this role will depend largely on the context of implementation. For instance, in the healthcare context, a hospital or physician might be trusted to act as a registration authority on behalf of one or more recognized DBSPs. Similarly, a placement agency might act as RA where job seekers are concerned.[90]

In the scenario whereby the DBSP does not observe its own registration processes, two sets of requirements will have to be met:

1. the entity performing the registration process will have to assume responsibility for the verification of the end-user's identity (see below)

2. the entity that wishes to act as RA must be formally recognized as being authorized to act as RA in the relevant context(s).

The enforcement of these requirements implies the implementation of certain technical and organizational measures.[91] From a contractual perspective, it is necessary that the delegation of authority from the DBSP to the RA is documented and agreed to by both the DBSP and the RA. This can be achieved in a number of ways. A first approach would be that the DBSP concludes bilateral

---

[89] This definition based on the definition of registration authority within the current draft of ISO and ITU-T joint project 29115/X.eaa (Entity Authentication Assurance).

[90] See TAS³ Deliverable D9.1 for further elaboration upon these scenarios. It is of course possible that an end-user contacts a DBSP directly for the sole purpose of creating a Dashboard account. In such a scenario the DBSP is likely to observe its own registration functions. A more plausible scenario is one where the end-user comes in contact with TAS³ through its interactions with another type of service provider who is already part of a particular TAS³ Network. In such a scenario there are essentially two options: either the 'local' service provider (i.e. the service provider that has direct contact with the end-user) redirects the end-user to a recognized DBSP (in which case the DBSP will conduct its own registration process), or the local service provider acts as RA on behalf of the DBSP. A third option would be that yet another entity (which is independent of both the local SP and the DBSP) acts as RA. We have chosen to focus on the second scenario for purposes of conceptual clarity. Similar considerations apply where the RA is an entity independent of both the SP and the DBSP.

[91] For more information concerning the components, processes and safeguards which need to be considered see B. Van Alsenoy, D. Cock, K. Simoens, J. Dumortier and B. Preneel, 'Delegation and digital mandates: Legal requirements and security objectives', *Computer, Law & Security Review* 2009, n°25, 422-430.

contracts with each entity it wishes to recognize as RA. This approach would arguably not scale well and would fail to take advantage of the contractual framework envisaged by TAS³. An alternative approach would be to bind every entity that wishes to act as RA by means of its participant contract. Provided that this contract adequately details the organizational and technical safeguards which must be implemented, the DBSPs within the Network will be able to rely upon this contractual binding when considering whether or not to allow other entities to observe registration processes on their behalf. In any event, records will need to be maintained (either locally or centrally) as to which entities within the TAS³ Network are authorized to act as Registration Authorities on behalf of a particular DBSP.

The initial interaction with the Registration Authority is likely to result in the completion of some type of application form. The personal information contained in such a form will vary according to the context of implementation. For instance, in the eHealth context an application form might contain a patient identifier or a reference to the patient's health insurance carrier. In the employability context such a form might list the individual's current employment status.

7.5.1.2 Identity verification

During the registration process, the identity of the end-user will have to be established and verified. This is necessary for a number of reasons. From a legal perspective, the first and foremost reason is that the service providers that participate in a given Trust Network are legally obliged to maintain the confidentiality and security of the personal data they control.[92] In order to be able to support the functionalities of the Dashboard (cf. *infra*), they will require assurance that an end-user of a Dashboard account in fact corresponds to the individual known to them. Without such assurance they run the risk of disclosing personal information to unauthorized entities.[93] The degree of assurance that a relying party has that an end-user is really who it thinks he or she is, is commonly referred to as the Level of Assurance (LoA).[94]

The Level of Assurance required for the registration process will be implementation-specific and depend mainly on the types of services that are offered within the Trust Network in question. For example, in the eHealth context one is likely to impose relatively high assurance requirements, as medical data is considered extremely sensitive. Note that the verification of the identity

[92] Although the security obligation is incumbent upon the controller, art. 17, 2 of Directive 95/46/EC requires that processors are contractually bound to the same obligation. Consequently this statement can be generalized to all service providers in the TAS³ Network, regardless of whether or not they may be qualified as controller.

[93] As will be discussed in greater detail later on, the Dashboard in fact supports many functions relating to data controller obligations. The participating service providers will therefore require appropriate assurance that the end-user asserting herself as a particular data subject is in fact the same individual.

[94] For more information see TAS³ Deliverable D7.1, third iteration, in particular section 4.1.2. Although the term 'LoA' is often used to refer to the degree of assurance supported during (remote) authentication, the LoA concept also extends to the individual components and processes that jointly determina the overall level of entity authentication assurance.

of applicants can be done either remotely or in-person, depending on how the registration process is organized.

7.5.1.3 Credential binding

Regardless of whether the registration process is conducted in-person or remotely, this process will have to establish how the applicant will be given access to his Dashboard account once it is created.

It is currently not envisaged that the DBSP will act as identity provider towards its end-users. In other words, it is not expected that the DBSP itself will issue the credentials that enable end-users to log on to their Dashboard accounts once they are created. This implies that use will be made of the services of (other) identity providers, who may either be TAS³ participants themselves, or offer their services without any formal affiliation whatsoever to the TAS³ Trust Network in question.

The Level of Assurance (LoA) required of the credentials to access the dashboard account will similarly be implementation-specific and depend mainly on the types of services that are offered within the Trust Network in question (comp. supra).

An interesting question to consider is who decides which credentials or identity providers shall be considered acceptable within a particular Trust Network for a particular service. These decisions could be made centrally (e.g., at the level of the Operator of the Trust Network) or locally (at the level of the individual DBSP). Under a completely decentralized approach, every entity determines for itself which credentials it is willing to accept. Every entity would specify on its own which LoA it requires for a particular transaction; as well as carry out its own assessment of which credentials are considered to satisfy each LoA. Under a completely centralized approach, the Operator of the Trust Network would specify the LoA requirements for each service, and mandate the use of certain credentials to satisfy these requirements. As described earlier (cf. supra; section 5.3), the centralized and distributed models exist as the two endpoints of a continuum. A hybrid approach might be one where the Operator of the Trust Network publishes a list of credentials which are recognized as supporting a particular LoA, but still allows each entity to specify its own LoA requirements for each transaction.

The choice for any of the aforementioned models is relevant from a legal perspective for a number of reasons. In first instance, the degree of centralization is likely to affect the assessment of whether or not the Operator acts as a co-controller in relation to certain processing operations. Secondly, even the slightest degree of centralization may imply the need for additional contractual binding, both at the ecosystem level ('TAS³ framework agreement') and the participant level ('TAS³ participant contract'). For instance, where the Operator of a Trust Network wishes to mandate the use of certain credentials for certain services, the framework agreement will have to provide for the obligation of each participant to abide by its decisions. Similarly, the identity providers which are recognized as supporting a particular LoA would have to be contractually bound

to (continue to) implement the corresponding technical and organizational measures to ensure the envisaged LoA is maintained.[95]

7.5.1.2 EULA

Once the identity of the applicant has been established, she will be asked to express her agreement with the TAS³ End-User and Licensing Agreement (EULA). A preliminary draft of a reference EULA for TAS³ implementations can be found in annex VIII.[96] It contains the following sections:

1. Scope
2. Privacy
3. Dashboard
4. Transparency
5. Security
6. Restrictions and obligations upon use
7. Complaint and redress
8. Limitation of liability
9. Changes in terms
10. Termination
11. Applicable law in jurisdiction
12. Contact information

One aspect which merits additional elaboration at this point is the scope of the TAS³ EULA. Its scope is articulated in terms of 'TAS³ services'. A TAS³ service can be defined as any service offered by a recognized TAS³ service provider which is clearly marked as being a TAS³ Service by means of the TAS³ service logo. The other party to the EULA is the Trust Network Operator.[97] As a result, the terms of EULA have implications far beyond the relationship between the end-user and the DBSP alone. This approach was taken for a number of reasons:

---

[95] In instances where an identity providers is not a member of the Trust Network, reliance will be placed on the Credential (or Certificate) Practice Statement (CPS) of the identity provider in question, and it will essentially be a business decision for either the Operator or participants of the Network to rely on its services.

[96] This draft is a work in progress, and will be improved in collaboration with the pilot partners and business developers as the exploitation plans for TAS³ mature.

[97] We do not expect that in practice there would be just one well-defined TAS³ Trust Network; but rather one or more TAS³-enabled trust networks. Hence the EULA would be between the end-user and the legal entity that acts as "operator" or "administrator" of a particular TAS³ trust network. However, we have chosen, for purposes of simplification, to refer to "the" TAS³ Trust Network Operator and "the" TAS³ Trust Network.

- in order to enhance transparency towards end-users: all of the end-user rights and obligations which remain consistent across TAS³ service providers can be listed in this document, so that the need for additional terms and conditions when interacting with recognized TAS³ service providers can be minimized;

- in order to enhance end-user trust: the Trust Network Operator acts as a 'trust guarantor' by warranting that recognized TAS³ service providers will adhere to the promises specified in this document[98];

- in order to leverage the TAS³ contractual framework: the EULA is in fact the counterpart of the 'TAS³ participant contract' which recognized TAS³ service providers must adopt. This implies that all rights and obligations specified in this agreement will (directly or indirectly) benefit and/or burden all the service providers participating in the Trust Network.

Where appropriate, rights and obligations which apply specifically in relation to the TAS³ Dashboard have been called out separately (see in particular sections 3 and 4 of the EULA).

7.5.1.3 Notice of Privacy practices

In addition to the EULA, the applicant will also be asked to (separately) express her agreement with the TAS³ Notice of Privacy Practices (NPP). A preliminary draft of a reference NPP for TAS³ implementations can be found in the annex IX.[99] It contains the following sections:

1. Information Collection,
2. Collection limitation
3. Purpose of Collection
4. Use Limitation
5. Consent
6. Access, Correction, Retention and Deletion
7. Security
8. Oversight and Accountability
    i. Audit
    ii. Complaint/Redress
    iii. TAS³ Commitment
9. Legal Compliance / Jurisdiction

[98] Under the current draft of the EULA, all the rights of the end-user which are consistent across individual TAS³ services are warranted by the Trust Network Operator. It is worth noting that this commitment goes beyond that which can be technically enforced by the TAS³ architecture. Under a lighter trust model, whereby the Operator is not able or unwilling to assume such a commitment, the Operator might limit its obligations to act a mediator and facilitator in the resolution of disputes among end-users and recognized TAS³ service providers.

[99] This draft is also a work in progress, and will be improved in collaboration with the pilot partners and business developers as the exploitation plans for TAS³ mature.

The TAS³ Notice of Privacy Practices (NPP) was drafted to work in conjunction with the TAS³ EULA. It aims to inform both end-users and prospective participants of the main types of processing which take place within TAS³, as well as of their rights as data subjects and relevant TAS³ privacy practices.

The NPP was organized according to the major requirements of EU data protection law. The NPP provides a plain language statement of the principle (such as notice, or purpose of collection) and then provides information on how TAS³ enables compliance with those requirements. The NPP also serves as the top line notice of what information is collected and how it is used. Because the concepts of notice, purpose of collection and use are so closely interconnected, we have supplemented the privacy policy with a matrix that relates the information elements connected to the TAS³ function, related concerns and relevant controls. The NPP also provides the TAS³ network level information on practices related to security, legal compliance/jurisdiction, consent and compliance and oversight.
.

7.5.1.4 Additional terms and notices

The TAS³ End-User Licensing Agreement and Notice of Privacy Practices do not cover every aspect of the relationship an end-user might have with a TAS³ service provider (other than the DBSP). Where the registration process is observed by a service provider other than the DBSP, it is likely that it is doing so in the context of one of its own services. The modalities of these services and the processing operations they involve are not covered by the TAS³ EULA or initial Notice of Privacy Practices. Depending on the current status of the relationship between the service provider and the end-user, consent to additional terms and notices may be necessary.[100]

An example might help clarify this issue. If a medical practitioner is conducting the registration process, he or she is probably doing so in the context of a relationship of care. The ultimate aim of the practitioner is not the creation of a Dashboard account as such, but rather to allow the patient to view and manage her personal health information. Depending on whether or not (and if so, how) the patient had already consented to the processing of her medical information, additional consent may needed to provide a legitimate basis for such processing.

7.5.2 Provisioning of a TAS³ Dashboard account

As indicated in the introduction of this section, every intake process will involve creation of an account with a recognized DBSP on behalf of the end-user. The end-user's Dashboard acts as the gateway to TAS³ services. All the functionalities that TAS³ seeks to offer end-users (see below) will be made available to them through the Dashboard.

[100] Similarly, consent to additional terms and notices are likely to be necessary once the individual has become an end-user of TAS³ and starts to interact with other service providers. However, the TAS³ EULA and NPP should allow such terms and notices to be shorter and more comprehensible, as service providers within the Network will be able to leverage these documents in their own terms and notices.

Provisioning occurs as a result of the completion of the registration process (phase 1). The completed application form (or a copy of its contents), along with relevant identity assertions, credential information, etc. is forwarded[101] to the DBSP and the latter creates an account for the end-user.

It is important to distinguish the TAS³ Dashboard from so-called Personal Data Stores (PDS). Within TAS³, a PDS is an account maintained by a recognized PDS service provider which allows end-users to store certain information about themselves.[102] This information can be made available to other entities in the Network at the discretion of the user.[103] The main difference between data contained in a PDS and data held by other service providers is that other service providers typically maintain this information for a different business purpose (i.e. a purpose other than merely facilitating user control).

Every end-user of TAS³ will need to have a Dashboard account, but not every end-user will need to have a PDS. The role of the Dashboard is to allow end-users to view and manage their personal information regardless of which entity within the Trust Network actually holds the data. These functionalities can only be provided to the extent that the data in question has been used in the context of a TAS³ service.[104]

The TAS³ Dashboard will offer end-users of TAS³ the following functionalities:

1. the ability to set privacy and trust preferences in relation to TAS³ services
2. the ability to authorize transfer of personal information from one service provider to another[105]
3. the ability to view which service providers within the Network store information about her (provided this information has at one point been used within the context of a TAS³ service)
4. the ability to view which operations have been performed upon this data[106]
5. a 'one-stop shop' for exercise of data subject rights and a complaint mechanism[107]

[101] In instances where a DBSP acts as its own Registration Authority the application information is simply transmitted to the logical entity charged with account generation.
[102] A PDS might contain information certified by third parties (data 'about' me) or self-asserted information (data 'by' me).
[103] The discretion of the user of course still remains subject to the policies of a particular Trust Network. For instance, the Operator or a service provider within a Trust Network might specify that information maintained by a certain type of service provider may not be released in the context of a job placement service, even if the user were to authorize such a transfer. Sectoral legal requirements (e.g. statutory duties of confidentiality) may impose additional restrictions. See also Deliverable D9.1, third iteration, section 4.1.2.1.
[104] See also section 4 of the EULA.
[105] As indicated earlier, such data portability may be subject to certain limitations contained either in legislation or in the policies of the Trust Network.
[106] This functionality is supported by the TAS³ audit and notifications services, which are described in detail in deliverable D8.2, second iteration (see in particular section 4.1.1.5).
[107] Section 6.2 of deliverable D2.1 (version 20) describes how the Dashboard enables end-users to exercise their rights of access, correction and deletion.

Service providers participating in the Trust Network (other than the DBSP) will have to lend their co-operation in order to support aforementioned functionalities. For example, each service provider will have to make available summary audit reports in order to support the audit trail viewer (which enables users to see what operations have been performed upon their personal information). Either the TAS³ framework agreement or the individual participant agreements shall include an obligation for each recognized service provider to forward summary audit reports.

7.5.3 Setting of privacy and trust preferences

Once the end-user has (been[108]) logged in to her Dashboard account, she will be invited to review her privacy and trust preferences for her personal information. This constitutes the final phase of the intake process.

Which information the end-user is able to specify preferences for at this stage will vary. In the scenario that an end-user directly contacted a DBSP for the sole purpose of creating a Dashboard account, there will not be much information to manage other than the information collected during the registration process (e.g., the contents of the application form). In the scenario where the Dashboard account was created in the context of a pre-existing relationship (e.g., to enable a patient to view and manage her health information), additional information may be available (e.g., the contents of her medical health record).

It is envisaged that the Dashboard will be configured with certain default preferences. Which default preferences are deemed appropriate and who specifies them will depend both on the context and model of implementation. For instance, under a centralized model, the Operator of the Trust Network might dictate that participating service providers configure certain default preferences. Under a decentralized model each service provider would specify its own defaults independently of other actors in the Network.

Regardless of who defines the default policies, the implementation context is likely to impose certain constraints on the freedom of the user. For instance, sectoral legal requirements (e.g., statutory duties of confidentiality) may impose certain limitations.[109]

Taking these constraints into account, it is envisaged that end-users will be able to express their preferences in the following terms:

- the categories of recipients of his personal data;
- what their processing capabilities shall be (read, write, edit, delete, ...);
- for which purpose.

[108] In cases where the registration process is completed online, it is likely that the end-user will be immediately directed to her account.
[109] See also Deliverable D9.1, third iteration, section 4.1.2.1.

Depending on the implementation, the end-user might also be able to formulate specific constraints (e.g. specify the time-period in which the processing operation is allowed to take place) and whether or not an operation is to be dependent on specific obligations (e.g. delete after two weeks).
Once the end-user has reviewed these preferences the intake process is complete.

8 Defining the Where

Jurisdiction in transnational transactions has always been inherently complex as the analysis is always one undertaken in two parts.[110] First is the most basic question of jurisdiction: does the Court or body in question have the right to regulate the conduct in question? In other words, is the court or body the right organization to adjudicate the matter? Once that is established, the conflict of laws issue must be addressed: namely, which law should apply to matter in question? The questions, taken together, sometimes create competing venues claiming jurisdiction wishing to apply different laws. As time progressed, land based complexity was augmented by planes and boats further requiring questions of jurisdiction to be answered outside of state boundaries, taking into account flag carriers territorial waters boundaries of air space to name but a few complicating factors.

The advent of the Internet and developments of global sourcing and cloud computing have exponentially multiplied this complexity. Information is now processed and distributed globally based on a variety of needs and across various communications channels. The basic question of jurisdiction in electronic commercial transactions on the Internet has never been answered: If Philippe, domiciled in Paris, visits a website hosted and owned by a company in Canada, has Philippe gone to the Canada to shop or has the Canadian Shop opened a store in Paris.

8.1 Internet Jurisdiction – European Perspective

Jurisdiction over e-commerce transaction in the EU is not an issue of first impression. In 2000, the EC adopted Directive 2000/31/EC on Electronic Commerce (hereafter referred to as 'the E-Commerce Directive').[111] The E-Commerce Directive adopted the principle of the country of origin, as evidenced by the following recitals:

> (22) Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives; to that end, it is necessary to ensure that the competent authority provides such protection not only for the citizens of its own country but for all Community citizens; in order to improve mutual trust between Member States, it is essential to state clearly this responsibility on the part of the Member State where the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established.
>
> (23) This Directive neither aims to establish additional rules on private international law relating to conflicts of law nor does it deal with the jurisdiction of Courts; provisions of the applicable law designated by rules of

[110] See generally: Kuner, Christopher Internet Jurisdiction and Data Protection Law: An International Legal Analysis, Draft version of article, available at *www.privacyconference2010.org/upload/Conflict%20**Kuner**_article.pdf*.

[111] Directive 2000/31/EC; Official Journal of the European Communities L178/4, 17, 7, 2000.

> private international law must not restrict the freedom to provide information society services as established in this Directive.

The E-commerce Directive, was not however the only EC activity on this issue. There is a long history in the legal framework of protecting consumer rights in online environments. The Brussels regime, consisting of the Brussels Convention[112], the Lugano Convention[113] and later the Brussels I Regulation[114] were developed to support a Single Market by making judgments enforceable across contracting states, but seeks to protect weaker parties by making the country of destination (consumer's domicile) the basis of jurisdiction.

The seeming conflict between the two positions, country of origin and consumer's domicile, while confusing, may not actually be a conflict[115]. The resolution goes back to our two part jurisdiction analysis. Brussels I applies to the first part or which court should have jurisdiction, while the E-Commerce Directive, specifically disclaims that it covers jurisdiction and concerns itself with what the applicable law should be. Thus it would be consistent with the legal framework for a consumer to be able to bring an action in their local court, but have it be decided based on the applicable law of the country of the seller.

While this seeming conflict is capable of resolution, we also have to factor in the jurisdictional elements contained in Directive 95/46 on Protection of personal data. In the case of the Data Protection Directive, the establishment of the controller seems to be a defining factor pursuant to article 4:

> Article 4
>
> National law applicable
>
> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
>
> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
>
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

---

[112] Convention of 27 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters.
[113] Convention of 16 September 1988 on jurisdiction and the enforcement of judgments in civil and commercial matters.
[114] Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. See in particular recitals (11) through (13).
[115] See Generally: Olof Leps, Jurisdiction in E-commerce: A non-existing conflict of law and the consequences for consumer protection and SMEIs, European Law Blog, 22, 6, 10 – http://olofleps.blogspot.com/2010/08/jurisdiction-in-e-commerce-non-exisisting.html

> 2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

A number of additional factors are at play when establishing jurisdiction in relation to data protection. As was noted above the largest is the concept of establishment – where the controller has set up shop at its most basic concept. The most interesting development of Article 4 is found in the paragraph describing the controller not being established in the jurisdiction but "making use of equipment, automated or otherwise, situated on the territory of the member state". The reason for the importance of this phrase is how it may be interpreted in today's technology; in the 1980s and 90s equipment of a physical and substantial nature that was related to the concept of establishment. In this regard, Kuner has noted that[116]:

> *The term 'equipment' betrays the origins of the EU Data Protection Directive in the pre-Internet era. At the time the Directive was adopted (in 1995, just before the Internet began to become widely popular), the concept of 'equipment' in Article 4(1)(c) was generally thought to refer to a computer, telecommunications network, or other physical object which a data controller could locate in a Member State and then operate remotely from an establishment outside the Community. The text of the Directive is of little help in determining the meaning of 'equipment', and the Explanatory Memorandum gives only 'terminals, questionnaires, etc' as examples, which hardly provides much guidance.*
>
> *Much controversy has been generated regarding application of EU law based on the use of so-called 'cookies' sent to the hard drives of users in Europe from servers based outside the EU. The Article 29 Working Party has taken the position that, in the case of the sending of 'a text file installed on the hard drive of a computer which will receive, store and send back information to a server situated in another country' (i.e., a cookie), the national law of the EU Member State of the user will apply to the processing of such data. The Working Party has affirmed this position, and has taken similar positions with regard to JavaScript, ad banners, and similar technologies. In addition, the Working Party has found that the personal computer of an individual located inside the EU that is 'used' by a non-EU based data controller constitutes 'equipment' that results in the application of EU law to the controller.*

Jurisdiction in the EU is thus a matter of the competence of the court to hear the case, a determination of what law should apply in the case and indicia of establishment and effect in within the EU in the case of controllers outside the EU.

[116] Kuner, Christopher Internet Jurisdiction and Data Protection Law: An International Legal Analysis, Draft version of article, *l.c.*, at pp 32-33

8.2 Implications for TAS[3]

In the longer term, as cloud computing becomes more prevalent and as computer aware environments create seamless interaction of services, people, preferences and objects, TAS[3] like all other service providers will need to come to terms with how to deal with concepts of jurisdiction predicated on national borders in an information society based on global information flows.

In the near term, TAS[3] has chosen to use the jurisdiction of the data subject as the contract jurisdiction for the End User License Agreement. Thus, much of the complexity that exists today at the consumer level may be avoided the consumer will be able to rely on local courts and Authorities.

The Governance Board of TAS[3] will be responsible for establishing the jurisdiction where actions can be brought by service providers. At the B2B level, TAS[3] will also benefit from the clarity of the E-commerce Directive in resolving choice of law issues.

TAS[3] may be exposed to greater jurisdictional complexity if some service providers rely on organizations to process information outside of the EU. Such global sourcing models are becoming more common across all sectors. Any TAS3 related transfer ourside of the jurisdiction would have to be compliant with legal requirements and enabled by explicit or supported by notice and model contracts (or one of the authorized approaches authorized by Directive 95/46). Service providers will be required to make compatible jurisdictional specification in those contracts and are also required to provide notice of transfer of information outside the jurisdiction and obtain required consents as appropriate.

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.

PART II
IMPLEMENTING THE CONTRACTUAL FRAMEWORK

1 Introduction

In the second part of this deliverable we provide structured overview of the main components of the contractual and governance framework of TAS³. This part II builds upon Part I of which has set forth the theoretical underpinning of these frameworks.

In section 2 we provide an outline of the governance framework of TAS³, which contains an overview of the layers, actors, and roles of the TAS³ ecosystem.

Section 3 provides a comprehensive overview of the contents and structure of the Trust Network Agreement. This section is supplemented by a number of important annexes, including the TAS³ End User License Agreement (EULA), the TAS³ Notice of privacy practices (NPP), the TAS³ Participant Questionnaire, an IT security requirements checklist and TAS³ technical capacity requirements.

Section 4 provides a summary overview of the intake processes for service provides and end-users, in order to maintain conceptual clarity in our overview of the components of the contractual framework.

Section 5 provides an outline of the TAS³ Ecosystem Contract (EC), which is the contract which binds all Service Providers joining the Trust Network to their general obligations as participants of the Trust Network.

Section 6 will detail the properties and components of TAS³ participant contracts, which will contain the specific obligations of a service provider in light of its role within the Trust Network and transactions it is likely to engage in.

Finally, section provides a glossary of relevant terms related to these implementation processes, providing a comprehensive overview of both actors and instruments.

All of the sections of Part II are interdependent: the governance framework, Trust Network Agreement, Ecosystem Contract, Participant Contracts, TAS3 policies and intake processes all work together. A good example is the interrelation and interdependence between contract and governance elements. TAS³ relies on the contractual framework to provide proper binding of rights and obligations across all parties. The governance framework provides the structural underpinning of the ecosystem and establishes the relationships and roles among the actors as well as the high level allocation of responsibilities via the governing board and the Trust Network Agreement. Binding to relevant TAS3 policies and more detailed operational rules are communicated and enforces by the Trust Network Operator through the Ecosystems Contract. Further operational requirements may be specified at the role or transaction level through Service Provider contracts and sticky polices.

Part II is presented in the order of events in order to assist the reader in better understanding the interaction and interdependence described above.

2 The Layers of the TAS³ Ecosystem

The TAS³ Ecosystem consists of three layers. Each layer is governed by an overarching set of rules, policies and procedures which must be complied with in order to render implementations of TAS³ trustworthy. The purpose of this section is to provide an overview of the different layers of the TAS³ Ecosystem, together with a brief description of the actors and roles envisaged for each layer.

The following three layers can be distinguished[117]:

1. the **TAS³ governance layer**: this is the layer where the rules and policies of the TAS³ Trust Network are established;

2. the **TAS³ administration layer**: this is the layer where the rules and policies which have been established for the Trust Network are enforced;

3. the **TAS³ operational layer**: this is the layer where transactions occur in accordance with the rules of the Trust Network.

Each layer of the TAS³ Ecosystem comprises a number of actors, which each have their own roles and responsibilities. The following figure provides a conceptual overview of the types of entities that operate on each layer:

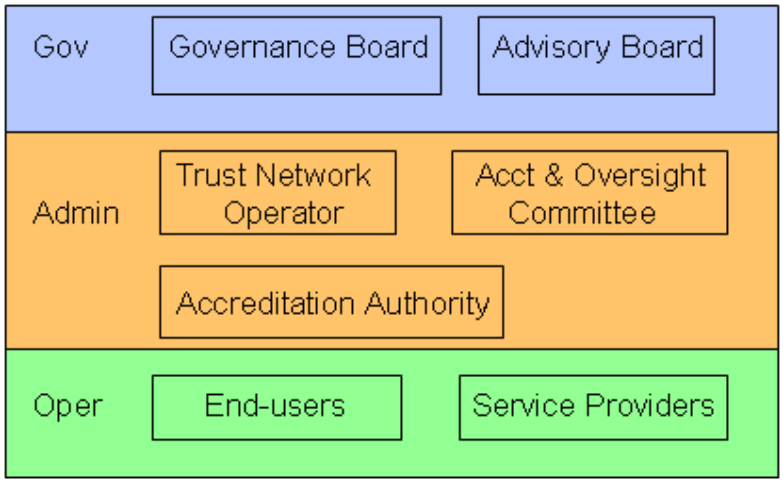


Figure 1 – Layers and Actors of the TAS³ Ecosystem

These relationships among the actors involved in each layer are determined by the document through which the founding members establish the Trust

[117] This representation of the TAS³ Ecosystem is an adaptation of the model found in the draft 'National Strategy for Trusted Identities in Cyberspace', which was issued by the US Department of Homeland Security (DHS) in June 2010 (full text available at: http://www.dhs.gov/xlibrary/assets/ns_tic.pdf) . Kindred models have been elaborated by other bodies such as the Kantara Initiative (see http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0) and Microsoft (see the Open Identity Trust Framework [OITF], available at http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/oitf.aspx) which have also served as a source of inspiration.

Network.[118] We refer to the agreement among the founding member of a particular Trust Network as the '**Trust Network Agreement**'.[119] As we discuss the various actors and their roles, reference shall be made to this document and the provisions it is expected to include. A detailed outline of the contents and structure of the Trust Network Agreement can be found in section 3.

2.1 The TAS³ governance layer

The TAS³ governance layer consists of the actors and interactions that establish the rules of the TAS³ ecosystem, including the criteria for participation within a particular Trust Network.[120]

The TAS³ governance layer is comprised of the following actors:

1) the TAS³ Governance Board

2) the Trust Network Advisory Board

2.1.1 The Trust Network Governance Board

2.1.1.1 Role

The Governance Board (GB) is the entity that presides over the Trust Network and its operations. The GB acts as the 'rule-maker' for the Trust Network.

2.1.1.2 Tasks

The GB is charged with defining the requirements, policies and procedures that will be implemented within the Trust Network. More specifically, it has the responsibility to establish and adopt:

- the criteria service providers must meet if they want to join the Trust Network (i.e. the criteria for becoming a 'TAS³ participant' or 'recognized TAS³ serviced provider');

- how the criteria for becoming a TAS³ participant will be assessed (e.g. self-assessment, independent audit, etc.);

- the rules which must be adhered to by the various participants to the Trust Network when interacting with one and other;

- rules, procedures and processes that must be followed by the actors charged with enforcement of the rules it has adopted;

---

[118] We do not expect that in practice there would be just one well-defined TAS³ Trust Network; but rather a number of TAS³-enabled trust networks. However, we have chosen, for purposes of simplification and conceptual clarity, to refer to "the" Trust Network.

[119] The signatories to this agreement are referred to as the 'Founding Members' or 'Founders' of the Trust Network.

[120] See also US Department of Homeland Security (DHS), 'National Strategy for Trusted Identities in Cyberspace', *l.c.*, 12.

- ultimate oversight of the proper functioning of the TAS³ Network.[121]

The decisions adopted by the GB will specify the requirements for the administration and operational layers of the TAS³ ecosystem. While this is described as a top-down development process, the GB is meant to be a learning body. As such the GB will institute mechanisms to receive requests and feedback in order to stay abreast of how its rules, policies and requirements are functioning.[122] The GB will also be responsive to changes in legal frameworks and decisions of relevant authorities on the implementation of the law to assure that TAS² rules, policies and procedures remain compliant.

2.1.1.3 Composition

The Governance board will be comprised of delegates of the service providers participating in the Trust Network. The initial members of the TAS³ GB are expected to be (delegates of) the Founding Members of the TAS³ Trust Network.[123] However, the Trust Network Agreement will need to consider the representative capacity of all players, including those that join the Network after it has been established.[124]

2.1.1.4 Mode of operations

The mode of operations of the Governance Board is established by the Trust Network Agreement. This agreement will at a minimum contain provisions concerning:

- membership criteria;
- frequency of meetings;
- voting procedures (including qualified majority requirements, balloting procedures etc.)

2.1.1.5 Relationship towards the administrative layer

The Governance Board will be empowered by the Trust Network Agreement to delegate certain tasks to the Trust Network Operator and to the Accountability and Oversight Committee (cf. *infra*), in order to accomplish the purposes for which the Trust Network was created. It should be noted that GB may also delegate the authority to create other required bodies to further the implementation of the Trust Network; thus creating a cascading scale of responsibility for the tasks and roles assigned.

---

[121] In all probability at least portion of these rules will be established at the outset of the creation of the Trust Network. For instance, the Trust Network Agreement should specify the actors at the governance and administrative layers, as well as the rules concerning their mode of operations and relationship towards one and other The rules that govern the operational layer should be formally adopted by the GB (even where a baseline set of rules might already be drafted in preparation of the creation of the Trust Network, the actual approach to implementation must be subject to GB approval).

[122] Particularly those entities that are charged with observing administrative and operational functions will have the ability to request changes.

[123] As discussed section 5.2 of part I, the creation of a Trust Network (i.e. the TAS³ implementation) can take place under a variety of organizational models: Trust Anchor, Trust Consortium Convenor, etc.

[124] For instance, not all participating service providers will be Founding Members. The Trust Network Agreement will have to set forth their voting rights in relation to decisions adopted by the GB.

As far as the rule-making process is concerned, it is essential that the rules that govern the Trust Network (beyond that which is specified in the Trust Network Agreement) are formally adopted by the GB. Certain rules applicable to the operational layer might be (further) developed in conjunction with one or more entities charged with the administration of the Trust Network.[125] Regardless of which entity or entities actually draft(s) these rules, they must be approved and formally adopted by the GB.

2.1.2 The Trust Network Advisory Board

2.1.2.1 Role

The Trust Network Advisory Board (TNAB) is a consultative committee comprised of stakeholders and external experts.

2.1.2.2 Tasks

The main task of the TNAB is to articulate recommendations towards the Governance Board on how to improve the functioning of the Trust Network (e.g., suggest additional requirements for service provider participation, recommend improvements to the technical architecture).

2.1.2.3 Composition

The TNAB is meant to be an independent body comprised of representatives of the various stakeholders of the Trust Network (e.g. consumer advocacy groups, regulators), together with independent experts.

2.1.2.4 Mode of operations

The mode of operations of the TNAB will be established by the Trust Network Agreement. It may be expected that for certain aspects the Trust Network Agreement limits itself to general terms and confers upon the TNAB to establish its own rules of internal organization. However, the Trust Network Agreement is likely to at least include provisions concerning:

- membership criteria;
- frequency of meetings;
- decision-making procedures and rules on the establishment of subcommittees[126];
- institutional safeguards designed to guarantee independency (e.g., avoid conflicts of interest).

Note that the TNAB does not have any voting rights within the Governance Board. This should facilitate participation of stakeholders who must retain the ability of being publicly critical (e.g., regulators). While the members of the TNAB might be subject to certain obligations of confidentiality (e.g., proprietary information on company operations, including potential new services or

[125] This may include interpretation of the policies and procedures as well as more practical implementation guidance. For instance, rules specified by the GB may be articulated in a general manner which need further specification when applied to a specific role or function.

[126] Creation of subcommittees may be appropriate where subject matter becomes extremely technical.

organizational changes), these obligations may not be of such nature that it would effectively impair their ability to publicly criticize the operations of the Trust Network in general or decisions adopted by the GB in particular.

2.1.2.5 Relationship towards the Governance Board

The Trust Network Agreement will specify the nature of the relationship of the TNAB towards the Governance Board and how these bodies are to interact with one and other. For example, the Trust Network Agreement might specify that the recommendations made by the TNAB must be considered by the Governance Board within a certain time-frame, or impose qualified majority requirements in case the Governance Board wishes to disregard (repeated) recommendations articulated by the TNAB.

2.2 The TAS³ administration layer

The TAS³ administration layer consists of the actors and interactions which ensure the application and enforcement of the rules decreed by the TAS³ Governance Board.[127] These actors are charged with ensuring that the Governance Board rules, policies and procedures are observed by the actors of the operational layer.

This layer includes the following actors:

1) the Trust Network Operator

2) the TAS³ Accreditation Authority

3) the TAS³ Accountability and Oversight Committee

2.2.1 The Trust Network Operator

2.2.1.1 Role

The Trust Network Operator (TNO) is the main administrator of the Trust Network.

2.2.1.2 Tasks

The TNO is charged with the implementation of the rules set forth by the Governance Board. More specifically, the TNO:

- ensures proper communication of the rules to service providers participating in the Trust Network ('TAS³ participants' or 'recognized TAS³ service providers');

[127] US Department of Homeland Security (DHS), 'National Strategy for Trusted Identities in Cyberspace', *l.c.*, 12.

- acts as the counterparty (signatory) on behalf of the GB in the relationships with the end-users and service providers participating in the Network;

- establishes and monitors the working of the TAS³ Accreditation Authority (cf. *infra*);

- specifies the detailed obligations for participants (consistent with those outlined in the Trust Network Agreement) in light of their expected activities within the Trust Network;

- receiving and handling complaints by individual end-users (which may involve consultation with or arbitration by the Accountability and Oversight Committee; cf. *infra*);

- administers appropriate sanctions towards TAS³ participants (which may have been preceded by consultation with or arbitration by the Accountability and Oversight Committee; cf. *infra*)

2.2.1.3 Composition

The TNO is a legal entity (or group of legal entities) that dispose(s) of the relevant expertise (administration, compliance, technical capacity) to administer the Trust Network. The TNO can either be:
- a separate legal entity created by the GB for the specific purpose of administering the Network;
- an existing organization (or group organizations) hired by the GB; or
- one or more of the members of the GB who under take this role pursuant to a delegation of authority by the GB.[128]

2.2.1.4 Mode of operations

The mode of operations will be defined in consideration of the composition of the TNO, but must be consistent with the general terms of the Trust Network Agreement as well as any specific rules adopted by the GB. The Trust Network Agreement should at a minimum establish how accountability towards the GB shall be ensured, as well as the relationship between the TNO and the Accountability and Oversight committee (cf. *infra*)

2.2.1.5 Relationship towards the Governance Board

The Trust Network Operator derives its authority directly from the Governance Board and acts as an agent on its behalf. It shall be accountable towards the GB at all times.

The Trust Network Agreement shall specify reporting obligations of the TNO towards the GB. Such reporting obligations should be both periodic (e.g.

[128] Where this is the case, the Trust Network Agreement shall detail the requirements to avoid conflicts of interest and establish how separation duties will be realized.

quarterly activity reports) and incidental in nature (e.g., investigations, breaches, issues with termination/addition of participants, operational issues.

In between reporting and in-person briefing, the TNO must keep a detailed record of all activities, detailing not only decisions and actions taken, but the rationale and supporting evidence for the action of decision taken. These records must be available for review by GB upon request.

The TNO shall not have not any formal rule-making authority, except that which is conferred upon it within the constraints set forth by the Trust Network Agreement.[129] The TNO might provide the GB with recommendations in light of its practical experience, but any rule change must be approved and formally adopted by the GB.

2.2.1.6 Relationship towards end-users

The warranty for end-users that their personal data will be processed in accordance with the rules of the Network is presented by the TAS³ GB through the TNO. End-users joining a Trust Network will contract with the TNO rather than (or in addition to) with a participating service provider (although one or more service providers might observe the intake process on behalf of the TNO; cf. *infra*; section 4.1).

The TNO shall (from a contractual perspective) either (a) take on (part of) the liability in relation to TAS³ services or (b) act as a mediator in the allocation of liability among the Network participants to the extent that a centralized method of indemnity or pooling is not in place.

2.2.1.7 Relationship towards TAS³ participants

Service providers joining the TAS³ Network will contract with the TNO. The TNO acts on behalf of the GB executing contracts with participants.

The TNO oversees the intake process for service providers which is observed by the TAS³ Accreditation Authority (cf. *infra*).

The TNO also has the operational responsibility to oversee the proper functioning of the Trust Network. In this capacity it will oversee that the operations take place in accordance with the rules of the Network, the enforcement of which may involve collaboration with the Accountability and Oversight committee (cf. *infra*).

[129] As indicated earlier, certain rules applicable to the operational layer might be (further) developed in conjunction with one or more entities charged with the administration of the Trust Network. However, regardless of which entity or entities actually draft(s) these rules, they must be approved and formally adopted by the GB.

2.2.2 The TAS³ Accreditation Authority

2.2.2.1 Role

The Accreditation Authority (AA) observes the formal recognition of service providers as TAS³ service providers.[130]

2.2.2.2 Tasks

The AA is charged with intake of service providers that wish to participate in the Trust Network ('prospective TAS³ participants'). Its tasks include:

- acting as registration authority towards service providers that wish to join the Trust Network.
- communicating relevant documentation concerning the criteria for participation, requirements and policies of the Trust Network;
- collecting and maintaining relevant application information (e.g., completed questionnaires, gap analyses)[131]
- evaluating the applications of prospective TAS³ participants (which may or may not result in a formal assessment of the service provider's capacity to comply);
- ensuring appropriate contractual binding of the prospective participant (which includes both the signing of the Ecosystem contract and the counterpart participant contracts which are tailored to the role the service provider plans to assume).[132]

In case of successful completion of the intake process, the AA issues the appropriate credentials to indicate that the service provider is a 'recognized TAS³ service provider'. Such credentials must include a specification for which types of services this recognition applies. In addition, the AA will confer upon the TAS³ participant the appropriate licenses to in relation to the use of TAS³ intellectual property (e.g., the TAS³ service logo) together with a specification of how and in relation to which activities this intellectual property may be used.[133]

---

[130] Of course, there is in principle no restriction as to the number of entities which might act as an Accreditation Authority. We merely use the singular for purposes of conceptual clarity.

[131] Under the current reference implementation prospective TAS³ participants must complete a self-assessment form and gap analysis (cf. infra; section 4.2). However, there are many other levels of vetting are conceivable, the rigor of which impacts the actual assurance offered by the TNO.

[132] These contract terms will bind service providers to technical and policy requirements, both in terms of those expressed at the intra- and inter-organizational level as well as in terms of using the appropriate trust technologies to honor the preferences and choices of users as to use and sharing of personal information. For more information see section 4.2.

[133] See also Kantara Initiative, 'Identity Assurance Framework: Assurance Assessment Schemes', v0.9, 12 October 2009, available at http://kantarainitiative.org/confluence/download/attachments/655421/Kantara+IAF-1300-Assurance+Assessment+Scheme.pdf.

2.2.2.3 Composition

The AA is an entity (or group of entities) with relevant expertise in the field of service provider accreditation and/or certification. The AA can either be:
- an organizational department within the TNO;
- an external organization (or group organizations) hired by the TNO; or
- one or more of the members of the GB who under take this role pursuant to a delegation of authority by the GB.[134]

2.2.2.4 Mode of operations

The mode of operations of the AA will be consistent with its composition (which might be specified to a certain extent by the TNO, but must be consistent with the general terms of the Trust Network Agreement as well as any specific rules adopted by the GB). The organizational practices of the AA are likely to be determined in part also by relevant standards.

2.2.2.5 Relationship towards the TNO and GB

The AA can be established in several ways. It might be established by the Trust Network Operator as a department within its own organization. Alternatively, the TNO might appoint an independent entity to perform the intake process on its behalf. In all cases GB approval is required for the final determination of how the AA is constituted and implemented. In addition, as the TNO answers directly to the GB, the AA shall remain indirectly accountable towards the GB.

In any case, where the AA is an independent entity the delegation of authority by the TNO to the AA must be appropriately documented and the Accreditation Authority will have to bound to observe the norms set forth by the TNO, the GB and/or the Trust Network Agreement respectively.

2.2.3 The TAS³ Accountability & Oversight Committee

2.2.3.1 Role

The Accountability and Oversight Committee (AOC) is the entity responsible for monitoring compliance of activities within the Network with the rules set by the Governance Board.

2.2.3.2 Tasks

The tasks of the AOC include[135]:

---

[134] The degree of independence of the AA (together with the level rigor applied when evaluating participants; cf. supra) is likely to impact the overall perception of trustworthiness of the Network.

[135] The tasks of the AOC will be determined largely by how much authority the Founding Members of the Network are willing to bestow upon it. Its powers of oversight may range from limited (e.g., verification of documentation and contractual binding) to moderate (e.g., running of online compliance testing protocols) to very high (e.g., on-site compliance verification of internal policies and practices of participating service providers). The

- receiving and handling appeals by individual end-users and participating service providers against decisions rendered by the TNO (which may involve investigations, meditation, arbitration and/or redress);

- running the online compliance testing protocols to verify proper implementation of the TAS³ architecture and compliance with the reference policies set forth by the GB;

- receiving and following up on notifications by TAS³ participants (e.g. security breaches, reports of suspicious behaviour by fellow participants);

- monitoring the implementation by the TNO of the requirements set forth by the GB.

2.2.3.3 Composition

The AOC is an entity (or group of entities) with relevant expertise in the field of audit and oversight. The AOC must be appointed directly by the Governance Board and must be independent of both the TNO and/or AA.[136]

The AOC may include (delegates of) members of the GB based where they have relevant expertise, but also must have non GB members. The AOC should be provided with the authority to retain specific experts to serve as advisors to the committee (e.g. if further expertise is required) and to appoint external auditors as needed.[137]

2.2.3.4 Mode of operations

The mode of operations of the AOC will depend largely on the composition of this entity and breadth of the powers the Founding Members wish to accord it (e.g., limited to running of OCT or also on-site compliance verification).

The mode of operations of the AOC shall specified at a high level in the Trust Network Agreement, with the details to be drafted by the GB (or by the AOC itself with the with review and approval of the GB). The GB should consult the Advisory Board when determining the composition and mode of operations of the AOC.

2.2.3.5 Relationship towards the Governance Board

The AOC will be established by the GB and will report directly to it.

The Trust Network Agreement shall specify reporting obligations of the AOC towards the GB. Such reporting obligations should be both periodic (e.g. quarterly activity reports) and incidental in nature (e.g., investigations, breaches,

---

overview provided here enumerates the tasks of the AOC under the current reference implementation model.

[136] The Accountability and Oversight Committee may not be an agent of the TNO as this would lead to conflicts of interest.

[137] The role of such auditors will depend largely on the scope of the investigative powers accorded to the AOC under the terms of the Ecosystem contract which is signed by all service providers participating in the Network.

issues with termination/addition of participants, operational issues). Where the AOC ascertains issues of compliance it will keep the GB apprised of any material issues in or risks to the network. The AOC is directed to work in conjunction with the TNO in addressing and resolving issues that arise (see below). The AOC shall immediately inform the GB if it believes that the TNO is either in derelict of its duties or otherwise engaged in behaviour that violates any of the rules set forth by the GB or as contained in the Trust Network Agreement.

2.2.3.6 Relationship towards the Trust Network Operator

The AOC and the TNO each have their own responsibilities in ensuring that the Trust Network functions in accordance with the rules set forth by the GB. Whereas the TNO is involved mainly in overseeing the vetting and contractual binding of TAS³ participants (ex ante), the AOC oversees compliance through audit reviews and oversight (post fact). Each is tasked with working constructively with the other in maintain the trust and operational effectiveness of the Trust Network. While needing to work together, both are also tasked with monitoring the proper functioning of the other and are to report any suspicious behaviour or irregularities they observe to the GB.

The TNO and the AOC also have a specific relationship with regards to complaint handling (see below).

2.2.3.7 Relationship towards end-users

The AOC has a direct relationship with end-users only in the context of complaint handling. If an end-user believes her personal data has been processed in an unauthorized manner, she should first either address the issue with the service provider in question (if she can readily identify that service provider), or direct her complaint to the Trust Network Operator[138]. The AOC is positioned primarily as an appellate body towards the TNO, in that it will receive complaints from individual end-users where they believe the approach adopted by the TNO is inadequate.

The role of the AOC as either a mediator or as a administrator of redress will depend on the nature of the warranty provided by the TNO in the End-User and Licensing Agreement (EULA).[139]

---

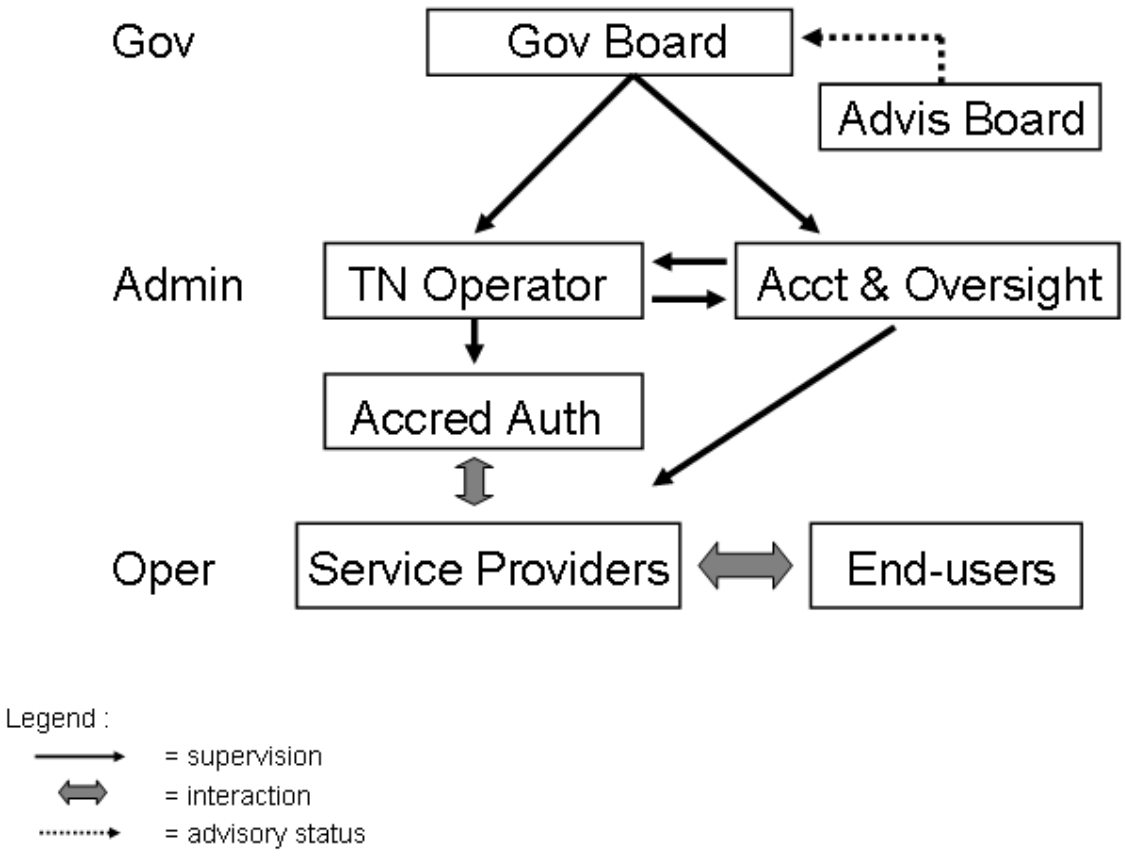
[138] This process is meant to increase the efficiency of resolution. All service providers are required to receive complaints regarding service and appropriately channel them through the Network. A user wishing to complain can thus do so to any TAS3 entity, but the further from the relevant service provider the longer it may take to properly direct and resolve. The end-user retains the ability .

[139] In the current draft of the EULA, the Trust Network Operator assumes 'front-end' liability for certain warranties made in relation to TAS³ services (e.g., enforcement of privacy and trust preferences specified through the Dashboard). The underlying notion is that the TNO should act as a 'Trust Guarantor' towards end-users for the operations that take place within the Network (at clearly identified levels of liability with further recourse to the service provider(s) causing the harm for any loss beyond those levels of liability), so that the user has a central point from which it can obtain redress in case of

2.2.3.8 Relationship towards TAS³ participants

The AOC shall receive certain powers of investigation and arbitration pursuant to its oversight and complaint handling powers. The breadth of these powers shall be determined at a high level in the Trust Network Agreement and specified in detail in the Ecosystem contracts which all participating service providers are bound to.

Where complaints have been found justified, but are merely of a minor or incidental nature (and provided they were not intentional), the AOC will request that the service provider implement the appropriate changes. Where a TAS³ participant either fail to adopt the requested changes in reasonable cure period, or has demonstrated an intent to violate rules or gross negligence related to their implementation or operation, or where remediation has legal consequences, the AOC will make a recommendation for Governance Board approval. Some of these issues may await the periodic meeting of the governance board, the most urgent matters may require a special meeting.[140]



breach. Of course, lower-trust models are conceivable whereby the TNO assumes no front-end liability; and e.g. limits the scope of the commitment to mediation and/or assisting the end-user in bringing its complaint before the courts.

[140] Meetings and voting of the board will need to be established by conference call and via e-mail to the greatest extent possible permitted by law.

Figure 2 – Relationships among actors of the Trust Network

2.3 The TAS³ operational layer

The TAS³ operational layer is the layer where transactions occur in accordance with the rules of the TAS³ Ecosystem.[141]

The TAS³ operational layer is comprised of the following categories of actors

1) End-users

2) Identity providers and Attribute Authorities

3) Trust Infrastructure Service Providers

4) Application-specific service providers

In the following section we will provide a brief description of the role assumed by these different actors. Note that the categorization of service providers is presented for purposes of conceptual clarity only. Each category identified below groups a number of functions and operations a particular service provider might engage in. It is not expected that service providers will be confined to one specific category, on the contrary. Service providers participating in the Trust Network can offer many different types of services and thus are likely to combine (subsets of) the various roles enumerated here.[142]

2.3.1 End-users

End-users are the consumers of TAS³ services. Their interaction with the administrative and governance layer is limited. In principle they only interact with application-specific service providers, except in the context of complaint handling.

The intake process for end-users is outlined in section 4.1.

2.3.2 Identity Providers and Attribute Authorities

An Identity Provider or Identity Service provider can be described as an entity that verifies, maintains, manages, and may create and assign identity

[141] US Department of Homeland Security (DHS), 'National Strategy for Trusted Identities in Cyberspace', *l.c.*, 12 and 14.

[142] From a contractual perspective, each service will have certain obligations and restrictions associated with it. The intake process for service provider will ensure that each service provider is bound to the obligations corresponding to the services it wishes to offer or the role it will assume (see also *infra*; section 4.2). We are currently exploring how to either define a set of service provider contracts that can be executed as needed, or develop a contractual template which contains all the required terms which remain static and which supports the inclusion of additional paragraphs able to be sourced form a library of role-based clauses. The latter approach has certain benefits over the former, as it would enable the easier addition of new roles, while preventing the replication of the more static template terms across a myriad of contracts.

information of other entities.[143] Within federations IdPs often have the role of facilitating Single Sign On (SSO).[144] Attribute Authorities are entities which confer attribute values (other than identity information) upon end-users. Both entities act an authoritative source within a particular context, in the sense that the information they provide is considered sufficiently reliable by the participants to a transaction.[145]

2.3.3 Trust Network Infrastructure Service Providers

Trust Network Infrastructure Service Providers (TNISPs) are entities that offer 'core' TAS³ services, i.e. those services that are critical to proper functioning of the Network at the operational layer. Such services include:

1. Dashboard: the Dashboard acts as the gateway for end-users towards TAS³. All the functionalities that TAS³ seeks to offer end-users will be made available to them through the Dashboard.[146]

2. Service integration: consists of operations that enable or facilitate the exchange of information across recognized TAS³ service providers (e.g., discovery of resources, identifier conversion, business process engines, SOA gateway).

3. Trust and reputation: comprises the operations that allow the association of a trust score or reputation with recognized TAS³ service providers (e.g., feedback mechanisms, rating systems, ranking of service providers).

4. Credential validation: consists of operations that verify the authenticity of credentials as well as whether or not they emanate from a trusted source.

5. Policy enforcement: this category comprises operations that ensure that each entity is only able to perform the actions it is authorized to perform (e.g., the capturing, retrieval and application of policies, the association of obligations or constraints).

6. Audit trail: consist of the operations which enable verification that the rules that apply within the Trust Network have been complied with (e.g., logging of transactions, communication of summary audit reports to authorized recipients).

Most of the aforementioned services (with the exception of the Dashboard) represent conceptual components of the TAS³ architecture. As such it is unlikely

[143] ITU-T SG 17, x.1252 Baseline identity management terms and definitions, available at http://www.itu.int/rec/T-REC-X.1252-201004-I/en.
[144] TAS³ glossary.
[145] See TAS³ Deliverable D7.1, 'Design of Identity Management, Authentication and Authorization Infrastructure', third iteration, 2010, section 2.2.
[146] As a result, every end-user intake process will involve provisioning of a Dashboard account. The Dashboard allows end-users to (a) set privacy and trust preferences in relation to TAS³ services; (b) authorize transfer of personal information from one service provider to another; (c) see which service providers within the Network store information about her (provided this information has at one point been used within the context of a TAS³ service) as well as view which operations have been performed upon this data; and (d) exercise of their data subject rights. See also section 4.1.

that any of these services are entirely centralized within one entity, seeing as the TAS³ architecture is distributed by nature. However, certain functions might be observed by dedicated Trusted Third Parties depending on the implementation model.

2.3.4 Application-specific service providers

Application-specific service providers are those entities which offer services directly towards the end-users of TAS³ (e.g., a hospital or placement agency). These entities are referred to as 'TAS³ participants' or 'recognized TAS³ service providers'.[147]

[147] End-users are bound to come in contact with TAS³ in the context of their interactions with such service providers which is why they might perform intake functions on behalf of the TNO and/or Dashboard Service Provider.

3 The Trust Network Agreement

3.1 Introduction

The previous section provided a conceptual overview of the layers of the TAS³ Ecosystem, as well as a description of the actors involved at each layer. Throughout the presentation of this overview several references were made to the Trust Network Agreement (TNA) and the provision it is expected to contain. The purpose of this section is to provide a comprehensive overview of the contents and structure of the Trust Network Agreement.

3.2 Outline of the Trust Network Agreement

As discussed in part I of this deliverable, the founders of a federation can organize themselves under a variety of models, among which the three models identified by the Liberty Alliance: Collaborative, Consortium and Centralized models.[148] Once the founders have decided upon and agreed to an organizational model, they will then need to define how the Trust Network will be governed and operated.[149]

The Trust Network Agreement is the contract among the founders that establishes the Trust Network and its organizational structure. The TNA further establishes, at a very high level, the operating rules for the Trust Network Network as a whole, as well as the roles, responsibilities and interactions among the top level administrative and governance bodies including: the Governance Board, the Trust Network Operator (and through it the Accreditation Authority), the Accountability and Oversight Committee, and the Trust Network Advisory Board.

The following overview is a conceptual outline of the contents of the Trust Network Agreement:

1. Contracting purpose/Founders' Mission
   1.1. Description of Governance Model
2. Organizational Structure – potential Incorporation, Cooperative model, etc
3. Governance Board
   3.1. Mission
   3.2. Composition
   3.3. Membership criteria
   3.4. Tasks
   3.5. Manner of voting
   3.6. Compensation/Reimbursement

[148] See section 5.2.1 of part I.
[149] The organizational model that is chosen will have significant impact on the allocation of responsibilities and definition of how both power and obligation are actually apportioned.

3.7. Right to delegate certain powers
  3.7.1. Creation of Committees
    a. Permissions or Exclusions (what role/function can/can't be delegated – may be by example)
    b. Powers
    c. Limitations/required GB approval
    d. Organization
    e. Operational procedures
    f. Reporting requirements
  3.7.2. Ability to retain third parties
    a. Types of activities
    b. Qualifications/Requirements
    c. Contracting consideration
    d. Conflicts check
  3.7.3. Authority to establish and empower a Trust Network Advisory Board as well as Administrative bodies needed to run the Trust Network including the Trust Network Operator and the Accountability and Oversight Committee

4. Trust Network Advisory Board (TNAB)
  4.1. Mission
  4.2. Composition (experts with relevant expertise and stakeholder)
  4.3. Membership criteria
  4.4. Structural elements (size, terms etc)
  4.5. Tasks
  4.6. Internal organization
  4.7. Convening requirements and advisory process

5. Trust Network Operator (TNO)
  5.1. Mission
  5.2. Composition
  5.3. Structural elements (separate legal entity)
  5.4. Tasks
    5.4.1. TNO will be the contracting entity with the service providers and will oversee and authorize agents able to execute the EULA.
    5.4.2. TNO will also develop the specific rules for the service providers in the Ecosystem and Service Provider contracts in a manner consistent with the TNO and subject to the review and approval of the GB.
    5.4.3. May be staffed by third parties, or GB employees with relevant expertise
    5.4.4. If GB employee(s) are involved, there must be a clear definition of job function and a signed employment agreement specifying responsibility and reporting to GB and confidentiality/non-disclosure obligations related to sensitive information of other GB members that do not need to be disclosed as part of the performance of the position.
    5.4.5. Detailed disclosure of potential conflicts related to any staff of TNO and required approval of GB by supermajority if potential conflict is found to exist
    5.4.6. Define reporting requirements to GB

5.4.7. Enable TNO to create needed subsidiary bodies, specifically the Accreditation Authority (AA), develop charters and operating rules for such bodies which should be submitted for review and approval to the GB

5.4.8. Allow TNO to develop and propose other detailed operating rules for GB review and adoption.

6. Accountability and Oversight Committee (AOC)
   6.1. Mission
   6.2. Composition
      6.2.1. May be staffed by third parties, or GB employees with relevant expertise
      6.2.2. If GB employee(s) are involved, there must be a clear definition of job function and a signed employment agreement specifying responsibility and reporting to GB and confidentiality/non-disclosure obligations related to sensitive information of other GB members that do not need to be disclosed as part of the performance of the position.
      6.2.3. Detailed disclosure of potential conflicts related to any staff of (AOC) and required approval of GB by supermajority if potential conflict is found to exist
   6.3. Structural elements (separate legal entity)
   6.4. Tasks
      6.4.1. AOC will have general responsibility related to accountability and oversight including overseeing the audit responsibility. The AOC will also serve as an appellate body that will review requests from individuals not satisfied with complaint resolution from the TNO.
      6.4.2. Define reporting requirements to GB
      6.4.3. Ability to retain experts to provide advice and assistance in completing their mission.
      6.4.4. Ability to develop and propose other detailed operating rules for GB review and affirmation
      6.4.5. Relationship between TNO and AOC including mutual oversight roles, AOC's appellate role, and shared responsibilities of complaint-handling and compliance

   6.5. Liability Model and Allocation among founders
      6.5.1. Determine how to create pooled Guarantee fund
      6.5.2. Contributions
      6.5.3. Purchase insurance
      6.5.4. Mechanisms for liability allocation
      6.5.5. Determine amount of liability to be covered (Guarantee)
      6.5.6. While Guarantee is meant to be available to aggrieved individual in case of harm, should this be a shared cost?
      6.5.7. Allocation of costs to replenish guarantee to organizations that were proximate cause of harm or otherwise negligent actors
         6.5.7.1.1. Shared allocation in case of system or architecture failure not occasioned by any single service providers
      6.5.7.2. Consider more general insurance coverage for larger harms
         6.5.7.2.1. Self-insured w/allocated percentage across all founders and service providers according to an agreed formula

6.5.7.2.2. Procure insurance and allocate premiums as costs across service providers and founders according to an agreed formula

7. Breach of contract provisions
   7.1. What constitutes a material breach
   7.2. Notice of breach
   7.3. Opportunities to cure
   7.4. Evaluation of cure
   7.5. Special conditions/limitation that may result from cure
   7.6. Failure to timely cure
      7.6.1. Notice
      7.6.2. Consequences

8. Terminations
   8.1. Notice of termination
   8.2. Voluntary
   8.3. For cause
   8.4. Rights of appeal
   8.5. Public notice
   8.6. Actions to remove privileges and access
   8.7. Returning, deleting or securing information assets both PII and TN in general
   8.8. Obligations surviving termination

9. Requirements to comply with law enforcement and legal process
   9.1. Review of compliance request
      9.1.1. Where permitted by law to be provided to TNO for response
   9.2. Requirement that requests comply with legal form and due process requirements
   9.3. Right to inform data subject or other TN participants subject to request where permitted by law so as to allow them to interpose defenses
10. Force majeure, four corners, severability, addresses, signatures and other boilerplate terms.

4 Intake

4.1 Introduction

In order to be able participate in the Trust Network, be it as a service provider or as an individual end-user, an intake process must be completed. These intake processes have been described extensively in part I of this deliverable.[150] The purpose of this section is to provide a summary overview of the respective process in order to maintain conceptual clarity in our overview of the components of the contractual framework.

4.2 Intake process for End-Users

The intake process for End-Users of TAS³ shall be comprised of three phases:

1) Phase 1: Registration
- Phase 2: Provisioning of a Dashboard account
- Phase 3: Setting of privacy and trust preferences

4.2.1 Registration

In the first phase of the intake process, the applicant will be registered for the purposes of creating an account with a recognized Dashboard Service provider and establishing a contractual relationship with the TNO. The registration phase involves four subprocesses:

5) Interaction with a Registration Authority;

6) Verification of the identity of the applicant according to a specified or implied Level of Assurance (LoA);

7) Binding of a credential with the applicant;

8) Consent by the applicant to the TAS³ End-User and Licensing Agreement (EULA), the TAS³ Notice of Privacy Practices (NPP).[151]

4.2.2 Provisioning of a TAS³ Dashboard account

Every intake process will involve creation of an account with a recognized Dashboard Service Provider on behalf of the end-user. The TAS³ Dashboard will offer end-users of TAS³ the following functionalities:

6. the ability to set privacy and trust preferences in relation to TAS³ services

[150] See section 7.5 of part I.
[151] The EULA and the NPP can be found in Annexes VIII and IX respectively.

7. the ability to authorize transfer of personal information from one service provider to another[152]
8. the ability to view which service providers within the Network store information about her (provided this information has at one point been used within the context of a TAS³ service)
9. the ability to view which operations have been performed upon this data[153]
10. a 'one-stop shop' for exercise of data subject rights and a complaint mechanism[154]

4.2.3 Setting of privacy and trust preferences

Once the end-user has (been[155]) logged in to her Dashboard account, she will be invited to review her privacy and trust preferences for her personal information.

4.3 Intake for Organizations

Other than the intake process for end-users[156], the intake process for organizations requires interaction with the TAS³ Accreditation Authority. The interaction with the TAS³ Accreditation Authority can be broken down into 4 main phases[157]:

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

4.3.1 Organizational guidance

In the first phase of the intake process, prospective participants of the TAS³ Network shall provided with guidance concerning the characteristics ('hallmarks') of accountable organizations.

[152] As indicated earlier, such data portability may be subject to certain limitations contained either in legislation or in the policies of the Trust Network.
[153] This functionality is supported by the TAS³ audit and notifications services, which are described in detail in deliverable D8.2, second iteration (see in particular section 4.1.1.5).
[154] Section 6.2 of deliverable D2.1 (version 20) describes how the Dashboard enables end-users to exercise their rights of access, correction and deletion.
[155] In cases where the registration process is completed online, it is likely that the end-user will be immediately directed to her account.
[156] In the case of end-users, intake functions are likely to be observed in whole or in part by a service provider that is active on the operational layer at the Trust Network. See section 7.5 part I.
[157] See section 7.1 through 7.4 of part I.

4.3.2 Self-assessment

In the second phase of the intake process, the prospective participant to the TAS³ Network is provided with a self-assessment questionnaire. The completion of this questionnaire will support the determination as to whether or not it meets the criteria for TAS³ participation in relations to privacy, security and technical capacity.

4.3.3 Gap analysis

During the third phase of the intake process a gap analysis is performed by the service provider in which the organizational policies of the prospective participant are compared to the TAS³ reference model policies. This gap analysis is then subsequently evaluated by the TAS³ Accreditation Authority.

The gap analysis is conducted by prospective service providers as way of explaining how they comply with the TAS³ requirements outlined in the TAS³ Notice of Privacy Practices and TAS³ security documentation. In the case of the NPP, the gap analysis should use the answers to the questionnaire and relevant policies of the service provider to explain how they meet the requirements outlined in the NPP. For security requirements, the gap analysis likewise maps the answers to the questionnaire with the relevant polices of the service provider to explain how they are meeting TAS3 security requirements.

Both the privacy and security gap analysis are submitted as inputs to the intake process which the AA will evaluate to determine whether the prospective SP has appropriately satisfied all relevant requirements. As part of this evaluation process, the AA may seek clarification or further support of compliance with requirements.

The gap analysis process exists in recognition that you may structure and group obligations across different policies. The broad variety of existing implementations, both technical and policy, coupled with the potential breadth of roles, nature of information, a scope of responsibilities make it necessary to have flexibility in implementation. Nothing in this recognition of flexibility however should be understood to mean a lessening of requirements, which is why the Gap Analysis is subject to review to assure that all needed requirements are satisfied.

While there may be some limited latitude in meeting the technical capacity requirements, there is no formal gap analysis process as there must be great consistency in the implementation of these technical requirements. Any accommodation in the method of implementation will be considered on an ad hoc basis.

4.3.4 Contractual binding

If the applicant service provider has successfully completed the three prior steps it will be asked to enter into contractual relationship. All prospective participants are required to sign the Ecosystem Contract, which binds them to

the policies mentioned above, as well as to general terms and conditions of the TAS³ Network. The main policies of TAS³ consist of:

- the TAS³ Notice of Privacy Practices (NPP);
- the TAS³ minimum security policy requirements; and
- TAS³ technical capacity requirements.

In addition, every participant will be required to conclude additional Participant Contracts in light of their role/functions they will assume within the Trust Network. Finally, service providers will be bound as well to transactional obligations as contained in sticky policies.

5 The Ecosystem Contract

5.1 Introduction

The Ecosystem Contract (EC) is the contract which binds all Service Providers joining the Trust Network to their general obligations as participants of the Trust Network.

The EC builds upon and must always remain consistent with the Trust Network Agreement. The EC must be formally adopted and approved by the GB.[158] Where the TNA has a more structural function (setting up the Trust Network, defining the roles and responsibilities of the main entities in governance and administration and the general rules of TN operation), the EC supports the structural elements of the TNA by binding all parties to more detailed statements of obligations and implementation of TN Policies and high-level rules of the TN. Other than this the EC is an operational document that implements TN requirements related to transactions. We highlight this difference to explain the slight different approach in outlining the contract framework for the EC. In the EC outline, we have grouped the obligations under organizing themes and types of requirements. This approach allows for a closer matching of contractual operational obligations to Trust Network functions.

It should also be noted that the EC serves as the central repository for obligations, the myriad references to policies are references to documents either annexed or incorporated by references. The drafting structure foresees potential for changes in policy to occur on a more frequent basis that revision of the contract.

5.2 Main properties

The main properties of the Ecosystem contract are as follows:

1. The EC will be executed between the TNO (acting on behalf of the GB) and the participating Service Providers

2. The EC will bind signatories to the general requirements of the Trust Network, including the requirement that service providers continuously adopt TAS^3 policies or have similar policies in place

2. The EC will incorporate the End-User and Licensing Agreement (EULA) as an attachment and establish that individuals that sign the EULA are made third party beneficiaries of the Ecosystem Contract.

3. The EC will build upon the structural elements of the Trust Network at the service provider level including:

[158] While in practice the Ecosystem Contract may be drafted by the TNO, it requires approval by the GB.

a) Defining participation criteria for service providers to join the Trust Network
b) Relationship between SP and GB, including potential for SPs to participate in GB either directly or through representatives as appropriate depending on the structure of the GB established under the TNA.

4. The EC application process will be subject to terms and conditions. While the terms and conditions will not be part of the EC, the obligations related to those terms and conditions (providing true, accurate and current information, for example) will survive the application process and be incorporated into the EC.

5.3 Terms governing the intake process for organizations

Prior to signing the EC any prospective SP must successfully complete the intake process. This section outlines the terms and conditions related to intake process. While not formally part of the EC , these terms and process requirements are so directly related to the EC that they discuss them here for purposes of conceptual clarity.

The terms related to the intake process shall include:

1) A statement which indicates that in order to successfully complete the Intake Process, a service provider must:
   a) Complete all questionnaires, evaluations, self-assessments and Gap Analyses for
      i) Technical capacity to participate in TAS3 Infrastructure and use TAS3 standards
      ii) Privacy, both in relation to dedicated TAS3 operations and for their general business operations
      iii) Security both in relation to dedicated TAS3 operations and for their general business operations[159]

   b) Provide all relevant documentation supporting sections a and b above; including but not limited to certifications, audits, evaluations and other objective reports which may attest to capacity to comply with technical or policy requirements, third party evaluations or certification of proper implementation and functioning of technical environment or business processes and reports on training of personnel or personnel credentials of technical or compliance capacity.

      i) All documentation provided will be made available as an input into the Reputation score of the SP

[159] Information stored outside of TAS[3] must also be protected by privacy and security policies that meet minimum requirements.

ii) To the extent that some information is too confidential or sensitive in nature, there is the potential for a redaction process.

iii) SPs must consider that such redaction, if related to information useful to prove capacity, may result in lower reputation scores.

2) Terms related to what constitutes a successful completion of the intake process, including:

a) The criteria and notification processes for a successful completion of the intake process that will lead to TAS3 certification

i) This will include defining any further steps required to become a TAS3 SP, including, but not limited to the execution of related contract documents.

b) The notification and reapplication process related prospective SPs that do not meet the success criteria of the Intake Process. General information should be provided to the failed prospective SP on what were the major shortcomings of the application. The information will be neither a detailed roadmap of changes nor indication of potential future success. There is a value in prospective SPs having a level of self-awareness of both needs and potential shortcomings.

c) The processes related to review by the TAS^3 Accreditation Authority

3) Consequences for providing false or misleading information

a) Any discovery of false or misleading information being provided in this process or of material information being omitted will be considered a material breach of the EC. Depending on the nature of the specific situation, the TNO will either detail the conditions for curing the breach, or may in its discretion suspend the SP and require a complete reapplication. Where a complete reapplication is required, the decision will be reviewed by the AOC.

b) If such omission, obfuscation or falsification set forth in Para g above is found to be intentional or resulting from gross negligence, the TNO may bar the SP in question from future participation in the TN or suspend the SP and require them to complete a reapplication and review subject to closer scrutiny and possibly requiring higher thresholds of disclosure or proof on specified elements related to the breach.

i) Barring SPs from future participation shall be reviewed by the AOC which will provide its recommendation to the GB for approval

c) Findings of material breach of terms, including whether such breaches have been cured, shall be provided in appropriate form to reputation engines and other trust/compliance elements of the TN.

i) Minor or incidental breaches of terms may only be reported by the TNO these entities with the approval of the AOC

5.4 Outline of the Ecosystem Contract

5.4.1 Foundational elements

The Ecosystem Contract shall in first instance comprise a number of foundational elements which will bind participating service providers to the general mission, policies and requirements of the Trust Network.

The execution of the Ecosystem Contract will entail that the service provider accepts:

1. The mission of the Trust Network as expressed in the Trust Network Agreement

2. That they are undertaking specific responsibilities for TAS³ participation in the TN as well as general responsibilities regarding their overall use of information, security and privacy controls.

3. That they will participate in the trust evaluation and oversight processes of TAS³, including, but not limited to: providing information to reputation engines, audit oversight processes, investigation and compliance processes.

4. That they shall be bound to the terms of the:

   4.1 The technical requirements of TAS3
   4.2 Notice of Privacy Practices and any, more specific, TAS3 privacy requirements
   4.3 Security requirements and any, more specific, TAS3 security requirements
   4.4 Any instructions which may be carried with the information within the TN. This instruction, often accepted by performance of the required tasks should be considered supplemental contract terms and treated as such.

5. That they shall be obliged to keep of and remain compliant with policy changes communicated by the TNO. The TNO will use its best efforts to assure that policies are made available in a timely manner with sufficient notice for implementation. Policy changes occasioned by incidents or that are required in shorter times by the circumstances will need to be accommodated.

5.4.2 Common obligations

The Ecosystem contract will also set forth the obligations related to operations as required by the TNA that are common across service providers in regards to at least the following topics :

1. Specification of manuals and/or standards to consult for detailed technical information relating to the operations within the Trust Network

2. Processes related to questions and issues regarding technical implementation or operation.

3. Processes related to information handling and secure deletion

4. Rules related to business processes

5. Rules related to the lifecycles of information within the TN

6. Processes related to providing correct and timely information to support discovery services. TAS3 relies on proper disclosure of policy and capacity to comply in informing discovery services which individuals rely on to choose service providers.

7. Processes related to providing periodic audit and other reports to the TNO

8. Process for creating Supplemental Notices of Privacy Practices

9. Processes related to potential proactive reviews and inspections including, but not limited to: prior notice, method of review, types of required documentation and personnel that may need to be available.

10. Processes related to complaints, incidents and investigations
    - 10.1 Need to support "no wrong door policy"
    - 10.2 Acceptance that these processes are also applicable to investigation of suspicious activity or complaints filed by other SPs or non- TAS3 parties
    - 10.3 Need for SP organizational process to support complaint handling and investigatory cooperation
    - 10.4 Record keeping and reporting requirements related to complaints
    - 10.5 Processes for reporting incidents or breaches of privacy or information security
    - 10.6 Processes for cooperation in investigation and remediation of complaints, incidents or breaches including:
    - 10.7 Identified points of contact at the SP and TNO
    - 10.8 Points of contact with outside investigatory agencies
    - 10.9 Incident/breach response plans
    - 10.10 Identifying needed team resources
    - 10.11 Identifying sequence of events
    - 10.12 Cooperation with technical and compliance staff
    - 10.13 Reporting/notification requirements to TNO, AOC and as required, other SPs, Trust Functions of the TN, individuals, and outside

authorities as appropriate under the response play or as required by law.

10.14 360 review[160] and post incident debrief plans

10.15 Explicit acceptance that the TNO will coordinate the internal investigation and will provide the aggrieved TN user with appropriate information requested to appropriately review what errors may have occurred and who may have been the proximate cause of those errors.

10.16 Recognition that where the aggrieved party may be another SP, the TNO will have greater discretion to evaluate the veracity and motive of the complaint, to assure that it does not arise from competing business interests as opposed to actual violation of TAS3 policies or requirements.

10.17 Explicit acceptance of cooperation, both directly and through the TNO and AOC where outside authorities, law enforcement or judicial proceedings are involved

11. Oversight and redress

12. Processes for disaster recovery and business continuity

13. Processes for timely adoption and formal acceptance of new processes or requirements related to the TN or TAS[3] standards.

14. Liability and Indemnification

14.1 The EC will require acceptance of liability allocations consistent with the TNO.

14.2 The EC will set forth enough information to provide a clear understanding of these obligations, including:

14.3 Type and scope of liability, including any limitations of liability

14.4 Insured/self-insured models

14.5 Financial cost contribution

14.6 Participation requirements in pooled liability guarantee, including how costs are allocated for initial contribution and further funding

14.7 Indemnification to other SPs/TN by SP that is demonstrated to be the proximate cause of the liability.

14.8 Possible liability implications (allocation formulas) of liability exceeding

14.9 Guarantee

14.20 Indemnification

14.21 Any further insurance

15. Conflicts of Interest:

15.1 TAS[3] may involve the participation of multiple providers who may have business relationships with each other, including competitive relationships.

[160] "360 review" refers to a comprehensive or 360 degree review considering an incident from all perspectives and impacts. Only a holistic process can provide a complete learning experience from an incident. The EC requirements only extends to TAS[3] related incidents, but all SPs would be well served t have such a process related to all incidents.

15.2 The EC shall specify detailed disclosure processes which will allow the existence or potential of conflicts , to be ascertained

15.3 To avoid potential conflicts EC will define processes of redaction and recusal that will isolate potential conflicted parties from information which might lead to compromise or access to information of a sensitive or confidential nature from a business/competitive view.

15.4 These requirements of recusal or redaction may be limited, depending on the nature of the specific situation, if the nature of the sensitive information is related to investigatory complaints and enforcement actions of TN, and of the potentially conflicted SP is involved on behalf of the TN in such process.

16.5 Any SP who is concerned with a potential conflict that they believe has not been sufficiently resolved may make a direct appeal to the TNO for reconsideration. If they remain unsatisfied they may ask the AOC for a further review. Both the TNO and AOC will keep the GB timely apprised of these requests for review and will have detailed documentation available related to the conflicts process.

16. Breach of Contract

16.1 Any material breach of the terms of the contract, for example:

a) Failure to follow processes related to complaints and investigations can be considered a material breach of the EC.

b) Provision or maintenance of incorrect information related to discovery services may be considered a material breach of the agreement.

c) Failure to provide complete and accurate information during the intake process as further specified in obligations of the Intake Process.

16.2 Notification requirements

16.3 Opportunity to cure

16.4 Potential heightened scrutiny or special conditions

16.5 Due process in decision making related to consequences of uncured breach finding

a) Rights of review and appeal to AOC and, in cases of termination, requiring GB approval by written procedure.

17. Termination: EC will set out termination rights and requirements

17.1 Conditions for voluntary termination of agreement on both sides

17.2 For cause termination

17.3 Actions resulting from termination

17.4 Privilege and credential termination

17.5 Public notices

17.6 Implications for stored information

17.7 Relationships with individuals and SPs

17.8 Special provisions for termination of Dashboard providers or other retaining large amounts of PII beyond the transaction

17.9 Requirements and processes for return or deletion of PII and sensitive PII
17.20 Processes related to audit information
17.21 Ability to maintain certain elements under strict security and access controls as required legally or as may be needed to support transactions that have ongoing obligations
17.22 Final accounting of information assets and financial obligations
17.23 Requirements and obligations that survive termination

18. Legal Compliance Requirements: EC will set forth terms related to provision of information to satisfy legal compliance obligations

18.1 Review of compliance request
18.2 Where permitted by law to be provided to TNO for response
18.3 Requirement that requests comply with legal form and due process requirements
18.4 Right to inform data subject or other TN participants subject to request where permitted by law so as to allow them to interpose defenses

19. Boiler Plate

19.1 Force majeure
19.2 Four corners
19.3 Severability
19.4 Contact information
19.5 Signatures

6 Participant Contracts

As has been highlighted in the preceding sections, TAS³ will create a cascading chain or responsibility. Through the TNA, the TNO is delegated the power of entering into an Ecosystem Contract, with the SPs, in which more detailed requirements related to operation and transactions are specified that are consistent with the rules, policies and obligations established in the TNO. Through this authorization (and EC specification), the TNO may also enter into Service provider contracts which supplement the EC at the transaction or the role level. For example, Dashboard Service Providers, which have such a central function in controlling and monitoring access to information across transactions, may be subject to additional requirements based on their role. Similarly, some transactions may relate highly sensitive information for which more restrictive controls may be required on the processing or sharing of information. The specific nature of these contracts will be further delineated in the next iteration of this document.

The structure of the contract has been considered and the current focus is on the creation of a master template – containing all the fixed terms of the contract with modular clauses that can be chosen from a library of clauses related to roles and types of transactions. This modular approach would help to limit the complexity of maintaining the contract ecosystem and tracking versions. We are also considering the potential of creating role based libraries of entire contracts where the same clauses have been used by a significant number of service providers.

The SP contract would optimally have a Meta data store of identified clauses so that users and practitioners can review whether those clauses have been updated in the clause repository and whether the SP contract needs to be updated. We foresee the technical automation of many of these contract creation functions to be useful topics of research for future projects.

7 Glossary

7.1 Actors

7.1.1 Trust Network

an end-to-end network of end-users, service providers, governance and administration bodies which operate under the rules and procedures established by and pursuant to a Trust Network Agreement

Also referred to as: the TAS³ Network

7.1.2 Trust Network Governance Board (GB)

entity which presides over the Trust Network and establishes the rules that will apply within the Trust Network

7.1.3 Trust Network Advisory Board (TNAB)

consultative committee comprised of stakeholders and external experts which issues recommendations towards the Governance Board

7.1.4 Trust Network Operator (TNO)

agent of the Governance Board charged with overseeing the implementation and enforcement of the rules of the Trust Network

7.1.5 TAS³ Accreditation Authority (AA)

entity charged with the intake and recognition of service providers that wish to offer services within the Trust Network

7.1.6 TAS³ Accountability & Oversight Committee (AOC)

entity responsible for the monitoring compliance of activities within the Network with the rules of the Trust Network

7.1.7 Identity provider

an entity that verifies, maintains, manages, and may create and assign identity information of other entities.[161]

7.1.8 Attribute Authority

entity that is functionally responsible for the collection, validation, updating and making available of information relating to other entities within a certain context[162]

[161] ITU-T SG 17, x.1252 Baseline identity management terms and definitions, available at http://www.itu.int/rec/T-REC-X.1252-201004-I/en.

7.1.9 Trust Network Infrastructure Service Provider (TNISP)

entity offering one or more services critical to operational functioning of the Trust Network

7.1.10 Application-specific service provider

entity which offers services towards end-users of TAS³

Also referred to as: 'TAS³ participant' or 'recognized TAS³ service provider'

7.2 Legal instruments

7.2.1 TAS³ Contractual Framework

combination of legal instruments which ensure appropriate binding of TAS³ participants

It consists of:

- the Trust Network Agreement;
- the TAS³ Ecosystem Contract;
- TAS³ Participant Contracts; and
- TAS³ End-User and Licensing Agreements.

NOTE: the TAS³ contractual framework is supplemented by the TAS³ policy framework.

7.2.2 TAS³ Policy Framework

combination of organizational and technical policies which govern the operations carried out within the Trust Network, as well as those policies which need to be implemented by TAS³ participants within their own organizations

NOTE: all TAS³ participants are bound to adhere to the TAS³ policy framework by virtue of the TAS³ Ecosystem contract and TAS³ participant contracts.

7.2.3 Trust Network Agreement

agreement through which the founding members establish a Trust Network and its organizational structure

---

[162] Based on X. Huysmans and B. Van Alsenoy (eds.), 'D1.3 Conceptual Framework – Annex I. Glossary of Terms', v1.07, report for the IBBT project IDEM, 17 December 2007, available at https://projects.ibbt.be/idem/uploads/media/2007-12-27.idem.glossary.v1.07.pdf, p. 9 (definition of authentic source).

7.2.4 TAS³ Ecosystem Contract

agreement between the Trust Network Operator and every entity offering services within the Trust Network that binds the service providers to the rules and policies that apply within the Trust Network

Also referred to as: 'TAS³ Framework Agreement'

NOTE 1: the Ecosystem contract provides for the baseline of obligations among TAS³ participants. It is completed in counterpart forms through the TAS³ Participant Contracts which are tailored to the role of each service provider.

NOTE 2: the TAS³ Ecosystem contract is drafted pursuant to and must be consistent with the Trust Network agreement

NOTE 3: the TAS³ Ecosystem contract shall contain third-party beneficiary clauses that will end-users to seek enforcement against service providers of their obligations under this contract

7.2.5 TAS³ Participant Contract

contract which details the specific obligations of a service provider in light of its role within the Trust Network and transactions it is likely to engage in

NOTE: a TAS³ Participant Contract acts as a role-based addendum to the TAS³ Ecosystem contract.

7.2.6 TAS³ End-user and Licensing Agreement (EULA)

contract between an end-user and the Trust Network Operator which outline the rights and obligations of the end-user as well as the warranties and disclaimers made by the TNO with regards to operations that take place within the Trust Network

NOTE: the TAS³ EULA enumerates those rights and obligations which remain consistent across TAS³ service providers and shall be supplemented by additional terms which govern transactions of the end-user with participating service providers

7.2.7 TAS³ Notice of Privacy Practices (NPP)

document which sets forth the privacy practices of the Trust Network including: types of information collected, purposes of collection, uses, access rights

NOTE 1: While the primary purpose of the NPP is to inform potential end-users of the privacy practices that apply within the Trust Network, it also serves to articulate the minimum practices that service providers must adopt (or at least have policies and practices consistent with its terms)

NOTE 2: where service providers need to provide additional notice or information related to their processing or specific transactions, such notice will be made available in a Supplemental Notice of Privacy Practices.

8 Annexes

8.1 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

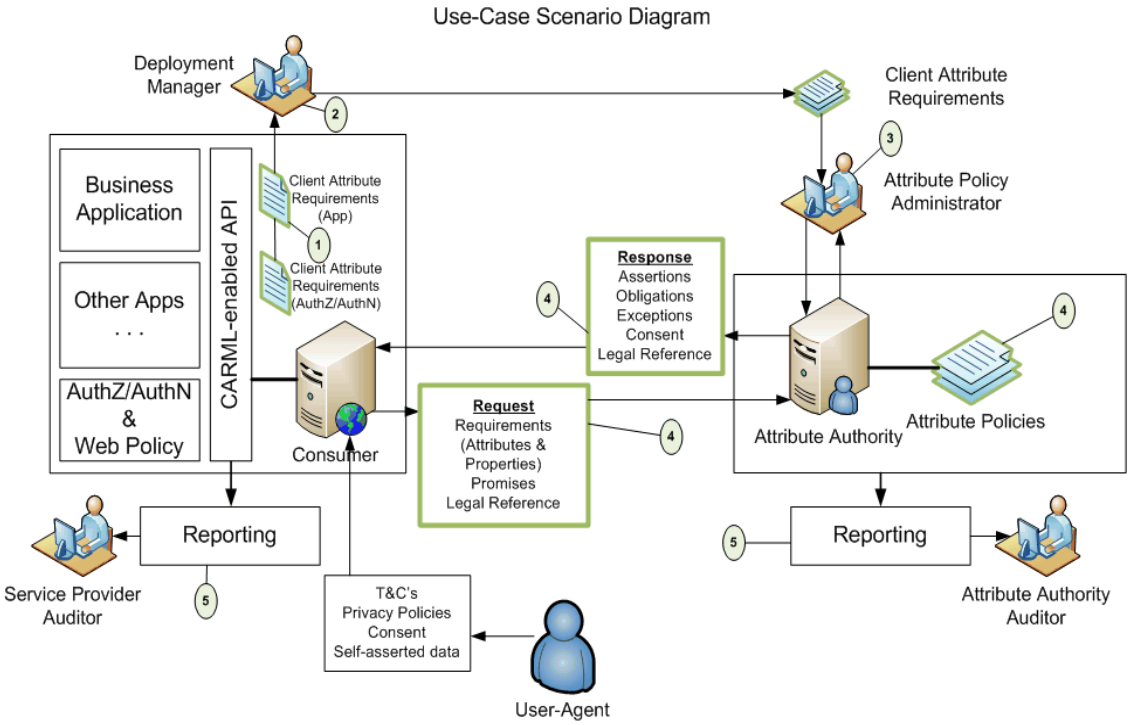
Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

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

8.2 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

8.3 Annex III - Definitions

Article 2 Definitions (Directive 95/46/EC)[163]

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;

[163] 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

8.4 Annex IV – WP 6 Requirements list

The following requirements have been developed from the legal and contractual framework set forth D6.1 and D6.2. During the third year of the projects, these requirements have been refined in light of the requirements interaction analysis performed for D1.2.

The current list is still not exhaustive and will continue to be updated. 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.

As to the vocabulary used in the expression of these requirements, we would like to note the following. The term 'MUST' is used to express that there is a direct legal obligation (emanating either from the EU Data Protection Directive 95/46/EC, national implementations or contract law) to comply with this requirement. The term 'SHOULD' is used to indicate that the articulated requirement does not reflect a clear and direct legal obligation, but rather is reflective of a 'best practice' which may enhance (but also facilitate) compliance. The term 'SHALL' is used where the articulated requirement is again not a clear and direct legal requirement, but will nevertheless need to be implemented in order to achieve the objectives of the TAS³.

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 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 (EDITED): Binding Effect of technical processes & policies. All TAS³ participants and users MUST agree to be bound by the technical processes within the TAS³ network, including the obligations resulting from the transactions they engage in or choices they exercise through the TAS³ architecture.
  - Req 6.5.1 (EDITED): All TAS³ participants and users MUST agree to accept the contents of TAS³ logs as evidence of their actions within the TAS³ network (to the extent the relevant logging mechanisms are working properly and their properties have been appropriately disclosed and consented to).
  - Req: 6.5.1: 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 6.5.2: It MUST be ensured that commitment to communicated policies and privacy preferences cannot be repudiated at a later time;
  - Req 6.5.3: 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 6.5.4: Policy information MUST be easily accessible to all relevant parties;
  - Req 6.5.5 Policies MUST be drafted and communicated in a way that is appropriately tailored to and accessible by its intended audience[164], so as to enable all relevant parties to understand their scope of application and which resources (data, services etc.) are governed by which policies[165];

[164] 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

[165] 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

- Req 6.6 (EDITED): Implementation of Required Policies. Organizations participating in the TAS³ network SHALL be bound to implement TAS³ defined or compatible policies (e.g. internal privacy and security policies) or as approved during the intake process.

- Req 6.7: 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 6.8: Allocation of roles and responsibilities: Responsible entities and roles SHALL be defined for at least the following tasks:
    - receiving and registering consent;
    - providing notice and transparency;
    - performing the appropriate authentications, authorizations and checks for every processing operation;
    - the maintenance of logs for the different processing operations that take place;
    - 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.

- Req 6.9 (NEW): Separation of duties: roles and responsibilities relating to the management of the TAS³ network, in particular those relating to policy enforcement, audit and oversight SHOULD be allocated in a way which limits the risk of conflict of interests.

3. Legitimacy of processing

- Req 6.10: Collection, use, and subsequent use, of personal data 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[166], and unambiguous[167].

---

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

[166] A consent may be considered informed when it satisfies all the elements listed in Req 6.50.

[167] From a technical point of view, this requires that the user "opts in" to the processing of personal data.

- 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 evidentiairy 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.[168]

- Req 6.13: The TAS³ network SHALL 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)

- Req 6.15 (NEW): Consent revocation and modification of privacy preferences: a mechanism or procedure MUST be specified which ensures that in instances in which the data subject either revokes her consent or modifies her privacy preferences, no further processing operations shall be carried out for which the legitimacy is no longer ensured.

4. Finality

- Req 6.16: 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 6.17 (EDITED): Consent Capture for New or Changed Use: If an entity wishes to process personal data in a manner which cannot objectively be considered as compatible with the originally specified purpose(s), a new informed consent MUST obtained from the data subject prior to this new or changed use, unless this processing is explicitly required or permitted by law.[169]

- Req 6.18: 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.

[168] See articles 7-8 of the Data Protection Directive.
[169]

- Req 6.19: 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.

    - Req 6.19.1: Such data handling policies MUST be compatible with the TAS³ governance framework;

    - Req 6.19.2: The data recipient MUST be legally bound to restrict itself to authorized usage and to execute the obligations specified in these data handling policies (see also Reqs 6.5);

    - Req 6.19.3: The data subject SHALL 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 6.20: Technical policy enforcement mechanisms SHALL be able to take into account the specified purpose when evaluating a processing request when appropriate. See also Req 6.21.

- Req 6.21: In order to enable verification that there has been a legitimate basis for processing, there SHALL be appropriate logging of asserted purposes and the ability to audit how the information was used against the purpose for which it was collected.

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

5. Data minimization

- Req 6.22: The collection and further processing of personal data MUST be relevant and non-excessive in relation to the specified purposes (see Req 6.16).

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

- Req 6.23: 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.

- Req 6.24 (EDITED): Response to attribute requests and granular access control: Technical policy enforcement mechanisms MUST have the ability to respond to data requests with only that information that the requesting entity needs to receive (sufficient level of granularity). See also Req 6.40.

- Req 6.25: 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 6.25.1: Mechanisms SHALL be in place to enable the user to choose which identity providers and/or attribute authorities shall be used for a particular service, subject to applicable policy (e.g. minimum level of assurance, prerequisite attributes for authorization decision etc.).

- Req 6.26: 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 6.26.1: 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 SHALL be done as part of the service/process definition.

    - Req 6.26.2: 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 6.26.3: The TAS³ network SHALL 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).

- Req 6.27 (NEW): Data minimization : appropriate measures MUST be in place to avoid unnecessary duplication of personal data in multiple repositories.

6. Data accuracy

- Req 6.28: 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 6.29.: 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 6.29.1: Where appropriate, review and update procedures MUST be in place for personal data which is being kept for an extended period of time.
- Req 6.30: Procedures MUST be in place on how to report and deal with suspected inaccuracies.
    - Req 6.30.1: Data subjects MUST have the ability to check the accuracy and quality of the data, and to report suspected inaccuracies. (see Reqs 6.58 et seq.);
    - Req 6.30.2 (EDITED): In the event of indirect collection, the accuracy of the data SHOULD be verified with the data subject where this is both possible and appropriate;
    - Req 6.30.3: 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 6.65)
- Req 6.31: 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 6.31.1: Indication of level of confidence: each element of personal data SHOULD have 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 6.32: The integrity of data maintained in authoritative sources MUST be appropriately guaranteed.
    - Req 6.32.1: Modification rights MUST be restricted to authorized entities on a 'need-to-modify' basis.
- Req 6.33: Data to and from authoritative sources MUST be authenticated through use of data origin authentication protocols to ensure authenticity and integrity where appropriate.
- Req 6.34: Relying Parties and other data recipients SHALL 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 6.34.1: Policies SHALL be in place which specify how a 'sufficient level of certainty' as to the origin and integrity of personal information is established.

- Req 6.35 (NEW): Unambiguous identification: TAS³ participants MUST ensure unambiguous identification of the data subjects with whose data they process.

  Note: This requirement does not entail that data subjects must be consistently identified in the same manner across service providers. See also Req 6.44.

7. Confidentiality and security of processing

- Req 6.36: Confidentiality. Appropriate organizational and technical security measures MUST be in place to ensure the confidentiality of personal data.

- Req 6.37: Security. Appropriate technical and organizational measures MUST be in place to protect against unauthorized/unlawful/accidental access; modification, disclosure, destruction, loss or damage to personal data.

- Req 6.38: An organizational framework for information security management (describing both organizational and technical measures) MUST be in place.

- Req 6.39: 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 6.39.1: Identities and credentials MUST be managed in way that they continuously provide a level of assurance proportionate to the interests at stake;

    - Req 6.39.2: Common authentication approaches and rules MUST be defined and enforced;

    - Req 6.39.3: 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 6.39.4: 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 6.39.5: Adequate measures and procedures MUST be in place to properly address instances in which the levels of assurance associated with a particular identity or credential has been compromised (e.g. identity theft), or there is a reasonable likelihood thereto. Such

measures might include credential revocation, notification to trust & reputation engines, etc.

- Req 6.40: 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 (see also Req 6.24):

    - Req 6.40.1: A list and directory of resources (e.g. applications, data) and categories of potential users/data recipients MUST be made.

    - Req 6.40.2: Personal data contained in data repositories SHALL be categorized according to a classification system that recognizes type and sensitivity of data.

    - Req 6.40.3: Roles and privileges of each entity MUST be defined based on legitimate organizational needs (in other words, on a "need-to-process" basis).

    - Req 6.40.4: 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 6.40.5: Acceptable purposes for access to data categories MUST be defined, emergency procedures for access beyond those purposes SHALL also be defined (break-the-glass).

    - Req 6.40.6: 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 time period.

    - Req 6.40.7: Adequate measures and procedures MUST be in place to properly address security breaches, including notification of relevant entities (e.g. audit & oversight committee)

- Req 6.41 (NEW): Delegation authorization policy: prior to allowing a delegation of privileges to take place, it MUST be verified that the delegator is in fact authorized to delegate those privileges (and to the envisaged delegate).

- Req 6.42: 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 6.43 (NEW): Mutual authentication: appropriate safeguards must be implemented to ensure that users are not misled into providing personal data to an unauthorized entity.

- Req 6.44: Avoid unnecessary linkability. TAS³ SHALL support advanced pseudonym management to limit the level of linkability or correlation among personal data to that which is necessary..

- Req 6.45 (NEW): Availability: the TAS³ technical authorization infrastructure MUST ensure that legitimate persons shall have ready to access personal data, particularly in emergency situations (e.g., when it is necessary to safeguard the vital interests of the data subject).
    - Req 6.45.1 (NEW): Where a user decides to override the ordinary authorization process under the pretext of an emergency, appropriate notifications and follow-up procedures to deter abuse must be executed.

- Req 6.46: Physical access restriction: Physical access to terminals and other resources MUST be restricted where appropriate.

- Req 6.47: Each participant MUST adopt internal privacy policies documenting security measures (specifying inter alia the persons responsible within the organization (e.g., security officers), what to do in the event of a security breach etc.).[170]

- Req 6.48: 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.[171] 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 6.49: 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.[172]

8.1 *Direct collection*

[170] Such policies must of course be compatible with the TAS³ governance framework.
[171] 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.
[172] The data subject MUST in principle be notified of the elements listed in Req 6.49 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).

- Req 6.50: Notice requirements where data is collected from data subject herself (direct collection):

    - Req 6.50.1: 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 6.50.2: The data subject SHOULD also be informed of:
        - 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 6.50.3: 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 6.51: Notice requirements where data is not obtained directly from data subject herself (indirect collection):

    - Req 6.51.1: 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 6.51.2: 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 6.51.3: 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 6.51.1-3 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 6.52: All the information elements listed in Reqs 6.44-6.45 SHALL 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 6.53: Layered approach. In order to limit complexity, the fulfilment of Reqs 6.51-6.52 need not necessarily take the form of a single document.[173] TAS³ SHALL adopt a 'layered' approach for notice when appropriate.
  - Req 6.53.1: This approach SHALL NOT contain more than three layers of information (short – condensed – full)
  - Req 6.53.2: The sum total of these layered notices MUST meet the notice requirements imposed by the applicable national legislation.
  - Req 6.53.3: It MUST be easy to ascertain which data processing operations are governed by which policies.

- Req 6.54: 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 portal provider itself, but SHALL also include a general notice with regard to the operations of entities participating to the TAS³ network as service providers.
  - Req 6.54.1: In addition to the elements in Reqs 6.44-6.45, this notice SHALL also contain a point of contact for questions and information and redress mechanisms

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

- Req 6.54.2: This general privacy policy SHOULD reference and link the privacy policies maintained by TAS³ participants (see Req 6.55) when appropriate.

- Req 6.55: 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 6.55.1: In addition to the elements in Reqs 6.44-6.45, this notice SHALL also contain a point of contact for questions and information on redress mechanisms
  - Req 6.55.2: These privacy policies SHOULD also cross-reference the TAS³ infrastructure privacy policy where appropriate.

- Req 6.56: Consent to notices. The consent of the data subject MUST (as a rule[174]) 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 6.56.1: 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 6.57: 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, EXCEPT where the processing is mandated by a legal obligation (see also Req 6.17).[175]

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

- Req 6.58: 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.

- Req 6.59: 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.

---

[174] 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 6.49 et seq.)

[175] Req 6.57 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 6.54-55.

9.1 *Right of access*

- Req 6.60: Upon request, the data subject MUST be provided with confirmation, as to whether or not data relating to her 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 recipients 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.
- Req 6.61: 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 6.62: Data subject requests to rectify, block or erase data MUST be accommodated at all times EXCEPT where an overriding legitimate interest exists.
    - Req 6.62.1: Such overriding interest SHOULD be specified in the TAS³ privacy policy notice(s).
    - Req 6.62.2: 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 6.62.3: In case of denial, the reason for denial MUST be communicated to the data subject.
- Req 6.63: 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 6.64 (EDITED): A procedure SHOULD be in place to adequately deal with the situation whereby a TAS³ actor receives a data subject request which is not competent to decide itself.

9.3 *Notification to third parties*

- Req 6.65: 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 6.66: The TAS³ user interface ('dashboard') SHALL make all the information listed in Reqs 6.53 readily available to data subjects in a user-friendly way.

- Req 6.67: 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 6.68: 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 6.69: 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*[176]

- Req 6.70: Processing operations involving personal data MUST be logged with a sufficient level of detail.

- Req 6.71: 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 6.71.1: Log files MUST detail which entity performed which action upon which resource, and at what time;

    - Req 6.71.2: Where appropriate, log files SHALL also record for which purpose (under which pretext the action took place/was authorized);

    - Req 6.71.3: Log files MUST contain explicit information as to the recipients to whom personal data has been transferred.

[176] 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.

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

- Req 6.72: Reliability: Appropriate measures MUST in place to ensure the authenticity, accuracy, integrity and completeness of the logs.

- Req 6.73: Transparency. The fact that processing operations are logged MUST be transparent towards users through appropriate notification (see Reqs 6.49 et seq).

- Req 6.74: Proportionality: Logging MUST organized in a proportionate manner (e.g. storage in a pseudonymized or de-identified format, separation of duties).

- Req 6.75: Confidentiality: Appropriate measures MUST be in place to ensure the confidentiality of the logs. See also Req 6.36 et seq.

    - Req 6.75.1: Privileges to access nominative log information SHOULD in principle only authorize selective access (no 'free search');

    - Req 6.75.2: 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 6.76: The proper implementation and functioning of all technical mechanisms and organisational measures MUST be documented and audited on a regular basis.

- Req 6.77: Definition of roles & responsibilities (see Req 6.8) MUST also include assignment of tasks with regards to audit and oversight.

- Req 6.78: 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 6.79: 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 6.80: Technical non-repudiation mechanisms MUST be supported when appropriate. For example:

    - Req 6.80.1: When forwarding personal data, it SHALL be ensured that the sender is not able to later deny having forwarded it;

- Req 6.80.2: It SHALL be ensured that the commitment to communicated policies and privacy preferences cannot later be repudiated at a later time.

- Req 6.81: Automated notifications SHALL be instituted for extraordinary processing operations (e.g. break-the-glass), and procedures SHALL be in place to further follow up such notifications (e.g. through audit & oversight committee).

  - Req 6.81.1: Automated notifications SHOULD also be considered for certain types of processing operations (e.g. access to particularly sensitive data)

- Req 6.82: 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 6.83 (NEW): Outsourcing/delegation of responsibilities of TAS³ participants: TAS³ participants MUST be bound to outsource or delegate only those tasks for which outsourcing or delegation is permitted.
  - Req 6.83.1 (NEW): Where a TAS³ participant decides to outsource/delegate a task which involves the processing of personal data, this entity must choose a processor providing sufficient guarantees in terms of technical security measures and organizational measures.
  - Req 6.83.2 (NEW): Any TAS³ participant outsourcing/delegating a task which involves the processing of personal data must ensure that the processing is governed by a contract or legal act binding the processor to the controller which stipulates:
    - that the processor shall act only on instructions from the controller;
    - that the processor is subject to the confidentiality and security obligations set forth by Directive 95/46/EC.
  - Req 6.83.3 (NEW): processors and other recipients MUST be bound to 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.

9.4 *Complaint handling*

- Req 6.84: Complaint capture system: Potential abuses to the system or concerns of either users or organizations MUST be captured.

  - Req 6.84.1: 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 6.84.2: Appropriate levels of proof are required to justify the consequences listed in Req 6.84.1 and complaints should therefore be corroborated on the basis of logs and other relevant documentation

- Req 6.85: Redress/oversight Processes: Once a complaint is captured, redress MUST be possible. In addition, an oversight process SHALL be in place which SHOULD also be involved in pro-active detection of non-compliance.

- Req 6.86 (NEW): Use of feedback information: Users SHALL have the ability to specify how the feedback they provide with regards to service providers and service experiences may be used (e.g. only for the purpose of calculating reputations)
  - Req 6.86.1 (NEW): The operator of the Trust Reputation server MUST be bound to only process user feedback information in accordance with the user's policies.

11. Notification & prior checking

- Req 6.87: 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

8.5 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.

8.5.1 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[177] 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).

8.5.2 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 identities, and the correlations between them. Additionally, the TAS³ approach

[177] 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.

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.

8.5.3 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 feed-back), 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.

8.5.4 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)

8.6 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.

Note: the current questionnaire has been developed by APEC as part of the implementation of the APEC privacy framework further iterations of this questionnaire will be tailored to TAS³

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 TAS³ 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 TAS³ 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.

8.7 Annex VII – IT Security requirements checklist

This document is a compendium of best practice requirements related to security for the general operations[178] of TAS[3] service providers.[179] We are using a combination questionnaire and requirements checklist to give service providers a number of options in how the demonstrate their capacity to comply with security requirements. Where prospective service providers are confident that they already have compliant polices, they can just provide copies of the policies/documents with a short description of how they comply with requirements.

To the extent that some are concerned of confidential or trade secret information in the disclosure, they are welcome to use the option of describing the relevant practices/controls or providing redacted polices. It should be noted, however, that failure to provide appropriate proof related to demonstrating a capacity to comply with security requirements may impact both reputations scores and trusted assurance levels.

Finally, because of the variety of roles related to service providers there is a distinct possibility that you may organize security and related policies in a different manner. If so please explain how you meet the requirements and why your organizational approach is equivalent or equally demonstrates compliance with the requirement(s) in question.

Service Provider contact information :

Name:

_____

Phone/E-mail:

_____

[178] Source: http://www.interpol.int/public/technologycrime/crimeprev/companychecklist.asp

[179] Note that there is a separate document that is used to evaluate the capacity of service providers to meet TAS[3] technical requirements. While we understand there is overlap between the documents, we wish to keep them separate because there is much less accommodation we can provide in how the technical requirements are met.

1. Management responsibilities

No	Question	Requirement	Documents Controls
1	Is there an information security policy and has it been written and/or approved by management?	You are required to have a security policy endorsed by management that addresses the requirements outlined in the questions that follow.	
2	Is there a process for reviewing and keeping the policy up-to-date.?	Provide a description of the process you use.	
3	Do you have a risk analysis process and was the security policy based on the outcomes of the risk analysis	Proper risk analysis from assessment to mitigation to identification of acceptable risk needs to be an organizational priority. Provide a description of the risk analysis process you use and the relevant findings that informed the security policy	
4	What is the role of management in reviewing or overseeing the development of: A security plan that defines security targets and how they will be realized? And A high-level security architecture that identifies technical security functions and the organizational needs to fulfill those functions	You should have management driven documents related to the organization's security strategy. Describe the security plan and architecture as well as Management's role in development, oversight or approval. Provide copies of relevant documents.	
5	Is there an Internet use and access policy?	You must have appropriate controls on Internet access and use. Describe the controls you have place on your employees and others that may be connected to your network on access to and use of resources.	
6	Is the organization for Information Security defined in the policy document and are there clearly identified contact persons and	In order for security to be effective there must be defined contact points, lines of organizational responsibility and appropriate	

	processes?	procedures. Identify the responsible parties and describe how they are organized and supported.	
7	Is there an Information Security training plan?	Updated training of all staff related to security is required on a periodic basis. Specialized training may be required for those people who directly handle or manipulate large quantities of data or more sensitive data. Please describe the training available for your staff.	

2. Organization and Operation

No	Question	Requirement	Documents Controls
7	Does an Information Security handbook exist? Has it been approved by the management?	Describe or provide copies of the handbook. Where practical and appropriate, it is useful to provide an externalizable version of your security practices written at a level appropriate to providing customers some assurance as to the credibility of your practices.	
4	Who is responsible for overseeing authentication and authorization? What controls do you have in place?	You need to have appropriate controls related to authentication of identity and authorization of privileges. Provide you policy or describe your controls that assure that access to data is appropriately limited and that privileges are limited to the up-to-date roles of current employees, agents	

[180] While we do not suggest providing access to networks and systems to those not formally employed by the company we include this question to assure that all persons who might access data are considered.

		or contractors.[180]	
5	Is there a defined group responsible for contingency planning and handling?	Contingency planning needs to be properly defined and supported. Identify the strategic team and describe the plan and implementation strategy.	
6	Is there an incident response team and plan?	There needs to be an incident response plan and a trained incident response team with clearly defined responsibilities. Implementation of the plan needs to be trained on and periodically reviewed. Coordination with other service providers and the Governance board of TAS[3] is also needed.	

3. Personnel (Employees)

No	Question	Requirement	Documents Controls
		All	
1	Are employees checked for References, education, etc within the bounds permitted by law?	There should be appropriate checks and controls on employees that have access to sensitive or confidential information.	
2	Are employees bond to uphold confidentiality agreements and policies?	Are employees required to sign confidentiality agreements and acknowledge the need to comply with security policies?	
3	Is staff informed on the consequences of breaking the security regulations?	There must be oversight of policy compliance and consequences for non-compliance.	
4	Are there established exit procedures for employees when they leave?	Personal information of employees and customers must be appropriately secured when employees	

		leave the organization. This includes securing information that may have been accessed by the employee and requires a timely termination of access credentials.	
Systems Administration Personnel			
5	Are systems administration personnel informed of specific security regulations for Developers, Network Administrators, including the need to respect both data minimization and least means access?	A 'root'-privilege does not imply authority to access all data/information. Appropriate controls and policies need to be in place to assure that only the proper information is accessed. Separation of duties and appropriate audit controls should also be implemented as appropriate.	

4. Third Parties and Outsourcing

No	Question	Requirement	Documents Controls
1	Are there written contracts with Third Party companies[181]? And do the personnel understand their responsibilities	There should be contracts with third parties that may have access to premises or equipment and thus personal information to assure that they can comply with applicable sections of your policies. There should also be assurance that Third party personnel understand the obligations through training or signing agreements.	
2	Are there any routines for end of assignments?	There should be controls and processes related to completion of assignment to assure that no information is compromised and any	

[181] Consultants, Service engineers and other service staff (guard, caretaker, cleaning service etc.)

		temporary access granted is terminated.	
3	Do you outsource any of your functions to Third Parties?	There needs to be contractual requirements on third party outsources assuring that your organization's security requirements are maintained. Provide a list of functions that are outsourced, the companies they are outsourced to and the way in which you assure that your security requirements can be honored.	

5. Software

No	Question	Requirement	Documents controls
1	Are there any instructions for bringing outside software/data into the organization? Is a security validation approval done before introducing new software?	There should be policies and procedures for determining which software should be introduced into the system to help limit the introduction of spyware and malware.	
2	Are security-related patches from developers and/or vendors implemented as soon as possible?	There need to be appropriate policies for patch management and software update.	
3	Are security options and configurations properly implemented?	All necessary steps should be taken and procedures used to properly configure and implement software security including the appropriate revision of default parameters.	
4	Do you have appropriate virus protection and intrusion prevention/detection software and are they kept patched and up to date?	There needs to be an appropriate use of virus protection and intrusion prevention/detection software at the enterprise and desk/lap top level.	

	Are employees made aware of the importance of maintaining and running the software on their machines?	There need to be internal processes and defined responsibilities to periodically run, patch and maintain such software.	
5	Do you appropriately test the security of your system?	There should be organizational requirements and processes related to the testing of systems and environments. System tools that are used in such tests should be appropriately secured with limited access.	

7. Hardware

No	Question	Requirement	Documents Controls
1	Is there any guidance related to required security features or types of hardware that can be introduced into the system?	Organizations should have policies to assure that only appropriately configured and secured hardware is introduced into the system.	
2	Are there instructions on how to discard equipment?	Organizations must have policies related to completely wiping data (files as well as fragments) off hardware that is being retired, transferred, sold, donated or discarded	
3	Are there policies related to the use of equipment and who may access it for what reasons?	There need to be polices that control the use and access to hardware. While incidental uses of the hardware for personal use may be permitted, those uses should be limited to the employee and the use still needs to comply with all aspects of corporate policy.	
4	Are there clear lines of responsibility for maintaining the security of hardware?	There should be a clear delineation of who is responsible for the maintenance of security of hardware, including which responsibilities are centralized and which distributed as well as who has responsibility for	

		remediation of security issues.	

8. Documentation

No	Question	Requirement	Documents Controls
1	Are the policies related to security properly documented and kept up to date? Are they made available, as appropriate, to the employees directly or in the form of a security handbook?	Security policies need to be appropriately documented, maintained and distributed or made accessible to employees is a usable manner.	
2	Are there any written rules defining responsibility and authority for each staff category?	While security polices are applicable across the company, each person should be aware of their role in properly maintaining organizational security.	

9. Computer media

No	Question	Requirement	Documents Controls
1	Are there polices related to the use of computer media	There need to be policies related to computer media which could either be used to improperly remove information or introduce malware from the system. Requirements for Labeling and inventory of such media when in use should be included.	
2	Are there		
8	Are there policies for handling media during service, including destroying media or reformatting media at the end of a particular use?	Polices that prevent media from being unattended, restricted it to a specific facility or that require encryption are examples of best practices that should be considered depending on the nature and	

		sensitivity of the information and use of the media. There need to be secure erasure polices related to computer media.	

10. Identification and Authorization

No	Question	Requirement	Document Control
	Identification/Authorization		
1	Is there an Identification/Authorization system that controls both users and resources? Does the system support two factor authentication?	Organizations need to have appropriate systems that identify and authenticate users and authorize them to have appropriate access and privileges. Organization systems should support two factor authentications, especially if sensitive information is phonetically accessed through the system.	
2	Does the system include logging and alarm functions?	Logging and alarm functions are desirable elements of systems as they help in oversight and investigation.	
3	Is there an organization to administer the Identification/Authorization system?	There needs to be an established responsibility for the administration of the Identification/Authorization system. Attention should be paid to the separation of duties in this instance to assure that access controls are not thwarted by the operational IT and processing groups.	
4	Does the system include access control to resources/objects?	It is essential for there to be appropriate access controls to both resources and objects. Again separation of duties should be considered in assigning responsibility for policy development and oversight.	
5	Is there a password policy?	There needs t be a policy requiring minimum password	

		length and complexity (for example 8 digits, alpha numeric with mixed case and symbols) that are periodically updated. There should also be limits on the reuse of passwords and prohibitions on passwords being the user name or linked to easily linkable information. There need to be requirements to never send a username password combination in the clear.	
6	How is the password policy enforced?	Lockouts should be enforced if passwords are not timely changed or are insufficient. Controls need to be in place to prevent users from expanding their own privileges.	

11. System Security

No	Question	Requirement	Documents Controls
1	Is there a routine to ensure the correct date and time in all systems and are they synchronized?	System time parameters (date, time synchronization) are be important to audit and other controls and there needs to be defined responsibility for maintaining their accuracy.	
2	Are there enhanced logging facilities in critical systems?	Enhanced logging of access and state changes for critical systems and sensitive information is a requirement that needs to be articulated in policy with a designated responsibility of implementation and maintenance.	

12. Communication

No	Question	Requirement	Documents

			Controls
	Internal		
1	Are there documented procedures for changes to the network configuration or connection?	There need to be documented policies and defined responsibilities related to administration of and changes to the Network. There also needs to be a requirement to document changes t network and configuration.	
	External		
2	Is there a firewall and are communication ports properly protected	A firewall needs to be in place, maintained and properly administered. Communication ports also need to be properly configured and protected as needed for the services provided.	
3	Is the use of encryption considered?	Encryption is moving from a suggested best practice to a requirement both for information at rest and in transit. The organization must have guidelines related to when encryption is required and when it is permitted or prohibited.	
What Safeguards (including encryption when needed) were considered regarding:			
12	- E-mail, Telnet. FTP, PPP, EDI, SNMP, DNS Services, Routing web sessions, Javascript, Active X, cookies, VPNs	Appropriate controls across these technologies are required, but the level of overhead may be predicated on the nature of the information and the level of assurance in question.	

13. Logging

No	Question	Requirement	Documents Controls
1	Is the logging system documented and is the default condition to log?	Logging systems provide required information for audit, investigation and reconstruction of transactions.	

		Logging should be sufficiently detailed for each of the purposed and appropriately enabled. Interruptions in logging should be noted as potential indicia of compromise or suspicious behavior.	
2	Are the log files protected against unauthorized access?	Log files must be protected against unamortized access or alteration to maintain log integrity.	
The following evens should be logged:			
4	- Login		
5	- Logout		
6	- Failed login		
7	- Exceptional behavior	User not acting normally. Might be sorted out via an IDS	
8	- Access violation	Unauthorized access to resources	
9	- Activities in the Identification and Authorization system?	New users, change of privileges, remove of users etc	
10	- Setting of date and time		
11	- Introduction/removal of new hardware		
12	- Introduction/removal of new software		
13	- Introduction/removal of files		
14	Are the log-files archived in a proper way?		

14. Back-up

No	Question	Comment	Yes / No
1	Is there a policy related to backing up information?	Backups are periodically required and need to be appropriately archived. The related policies and defined responsibilities should be articulated in a back u policy, which should also address the conditions for	

		storage of backups.	

15. Physical Protection

No	Question	Comment	Yes / No
1	Are there policies related to physical security?	Physical access controls need to be in place to assure that access is controlled to facilities in general as well as computers and network components. This may be accomplished through restricted access zones as well admission control systems. Physical access controls, are of course only as effective as the personnel authorized access lists are accurate.	

8.8 Annex VIII – TAS³ EULA

DRAFT TAS³ INDIVIDUAL END-USER AND LICENSING AGREEMENT

Between: end-users of TAS³ ("you") and TAS³ Trust Network Operator [XYZ[182]] ("us" or "we")
Date: xx/xx/xx
Version: v1.1

Preamble

The TAS³ Trust Network is a network of service providers that have committed themselves to advancing user privacy and trust. Each recognized TAS³ service provider has agreed to provide end-users of TAS³ services with more control over their personal information, as well as more transparency with regards to the uses of their personal information.

In order for you to benefit from these commitments, you must first register with the TAS³ Trust Network as an individual end-user. Your agreement to these terms and conditions listed in this document is the first step in this registration process. This document periodically cross-references other documents, such as Our Notice of Privacy Practices or our user manual. These documents may help inform you of the features and options you will have in relation to TAS³ services. They will also inform you of important organizational policies of the TAS³ Trust Network. These documents should be consulted prior to making a decision about joining the TAS³ Trust Network.

1. Scope

The following sections describe the terms and conditions under which **TAS³ services** [*glossary link*] are provided. The purpose of this document is to outline our respective obligations and rights in relation to these services. These terms will govern our legal relationship should you decide to sign up to the TAS³ Trust Network as an individual end-user.[183]

---

[182] We do not expect that in practice there would be just one well-defined TAS³ Trust Network; but rather one or more TAS³-enabled networks. Hence the EULA would be between the end-user and the legal entity that acts as "operator" or "administrator" of a particular TAS³ enabled network. In practice the "us" would read "XYZ, a TAS³ enabled network operator". As this draft EULA is intended to be a benchmark, we have chosen, for purposes of simplification, to refer to "the" TAS³ Trust Network Operator and "the" TAS³ Trust Network.

[183] This End-User and Licensing Agreement (EULA) is to be provided to any individual natural person that joins TAS³ by creating an account at a TAS³-recognized Dashboard Provider. It is aimed at data subjects, not at service providers participating in the TAS³

Any transaction with a recognized TAS³ service provider will be governed by the terms which are specific to each service. These terms may specify additional rights and obligations which shall apply in your direct relationship towards this service providers, but they shall not abridge any of your rights and obligations set forth in this document.

2. Privacy and transparency

Our **Notice of Privacy Practices** [*link*] provides you with an overview of the different types of information that are collected and processed in order to provide you with the basic TAS³ experience.

This Notice of Privacy Practices identifies several types of processing which may not be readily apparent. For example, the enforcement of your privacy preferences requires the capturing, storage, and communication of these preferences. While your privacy preferences themselves will be clearly visible to you, the storage of these preferences as well as the communication thereof to authorized entities will typically not be immediately visible to you as such. The Notice of Privacy Practices serves to provide you with a clear overview of these and other types of processing.

Be aware that any transaction with a recognized TAS³ service provider is likely to involve additional data processing. These data processing operations are not described in detail in our Notice of Privacy Practices, but our participating service providers are contractually bound to provide you with additional information as appropriate to ensure continuous transparency.

3. Your TAS³ Dashboard™ [184]

Once your registration is complete, your personal TAS³ Dashboard™ will be created. This Dashboard is your gateway to TAS³ services. For a comprehensive overview of the TAS³ Dashboard™'s functionalities consult our manual [*link manual*]

We apply best efforts to ensure that you have continuous access to your TAS³ Dashboard™ account. However, access might be temporarily restricted due to maintenance needs.

Network ('recognized TAS³ service providers') or any of their employees, representatives, or independent contractors acting in a similar capacity.

[184] We assume that from an operational perspective the security of the Dashboard is an obligation of the Dashboard service provider. In our current trust model, the Trust Network Operator will assume front-end liability (in other words: provide the user with immediate indemnification in case of justified complaint and then seek recourse upon the Dashboard service provider). In lower-trust models, whereby the Network Operator is unwilling to assume this type of liability exposure, there is likely to be a greater emphasis on the distinction between the Dashboard Service Provider and the Trust Network Operator.

3.1 Your privacy and trust preferences

The way in which you set your privacy and trust preferences is one of the ways that you can grant others (e.g. service providers, individuals) permission to access or otherwise allow processing of your personal information. ***It is important that you carefully consider how you set your privacy and trust preferences as the setting of those preferences will be considered an explicit consent to the operations authorized by your preferences***.

Every account is preconfigured with generic default settings. You are expected to review the default settings and to set your preferences in a way that reflects the type of data processing you wish to authorize.

Your privacy and trust preferences will be honored within the context of any TAS³ Service (see also below, section 7). Only in the following instances shall these preferences be overridden:

a) *Compliance obligations*: we, or our recognized service providers, might be required to override your preferences in light of a statutory provision, court order, enforcement action or an injunction issued by a governmental body that has jurisdiction over us or one of our recognized service providers respectively. Where possible, we will undertake all reasonable efforts to inform you when compliance involves processing of your personal information.

b) *Break the glass*: emergency situations may make it necessary to override your preferences. A situation shall qualify as an emergency situation for purposes of this provision only when the situation is of such a nature that either the vital interests or the physical or moral integrity of you or a third party are at stake.

3.2 Binding effect of your actions

By signing this agreement, you agree to be bound by any action you perform in the context of TAS³ services. For example, if you click a 'send personal information' button displayed under an information request made by a service provider, this shall be considered explicit and written consent for the transmittal of this information. Similarly, if you agree to the terms of service of a recognized service provider you will be considered as bound by this consent.

3.3 Your feedback

Every TAS³ user is provided with the opportunity to provide feedback and rate their transactions with recognized TAS³ service providers. The TAS³ Trust Rating System™[*link*] keeps track, among other things, of user trust ratings and manages the overall trust rating of service providers participating in TAS³.

We commit ourselves to incorporate your feedback in the TAS³ Trust Rating System™, unless we have reason to suspect that you maliciously submit poor trust ratings or otherwise attempt to falsify the TAS³ Trust Rating System™.

3.4 Data portability

You may want to share your personal information with entities which have not been recognized as TAS³ service providers. We warrant that any personal information you provide (or which is otherwise used) within the context of a TAS³ service shall in principle be transferrable such service providers. Specifically, you may at any time request a certified (paper-based) transcript of this information and/or delivery in an electronic format which has been recognized by us [*link list of accepted formats*].[185] However, be advised that the warranties provided in this end-user and licensing agreement in relation to TAS³ services shall not extend to the activities of entities that are not recognized TAS³ service providers, and that any request for transfer of your personal information to such an entity is entirely at your own risk.

We may not be able to honor your right of data portability in instances where the statutory or contractual obligations of the data holder prevent him from making available such information (e.g. in case of a professional duty of confidentiality).

4. Transparency

Your TAS³ Dashboard™ shall provide you with the ability to view:

- what information you have provided in the context of TAS³ services, under which policy, and where it is currently being maintained;

- which other types of personal information about you, but not provided directly by you, are being maintained by recognized TAS³ service providers where such information was obtained in the context of a TAS³ service;

- when and how your personal information has been accessed or processed in the context of TAS³ services

Note that there may be instances in which it would be unlawful to provide you with certain information related to access to or use of information when such processing is required by law. Where we are legally required to withhold certain information from you this information will not be made available to you through your Dashboard.

5. Security

Each recognized TAS³ service provider is required to document their commitment to security before becoming a member of the TAS³ Network [*link TAS³ intake criteria*]. In some cases, providers may also have submitted certification of other

[185] Needless to say, the Trust Network cannot support every type of data format available, and therefore absolute data portability cannot be guaranteed. However, it is expected that the Trust Network would support those formats which allow end-users to export their information to major service providers. A list of accepted data formats will be provided and updated as the Network matures.

proof of compliance. In order to help you evaluate the security of such providers we will provide information related to the nature and levels of documentation or proof provided.

While we strive to ensure the best possible protection for your personal information, it is important to realize that you yourself play an equally important role in ensuring the security of your personal information. As such, you will be expected to:

1. *Protect your credentials*. Regardless of which credentials you use to access your account (e.g., username and password, one-time password, eID card, …), you are responsible for protecting these credentials. For instance, you should not share your passwords or pin codes with anyone. If you want to grant access to your account you should use the mechanisms and interfaces that were designed for this purpose (e.g. delegation service) and not share your credentials as such. In case of loss or compromise of your credentials, you are responsible for taking all necessary precautions to prevent possible misuse (e.g., password change or revocation)

2. *Protect your hard- and software.* We can only control what happens on our systems, but we cannot control what happens on yours. You are expected to take every reasonable step to ensure the security of your hardware (e.g. laptop, PC, smart phone) as well as any software you are running on it. This shall at a minimum include the use of up-to-date, mainstream virus protection as well as keeping up with updates of your software, including your Operating System.

6. Restrictions and additional obligations upon use

You are obliged to refrain from:

1. Taking any action with fraudulent or harmful intent as relates to systems or infrastructure of the TAS³ Trust Network and its participating service providers, or to intentionally mislead others that may rely on information provided to their detriment (including, but not limited to, the submission of malicious trust ratings in an attempt to falsify the TAS³ Trust Rating System or the communication of false information about yourself);

2. Creating accounts on behalf of third parties unless
    a. you hold a mandate to do so
    b. you are the legal guardian of the person for whom the account will be created

    In both the case of a) and b) you must provide us with appropriate evidence thereof [*link*] (e.g. delegation agreement, proof that you are the legal guardian).

3. Transferring accounts to third parties unless you have either (a) received our prior written consent or (b) complete this transfer using a TAS³ interface explicitly dedicated to this purpose;

4. Uploading any information about third parties without either their express and prior written consent or unless they have authorized you to do so using a TAS³ interface explicitly dedicated to this purpose (e.g., delegation service);

5. Attempting to access any information about other end-users of TAS³ (including people you know or to whom you are related) without appropriate authorization is prohibited by this agreement, and if intentional it is considered a breach of the terms of this agreement. Should you accidently access information of others you are expected to refrain from making any use or copy of such information and are expected to inform us of such access;

6. Copying or making use of the TAS³ logo, domain name, TAS³ certificates or any other protected intellectual property of TAS³ [*link IP overview*] unless you have received our prior written consent;

7. Doing anything that could disable, overburden, or impair the proper functioning of the TAS³ infrastructure or TAS³ services (such as, but not limited to, introduction of viruses or the launching of a denial of service attack);

8. Using TAS³ services unless you have reached 18 years of age, or have supplied us with the written consent of your legal guardian.

Your are obliged to:

1. Comply with all applicable laws and regulations when making use of any TAS³ service, as well as any operational policies that apply to them;

2. Provide truthful and accurate information only; and take every reasonable effort to help ensure that your personal information remains accurate up-to-date [*link update procedures in manual*].

3. Make use of TAS³ services only for the purposes and in the manner for which they are intended as set forth in the manual or other directions we or our recognized service providers supply on how to use the services

7. Complaint and redress

If you have any complaint related to any TAS³ service (e.g., if you suspect that your data has been used in a manner in which you have not authorized) you have several means of obtaining redress. We subscribe to a 'no wrong door' policy, which implies that you may direct your complaint to any recognized TAS³ service provider or directly to our helpdesk.

We will follow-up on your request in [xyz] days. If your complaint is found to be justified, and within the scope of the warranties articulated in the terms of this agreement, we will attempt to provide you with appropriate redress, which may

include compensation for any actual harm you may have suffered.[186] The limitation of our commitment on this point our set forth in the following section. If you are not pleased with our proposed resolution of your issue, you may appeal to the TAS³ Audit and Oversight committee [*link*].

In any event, you retain your ability to obtain redress through the normal legal system at all times. Should you choose this option we will provide as much assistance as we reasonably can in order to provide you with information relevant to your complaint (e.g., a certified transcript of relevant audit trail information).

8. Limitation of liability

We make every reasonable effort to deliver on the promises we make. However, there are certain limitations as to what are able take assume liability for, such as:

1. *Trust Rating*. The TAS³ Trust Rating System™ is based, among other things, on the feedback provided by individual end-users. The algorithms that are used to assign a particular trust rating are public [*TTRS link*]. However, we do not wish to restrict users in submitting their personal ratings (we only ask that every user acts fairly), and we cannot reasonably monitor every rating. It is important that you realize that it is your personal choice whether or not you rely on a particular trust rating. The only guarantee that we offer is that the rating in question was assigned in accordance with our established TAS³ Trust Rating System™. Note also that each recognized TAS³ Service Provider is provided with an initial baseline rating that is predicated on the level of proof they were able to provide to substantiate their certification statements related to their compliance, security and privacy practices. For more information see [*TTRS link*].

2. *Fitness of purpose*. Your TAS³ Dashboard™ is only fit for the purposes which are advertised explicitly or unambiguously implied. Individual services offered by a recognized TAS³ service providers are only fit for the purposes stated by the respective service provider.

3. *Security breaches*. As indicated earlier, we take every reasonable effort to ensure your personal information is protected by a high level of security. The security of TAS³ services is based on the implementation of TAS³ technical specifications, organizational practices and procedures set forth by us, together with the best efforts of recognized TAS³ service providers to uphold those specifications. Even the best security can be breached so we cannot guarantee an outcome beyond generally accepted industry best practices. We also do not accept liability for security aspects beyond any control of TAS³, such as security breaches which occur as a result of a

[186] In a lower-trust model, whereby the Trust Network Operator wishes to limit its involvement in dispute resolution to mediation this might read: '… not only take action against the participating service provider in question, but attempt to reach an appropriate settlement on your behalf'.

compromise of security in the end-user environment of individual TAS³ users (such as yourself).

4. *Actions of recognized TAS³ service providers outside the context of TAS³ services.* The TAS³ Trust Network is comprised of many different service providers [*SP overview link*]. The representations and warranties contained in this agreement only apply in relation to TAS³ services. To the extent that you have (or have had) independent relationships with a recognized TAS³ service provider (i.e. a relationship outside or beyond the context of a service advertised as being a TAS³ service), these relationships are not governed by the terms of this agreement. Consequently none of the warranties provided in this document extend to these relationships. These transactions and relationships are governed solely by your (separate) agreements with these actors.[187]

5. *Enforcement of privacy and/or trust preferences towards service providers who are not recognized TAS³ service providers.* If you choose to disclose personal information to a service provider who is not a recognized TAS³ service provider we cannot guarantee the enforcement of your privacy and/or trust preferences. We can only guarantee that the content of your preferences will be communicated to such third party recipients even if they are not part of our Trust Network. We will not monitor their compliance in any way nor provide you with any form redress or indemnification in case of non-compliance.

6. *Liability and redress.* As explained above, we provide a central point-of-contact to receive complaints concerning the activities of any recognized TAS³ service provider by means of the TAS³ Oversight committee. We commit ourselves to providing appropriate redress in the form of a proposal for indemnification in instances where your complaint is considered well-founded by the TAS³ Oversight Committee. No indemnification shall be provided if, nor shall we liable for:

    a) Any damages caused or augmented as a result of your default upon any of your obligations identified in this agreement;

    b) Any damages exceeding the sum of [XYZ][188]

---

[187] In a lighter trust model this portion would read: 'We apply reasonable efforts to monitor that every recognized TAS³ service provider adheres to the reference policies and rules that govern the Trust Network's activities. As a result of your use of TAS³ services some of our participating service providers may retain certain information related to this transaction. Every recognized TAS³ service provider is bound by contract to only make use of information in a manner and for the purposes which you have authorize and as identified by our Notice of Privacy Practices.'

[188] We expect that the Trust Network operator will choose to set a limit ('cap') for the liability it is willing to assume for the activities of recognized TAS³ service providers; and that this limit will be articulated as a nominal amount. This amount is likely to be decided at the level of each Trust Network individually, though a certain benchmark might be set in order to avoid dilution of the TAS³ logo.

9. Changes in terms

The terms of this agreement may be subject to change. Any changes to the terms of these agreement will be notified. Such notification will be sent both to your email-address of record and will also be highlighted through your TAS³ Dashboard™. You will be given a period of [xyz] to opt-out when such notification is given. If you choose to continue to use your TAS³ account or any TAS³ service once notification has been provided, this will be considered as unambiguous and written consent for the new terms, and all activities from that date forth shall be governed by the revised terms.

It is also possible that legislative developments require us to modify our policies one way or another. If that is the case we will, whenever possible, provide you with the same period of [xyz] to opt out. Keep in mind that the legal requirement may be of such a nature that it must be applied with immediate effect, and that as a result we might not always be able provide you this period for consideration.

10. Termination

You may decide to stop using TAS³ services at any time. Simply notify us of your wish to terminate our agreement and we will delete your account.

We may be required to retain certain data related to your account or specific transactions for compliance and security verification purposes, as might any recognized TAS³ service provider. We will notify you of such instances at the occasion of termination, but will in any case ensure that these data are deleted as soon as there is no longer any legitimate reason to keep them.

In case of termination you will be offered the opportunity to receive a certified (paper-based) transcript of this information and/or delivery in an electronic format which has been recognized by us [*link list of accepted formats*]., except where such communication might infringe upon a legal requirement.

We also have the right to terminate your account if you do not adhere to the terms of this agreement. Arbitration may be requested through the TAS³ Oversight Committee. Such termination or arbitration does not affect any of our rights to legal recourse.

11. Applicable law and jurisdiction

This agreement is governed by the laws of your country of residence at the moment of your entering into this agreement. All claims may be brought before a court of the country in which your reside at the moment of your entering into this agreement.

12. About Us

The TAS³ Trust Network Operator is a private company [xyz] established in [xyz]. It is subject to [xyz]. We can be reached at [xyz]. All correspondence which cannot be communicated through a dedicated TAS³ interface should be sent to this address.

8.9 Annex IX – TAS³ Notice of Privacy Practices

The following is the proposed general or top level Notice of Privacy Practices for a TAS³ *implementation (for example one in health care, employment or placement). Within this document, italicized guidance is provided to enable implementers of each TAS3 implementation to provide more specifics or customization (for example more detailed information related to use or purpose of collection for specific data elements or the actual links to complaint URLs etc). Some of this information will also be useful in developing some of the needed ancillary forms that will need to be tailored to web implementations.*

In Year 4 we will develop further guidance based on the experience of the demonstrators to further assist implementers in properly implementing this Notice. While we have tried to make the notice clear and user-accessible, it remains very long. In year 4 we also propose to provide a short form Notice of Privacy Practices. Since simplification and clarity of notice is one of the work items considered in the review of Directive 95/46 we hope that useful guidance may be provided in the first quarter of next year on what form the EC simplified notice may take.

TAS³ Draft Privacy Policy v.4

TAS³ NOTICE OF PRIVACY PRACTICES

1. Introduction

The Trusted Architecture for Securely Shared Services is a technical, policy and legal infrastructure designed to promote greater trust in the use of online portfolios and the sharing of information from those portfolios for related services. The TAS³ model is predicated on concepts of access control, data minimization, purpose limitation and strong audit controls. All of these features serve to enhance security and protect privacy while empowering individual users to control use and sharing of information. This policy is provided to inform individual users of what information will be collected how it will be used and their rights related to personal data.

2. Information Collection, Purpose Specification and Use Limitation

Information Collection, Purpose Specification and Use Limitation are separate concepts that are very closely intertwined with one and other. These concepts are elaborated separately in the paragraphs that follow, but will these elements, controls and how they relate to each other will be combined in a Matrix.

a) Information Collection

All business models and technical operations require the collection of information. In some cases information is directly collected through forms and other direct forms of information collection. When using online applications,

incidental technical information may also be collected: related to equipment, both software and hardware; how you navigate a site; response times; quality of service etc.

The elements of personal data collected within TAS³ include:

- The personal data you directly provide to a service provider; enter into your dashboard or personal data store; and/or provide as part of proving identity, credentialing or authentication
- Supplemental information and personal data you may provide in relation to specific transactions
- Technical information that is:
    - Needed to establish and support communication protocols (e.g., type of browser, possibly port configurations, encryption (SSL) status of communication)
    - Incidental to your use of a website, this may be collected through log files, cookies of various types and other technologies that capture information related to your use of the website:
        - Where you have not logged into a website, this information will either be collected anonymously for the purpose of maintaining the session and for security and convenience purposes (note that while you may not be identifiable as a specific person, you are likely identifiable as a unique individual so some tracking may be possible)
        - Once you log into or are otherwise authenticated to a site, your behavior on the site will be traceable to you as an identified individual.
        - In both cases information could include: what web pages on the site you have seen, your navigation paths to (the site from which you came may be transmitted) through the site (the order of links and pages on the specific TAS³ service provider site visited) and the next link you navigated to after leaving the site.
    - Some of this information may be accessible across TAS³ service provider interactions to facilitate the provision of audit and dashboard services but controls exist, as described in the following sections, to prevent misuse of this information.

- Third party information relating to you that may also be collected which could include validation of credentials, reports from supporting organizations or services (e.g., lab results, employment records…). TAS³ provides mechanisms, described in the following sections, which enable you to manage and review how and when third parties are consulted.

Note to implementers: We have described the generic types of information collected; where possible provide more detailed information or specific examples of the information your implementation of TAS³ will collect. Service providers should also consider providing a Supplemental Notice of Privacy Practices should their information collection requirements be different than those represented in the general Notice.

b) Collection Limitation

In order to be most respectful of privacy, the recommended and legally required best practice is to collect the least personally identifiable information necessary to accomplish the purposes for which information is collected. TAS³ accomplishes this by enabling users to implement granular controls on information elements helping to control their use and sharing. TAS³ attempts to find an optimal middle ground between requiring individuals to micromanage information and enabling granular choice through privacy respectful default settings.

c) Purpose of Collection

Personal information can only be collected for legal and legitimate disclosed needs. These needs are referred to as the purpose of collection. Personal information collected for an identified purpose must be relevant to that purpose. This concept is directly related to the collection limitation principle.

TAS³ provides mechanisms for individuals to control access to information and scope of sharing. Personal preferences related to sharing of information, may, however, conflict with the amount of information a provider feels is required to accomplish the requested service. TAS³ provides a discovery function whereby individuals may set forth the term under which they will allow information to be used, which will allow you to match those terms with available service providers that can meet those preferences. You are also provided opportunities to limit purposes for which information may be collected in each of your transactions in TAS³.

There are five main reasons to collect information in any transaction:

1. **To accomplish the purpose of the transaction,** for example, his may include contact or residence information if something needs to be delivered or financial information if payment is required.
2. **For Operational Purposes.** This may include the technical information captured by a website or needed to use a communication protocol as well as information required to correctly process- or maintain information. Some of this information may be the same as that which is required to accomplish the purpose of the transaction.
3. **To Improve the Service.** This information is collected for purposes tied very closely to operation but may be used beyond the processing related to the transaction in order to track or improve the functioning of the service (e.g., screen refresh times, service delivery, quality and response information, information related to site navigation). A special case of this concept would also be information for medical or socio-statistical research purposes. As there are compelling public policy reasons for information to be made available for these purposes and they are also usually the subject of detailed regulations created to ensure the security and confidentiality of that information.
4. **In Response to Legitimate Legal or Governmental Requirements.** This can include all types of information that has been collected and can range from complying with regulation, to requirements of law enforcement and national security to legal requirements of courts and litigation. A

special type of this requirement may apply to financial information as it relates to credit application and fraud prevention.

5. **Marketing.** Lastly, information may be collected for marketing or other business discretionary purposes. We have included marketing for completeness. Please be assured that facilitation of marketing is not a main purpose of TAS³. If there may be instances where some information is explicitly requested for marketing, it would be subject to explicit consent.

While a number of these purposes are closely related, we have split them into these categories to track emerging models of user concerns and to better enable the application of user controls to categories of information.

3. Use Limitation

Much like the principle of collection limitation, the principle of use limitation is a best practice requiring that information be used only for the purposes specified or those directly related to providing the requested service or transaction. The definition of purposes and related uses within the TAS³ architecture help assure the narrow interpretation and direct relation between the stated purposes and uses of information. Users have further ability to choose among specified controls to further customize some of the uses. TAS³ has implemented privacy defaults and selected choices in an effort to enable meaningful customization and control without creating undue burdens of information management and technical control on the individual.

Use categories are the same as those related to the specified purpose of collection and obviously closely related to what information is collected. Use limitation within TAS³ has two major components: data minimization and user controls. Data minimization is directly related to concept outlined above and is a design principle inherent in TAS³: use the least amount of information needed to accomplish the service or process. These concepts are implemented by the Trust Network and participating service providers in the way they configure their system, but are also supplemented by user controls and preferences which allow further customization to your requirements. Infinite customization to a unique individual preference set may not be possible, but TAS³ provides both a preference expression and management system in the dashboard to help assure you that service providers identified by the discovery service are compatible with your preferences as well as policy negotiation tools to help you enable a supplemental matching of use preferences at the transaction level.

Please refer to the Matrix attached to this policy for more detailed information of the interaction across the various elements, specific considerations you should be aware of and related TAS³ controls.

4. Consent

Users must consent to the collection and use of personal information. Consent must be both affirmative (opt-in) and informed. The TAS³ technical architecture enables users to consent to uses of information at a granular but user-friendly level. Your personal information that is used in relation to TAS³ services is

accessible through a Dashboard, and the user can manage her privacy preferences and controls through the same interface. Use of previously collected information, not related to a purpose disclosed and consented to at time of collection, requires new or additional consent.

You should be aware that there may be some instances where you may not have the opportunity to provide consent related to the use of information. These are based on requirements of legal compliance or compelling public policy need.

Implementer should provide details of any other way in which consent is enabled at the transactional level or any additional information relate to consent which may be outlined in a supplemental notice or privacy practices...

5. Access/Correction/Retention and Deletion

Individuals have a right to be provided with a list of what personal information is in the possession of the entity who controls the data (often the entity that collected the data) as well as information on how it is being and has been used (including who it has been shared with). Beyond the ability to merely access the personal information, the user has also has the right to correct the information where it is inaccurate, and in some cases also to have the information deleted. Much of your personal information is either directly uploaded by you into the Dashboard, or via a service provider or other entity that you have requested to provide information to TAS^3. Some personal information about you may also be generated as a result of transactions you engage in on the TAS^3 network. The audit function of TAS^3, available through your Dashboard, is a resource that can provide you with answers to inquiries related to what information have been collected and how it has been used within the network.

As was highlighted in the Collection limitation and purpose section, personal information is collected in a limited fashion for specified purposes. That personal information can only be retained for a period of time that is relevant to stated purpose of collection. Thus a delivery address for a present purchased by a customer should not be maintained beyond the assurance of delivery or some logical time thereafter during which a question related to delivery might arise. The purchaser's information may need to be maintained for a longer period of time for tax, warranty or other legitimate governmental or business purposes.

Seeing service providers may also need to store certain elements of personal information for a period of time for transaction related purposes, inquiry should also be made of service providers that you have dealt with. To facilitate this process, a global form is available to make that request of selected service providers

The implementer should develop a form with a checklist of providers that is automatically sent to the correct contact for every service provider that the user checks which has boilerplate language requesting a response to information held, use and sharing needs. A supplemental form would be attached with the reply information to facilitate requests for correction, deletion etc.

While TAS³ will use its best efforts to honor your request for correction and deletion, please be aware that some transaction related information may need to be maintained despite your request to fulfill legal requirements or as related to audit, log and security functions. TAS³ commits to using that information only for those narrow and specified purposes during the time for which it must retain the information after a deletion or correction request. Where not prohibited by law, TAS³ will inform you of cases where your request cannot be fully honored.

Requests for access, correction and deletion will be honored or have delays explained with proposed completion date (where clarification is needed or access request encounters problems) within 30 days. Confirmation of actions taken is available upon request.

6. Security

Security is an integral part of data protection and all organizations that control or process data are obliged to provide appropriate security of personal data. TAS³ addresses security requirements in two ways. First, the TAS³ transactional infrastructure has been designed with security in mind and utilizes encryption, authentication and other technologies to secure information that is within the TAS³ infrastructure. These technologies secure information during TAS³ transactions. TAS³ Technology is also supported by policies and contractual obligations that relate to the TAS³ transactional infrastructure. As was discussed in relation to Access/Correction Retention and Deletion, some personal information may be stored by service providers to accomplish the purposes of the transaction or for required business or governmental purposes related to the transaction. That information will be maintained by the individual service provider within their infrastructure that is beyond the contrail of TAS³. While the security of that infrastructure is the responsibility of that service provider, TAS³ does provide minimum security requirements that all service providers are contractually bound to follow and further requests providers to provide information related to their security practices.

In order to assist you in choosing and evaluating service providers, summaries of this information will be made available (at a level and in a way that neither compromises their security or company confidential information) as well as whether they adhere to certain established security or other relevant broadly accepted standards of practice. Where available, we will also provide information on whether their practices and implementation have been evaluated, certified or otherwise validated by third parties. As TAS³ matures, we expect more third parties to provide services which will assist end users in evaluating reputation or levels and effectiveness of security. To the extent possible TAS³ will also include those criteria in the reputation scores it develops for its service providers. Recall that those score are partially dependent on user feedback as well.

While we encourage all of our service providers to use the minimum security requirements as a baseline across their operations, the actual legal obligation is related to securing information related to TAS³ transactions. Thus if you have or develop independent relationships with such providers you should take appropriate steps to understand whether the security provided related to those services is appropriate to your needs.

7. Oversight and Accountability

In order to provide you with security and trust in TAS³ we provide oversight through compliance and visibility functions, supported and enabled by tools, practices and policies (collectively referred to as "compliance functions"). These tools, policies and practices are designed into the legal, policy and technology architecture of TAS³and are made available in an appropriate manner to users, service providers and other related parties. Due to the integration of features and architecture, some of these have been previously referenced. We also remind you that more detailed descriptions on the functionality and operation of these features are available in the user manual.

User: Individuals are an important element of oversight in any architecture. While technologies are designed with protections and controls, technical errors can happen and persons or organization may inadvertently or intentionally fail to follow policies and practices.

As a user of TAS³ , you are provided with a Dashboard that provides oversight visibility into the information you have provided as well as how it has been used through audit and related functions. You are further provided the ability to request information on what data concerning you are being held by a service provider to enable you to get a more complete understanding of your data and its operation and lifecycle.

At the inception of your relationship with TAS³ you also signed an End User License Agreement (EULA) which specified your rights and responsibilities related to your participation in TAS³. Recall that while most obligations are on the service providers you too have obligations related to maintaining the security and the appropriate use of information.

TAS ³: It is usual for one or more service providers to be the natural organizational interface for individuals who participate in TAS³. In a number of cases individuals may also have Dashboards and personal data stores provided by third parties which also form another major interface to TAS³. Organizationally, all TAS³ service providers are bound to respect both this set of Privacy Practices as well as the other generally applicable policies of TAS³.
It is impossible, however for one general policy to cover the details of each service provider's operation, thus individual service providers may provide supplemental notices of privacy practices which you should also read carefully. If no supplemental Notice of Privacy Practices exists, then you can rely on this Notice of Privacy Practices to be the complete statement of the service provider's practices.

We are not attempting to create more work for you by asking that you read more than one policy, but rather attempting to provide the most specific information possible related to the type of service you are using without your having to determine which part of a huge statement of practices may apply to any given service provider.

Audit: TAS³ provides an audit functionality that is used in two main ways. In first instance, it enables the re-creation of transactions for purposes of investigation and non-repudiation. Secondly, the audit trail is available to you through your dashboard as a way of reviewing compliance. Audit information is maintained by the various services providers as part of their accountability framework, but can also be reconstituted across service providers by TAS³ in response to inquiries, complaints or investigations. There are strict controls related to how and when such review of information across service providers can occur. Lastly, the ability of TAS³ to audit is supplemented by periodic audit reports which are reviewed by an Accountability and oversight Committee as part of proactive accountability as well as to be a spot check of service provider compliance

Complaint/Redress: One way in which we hope to facilitate the compliance process for you is to have a "no wrong door" approach to complaints. While we provide a general e-mail link (*to be inserted by implementer here*) for complaints about any aspect of TAS³, you may lodge a complaint with any TAS³ service provider and it will be raised to the appropriate group within TAS³ for resolution. In some cases you may not be able to tell which organization might be the source of the issue you are having, so we have developed internal mechanisms to assure that you can lodge a complaint across all TAS³entities. In order to facilitate this process and assure that we have all the information needed to address and resolve the complaint, a form is provided (*implementer insert form link here*) to facilitate your providing us with the needed information. While we will attempt to limit our requests, in some cases further information or detail will be required and you may be contacted by e-mail or other means you specify in the form to clarify information provided or to provide supplemental information to help us address your issue.

You waive none of your legal rights to take complaints to outside Authorities by participating inTAS³, but we ask you to first use the complaint mechanisms provided as we believe that they provide the most expedient method of resolving issues. Further details on the compliant process can be found in the TAS³ manual.

TAS³ Commitment: Recall that the TAS³ architecture was designed to further privacy and security. The service providers who participate have recognized the value of privacy and security and are striving to create a safe and user-friendly environment that earns your trust. Despite the best intentioned technology and policy solutions, mistakes can happen, so we have developed what we believe to be effective compliance and redress mechanisms. As a demonstration of that commitment, the service providers participate in providing a pooled fund to insure against liabilities in the amount of _____ (*amount to be determined by implementers*). The purpose of this fund is to demonstrate the group's commitment to effective and timely redress. The fund is not meant to be a cap of all liability, but rather serves as a source of quick assistance to

individuals who may have suffered harm in the course of their participation inTAS³.

Further recourse against the service provider(s) who caused the harm is always available and TAS³ will provide assistance to you in determining which provider(s) may have contributed to causing the harm.

8. Compliance with Law / Jurisdiction

All TAS³ service providers are subject to the legal compliance obligations of the jurisdiction of their establishment, as well as the jurisdictions which they operate in. TAS³ service providers will do their best to protect the confidentiality of your information and will require that appropriate legal requirements are met in any governmental or other requests for information that are made pursuant to legal process (court-ordered production of information etc).

Implementer should make sure that Notice provides any relevant information of processing outside of the jurisdiction of the individual. These may be most relevant in the service provider Supplemental Notice and should be clearly highlighted. There may also be affirmative consent required depending on circumstances.

9. Compilation of Important Contact Information

Implementers should provide the email addresses, physical address and any related phone numbers for contact. It is also suggested that the link to the complaint form be provided her as well. Finally, depending on the size of the TAS³ *implementation, it may be wise to create a "Privacy Central" site with links to all of the service provider Supplemental Notices of privacy Practices.*

Matrix: It is very difficult to properly understand personal data collection, purpose and use in isolation. This is even more so when considering information that is incidental to the purpose of collection, but technically required or used for operation of improvement of services. For example, one purpose inherent in information collected is the proper functioning and enhancement of the delivery of services. For instance, information collected about the speed of a web page loading and the best way or order to present web pages related to the service are among the inherent and technical purposes for which information is collected and used. The matrix table provided below will help you better assess and understand the relationship between the types of information collected, the function it is relevant to and purpose for which information is collected/used and the related TAS^3 control.

Implementer should provide further customizations to the matrix table to provide a more granular view of the interaction between distinct information elements, purpose of collection and permitted uses to provide greater transparency to the user.

Data Element Type	TAS³ Function	Purpose(s) of collection and uses of data	Special Considerations	TAS³ related control
Contact Information Name , Address, e-mail, Home phone, business contact information, e-mail Mobile phone	Almost all services require some level of access to this information, including aspects of; Intake/Registration, Operation, Transaction, Legal compliance and Audit/Oversight	Authentication, fulfillment of service, support, proper operation and improvement of the service (majority of site operation/improvement can use aggregate as opposed to personally identified data); audit, or oversight. All of these purposes apply to the related service either provided directly by the data collector, through a processor or in conjunction with a co-controller of the data	In both employment and health scenarios, the mere existence of your name as the subject of a file or as person with a medical or employment relationship can create implications to third parties that you might prefer to keep confidential. You should consider who might have access to the communication channel you specify. Note that e-mail and mobile telephones may be more easily under your control as they may be less accessible to other people in you workplace or home. Note however that both e-mail and mobile phones, of necessity, create digital records that may be	Access to what elements of this information are used and how may be available both in the dashboard and in options that may be configurable at the transaction level.

			available to service providers related to the communication technology.	
Intake / Registration Data elements related to Intake/Registration would include contact information as well as information related to: • Information which confirms or proves that you are who you say you are such as information about you type of ID or proving an attribute, perhaps age, • Including related credential(s)	Identity verification Credential binding EULA execution Account provisioning Transactions Operations Audit Legal Compliance	Dashboard Service Providers and RA's need to collect this information in order to accomplish: identity verification and properly bind the credential, which are required steps to execute the license agreement that allows you to create a TAS³ account. Your TAS³ account and credential enable you to use your Dashboard and other tools which should be considered both your gateway and control center for preferences and personal oversight.	Different categories of assurance will require different types of credentials and levels of proof of identity. You need to consider the type of service being provided and the level of proof being sought. You do not need to provide more information than is required to establish the needed assurance. While service providers are bound to protect the confidentiality of information, it is a good practice to provide only the amount of information and related credential needed to obtain the service. Once an account has been provisioned you have the opportunity to set your privacy preferences – it is very important that do this expeditiously and pay close attention which preferences you choose as they will	Dashboard offers the ability to set privacy and trust preferences in relation to TAS³ services and -the ability to: authorize transfer of personal information ; -the ability to view which service providers within the Network store information about you -the ability to view which operations have been performed upon your data, and -a complaint mechanism

			directly impact the services providers that are made available to you and the types of policies or preferences they can support.	
Personal Data You Provide/Store One of the core functions of TAS3 is to enable users to create portfolios of information relevant to employment and health. It is likely that most users will provide information to populate such portfolios as part of the use of TAS^3.	Transaction fulfillment Legal compliance	This information will be used in accordance with your preferences by the providers you choose to deliver requested services. Service providers are contractually bound to maintain the confidentiality and security of this information and to use only that information which is required to accomplish the requested service	Here again we stress the need for you to properly define your preferences. Service providers will indicate how much information they need to provide a service at a defined level of assurance. If you do not take care in defining your preferences and setting the appropriate controls, you may inadvertently be providing more information than you need or intend to provide. You should also periodically use the audit function of your Dashboard to see who has accessed your information and how it has been used. While there are protections against misuse built into the system, privacy protections are	Dashboard • Audit • Privacy and Trust Preferences

			personal and this periodic review will help assure that your preferences are properly configured and correctly being honored.	
Transactional Information The additional data elements in question will be defined based on the service requested.	Fulfillment of the service requested. Discovery Service Audit Legal Compliance	We ask that each service provider publish any additional information needed on the collection and use of personal information in a Supplemental Notice of Privacy Practices. Transactional information is captured in a secure and distributed manner to enable the recreation of audit trails related to transactions.	While TAS3 technology, policies and contracts are designed to help assure that all service providers are held to TAS3 compliant privacy standards, you are responsible for making sure that you have read any relevant notices provided related to those services. We have not only required that service providers clearly and conspicuously post their Supplemental Notice of Privacy Practices on their site, but have provided a centralized set of links to these Supplemental Notices which can be found as and an annexed page the main TAS³ NPP.	-Dashboard preferences inform the TAS³ Discovery service which is designed to match service providers who can meet the specified privacy preferences. -Centralized NPP and SNPP links
Technical Operational Information	Technical operation Technical	In most cases this information's utility is in the aggregate – to see how	It is common for websites and technology service providers to use this type of	Consent, where applicable

This refers to the information a site requires to maintain or improve operations. It can include site refresh times to navigation information, browser type, level of encryption used, types of services selected, and connection information among others.	improvement Potentially across all functions	the website or technology is functioning, and where it may be improved. In some cases, your information may be considered in a way that it can be identified if you have run into a unique service difficulty or disruption. Apart from the contractual bindings and policies of TAS3, all service providers remain obligated to comply with local laws and where information used is personally identifiable remain accountable for obtaining any applicable consents required to use the information in such manner.	information to maintain and improve their services. You should be aware however that most of this information collection and use is not visible to you because most all of this information is captured in a manner incidental to the service provided or use of the website/relevant technology. You should also be aware that in some cases this information may be used in determining the proper function of a system or architecture which may involve review of the use of information across service providers. TAS3 policies and legal obligations require that this information only be used for the specified purpose of maintaining or improving the site, service or technology in question.	

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
3.1	22-12-2010	Brendan Van Alsenoy	Integration of end-user intake process
3.1	23-12-2010	Joseph Alhadeff	Extension of intake process for service providers
3.2	24-12-2010	Brendan Van Alsenoy	Integration update controller-processor section
3.3	26-12-2010	Joseph Alhadeff and Brendan Van Alsenoy	Integration part II
3.4	27-12-2010	Brendan Van Alsenoy	Integration EULA
3.5	28-12-2010	Joseph Alhadeff	Integration Notice of Privacy Practices
3.6	31-12-2010		Release