GLOBAL IDENTITY NETWORKING OF INDIVIDUALS

The Individualised Digital Identity Model

A Regulatory Framework for INDI Operators

April 27, 2012

Project Name	GLOBAL IDENTITY NETWORKING OF INDIVIDUALS
Project Number	FP-258630
Work Package	WP3: The Legal and Regulatory dimension of the INDI Domain
Document title	A Regulatory Framework for INDI Operators
Document type	Report
Deliverable number	D3.2
Authors	B. Van Alsenoy, Dr. E. Lievens, Dr. Katleen Janssen, Prof. Dr. J. Dumortier (ICRI, KU Leuven), Prof. Dr. K. Rannenberg, S. Yang (Goethe Univ., Frankfurt a.M.), Prof. Dr. T. Andersson, Q. Abbas (IKED), H. Leitold, B. Zwattendorfer (TU Graz)
Editors	B. Van Alsenoy (ICRI, K.U.Leuven)
Date	2012.04.27
Version	1.2
Status	Confidential
Total number of pages	63

Table of Contents

Executive Summary

GINI-SA aims to examine how a **Personalized Identity Management (PIM) ecosystem** can be created where individuals can manage their own digital identities and exercise control over the exchange of their identity information. The objective of this deliverable is to identify areas in which regulatory intervention is warranted in order for

1. **an operator-driven infrastructure** to be established, become operational and function smoothly across EU borders;
2. in a manner that guarantees **privacy**, gives **choices** to individuals; and
3. allows **institutional actors** to oversee the **respect and enforcement of legal rules** to the benefit of the public interest and the private interests of individuals.

This deliverable starts by analysing the concept of an **identity trust framework**, a concept which is referenced increasingly in policy, research and industry papers that seek to promote trust in online digital identities. In doing so, it articulates the key *functional*, *legal* and *trustworthiness* issues at stake. Such issues include: the accuracy and integrity of identity information; the reliability of authentication processes; the (data) privacy interests of the individuals concerned and the accountability of the participants to the ecosystem.

In the subsequent chapter, this deliverable describes the **regulatory options available to EU policymakers**. These options are divided into two main categories: *legislative* and *non-legislative* measures. This chapter then proceeds to outline the possible relationship(s) between the identified regulatory measures and trust frameworks. It concludes that this relationship will hinge mainly upon the *level of involvement of governmental authorities in the setting and administration of a trust framework's policies*. In addition, regulatory measures can also be used to provide *incentives and/or co-ordination* to either (a) promote the emergence of one or more trust frameworks and/or (b) align their functioning with one or more policy objectives.

Finally, this deliverable identifies a number of **areas in which further regulation appears warranted** in order to realize the GINI vision. Such areas include: privacy enhancing technologies; data portability; accountability of data controllers; re-use of public sector information; and the mutual recognition of electronic identities. While this chapter remains far from being conclusive for each of the identified areas, it does point to specific gaps and lines of further inquiry, and outlines the types of regulatory measures best suited to address these gaps.

The findings of this deliverable serve, together with the findings of D3.1, as input to deliverables D5.1 (Research and implementation roadmap) and D5.2 (White Paper).

1 Introduction and scope

GINI-SA aims to analyse how a *Personalized Identity Management (PIM) ecosystem* can be created where individuals can manage their own digital identities and exercise control over the exchange of their identity information. In recent years, much research has been performed on the topic of user-centric identity management.[1] The main aim of these research projects was usually technical feasibility rather than legal realization. In addition, much of the legal research in this area has focused on compliance aspects. Only limited research has been conducted to identify the potential legal barriers towards the development and actual deployment of user-centric identity management services, be it on a national or pan-European level. Similarly, only limited research has been performed to determine whether additional regulation may be needed in order to enable the development of a PIM ecosystem.

In deliverable D3.1, we analysed the main elements of the current EU regulatory framework affecting the development of a PIM ecosystem and the provisioning of INDI Services. The objective of this exercise was not only to identify relevant legal requirements, but also to articulate potential barriers and gaps. To this end, four areas of EU regulation were investigated, namely:

1. Data protection and privacy;
2. Re-use of public sector information;
3. E-Commerce; and
4. E-Signatures.

Building on the findings of D3.1, the current deliverable (D3.2) aims to outline areas in which further regulation or other policy initiatives may be needed in order to create a (legal) framework which is sufficiently conducive to the development of privacy enhancing identity management services which are based on an operator-driven infrastructure.[2] Specifically, this deliverable aims to

1. suggest the areas of regulatory intervention that may be necessary at national and/or EU level in order for an operator-driven infrastructure across EU borders to be established and function smoothly,
2. in a manner that guarantees privacy, gives choices to individuals, and
3. allows institutional actors to oversee the respect and enforcement of legal rules to the benefit of the public interest and the private interests of individuals.

In order to frame our analysis, we will start by analysing the concept of an *identity trust framework*, a concept which is referenced increasingly in policy, industry and research papers that seek to

[1] See e.g. PRIME (https://www.prime-project.eu); PrimeLife (http://www.primelife.eu) and PICOS (http://www.picos-project.eu).

[2] The PIM ecosystem envisioned by GINI is based on a network of Operators. The main role of these ('INDI') Operators is to act as trust mediators. Their services are designed to provide other entities within the PIM ecosystem with the assurances they need in order to enable the disclosure and reliance upon identity information, even where the parties involved do not have pre-established trust relationships. As described in GINI D3.1, the INDI Operator is to be seen as a 'logical entity', which could in principle both be a separate legal entity which is charged with performing certain processing operations, but it could also be a purely technical application (e.g. a software component which runs locally on a device controlled by the INDI User). Naturally, the choice for either implementation model will have substantial privacy ramifications. See also GINI D3.1, section 2.2.

address trust in online digital identities.[3] In adopting this approach, we hope to more accurately identify the key functional, legal and trustworthiness issues involved in the development of a PIM ecosystem. Once this analysis has been completed, we will outline the regulatory tools available at EU level, and how they might be used. Finally, we will identify a number of areas in which further regulation may be necessary in order to promote the development of privacy enhancing identity management services which are based on an operator-driven infrastructure. The findings of this deliverable will, together with the findings of D3.1 serve as input to deliverables D5.1 (Research and implementation roadmap) and D5.2 (White Paper).

[3] See e.g. M. Rundle (ed.), 'Open Identity Trust Framework (OITF) Model', March 2010, available at http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/oitf.aspx (last accessed 18 February 2012) [OITF]; The White House, *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011, Washington, p. 25, available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (last accessed 18 February 2012); DLA Piper, Sealed, Time.Lex, Price Waterhouse Coopers SG&A, 'D1.1 IAS in the European policy context' (draft version), *Study on an electronic identification, authentication and signature policy (IAS) project*, p. 3 et seq., available at http://www.iasproject.eu/docs.html.

2 Identity trust frameworks

2.1 What is a(n identity) trust framework?

Trust is an amorphous concept. Many attempts have been undertaken to define the term 'trust', but a universally agreed definition is yet to emerge.[4] To a large extent, this may be attributed to the fact that the term often receives a context- or discipline-specific connotation. In certain contexts, the term has even been used to convey entirely disparate meanings.[5] Notwithstanding these discrepancies, there appears to be a common baseline understanding of the meaning of trust; at least from a high-level perspective. In almost all disciplines, the existence of a trust relationship is typified by a *willingness, of one entity* (the trustor), *to accept vulnerability based upon positive expectations of the intentions or behaviour of another entity* (the trustee).[6]

In the context of identity management, trust is typically understood in its operational sense.[7] From this perspective, an entity can be said to trust a second entity when it makes the assumption that the second entity or system will behave exactly as it expects.[8] Or when, in absence of such an assumption, it demonstrates the willingness to assume the risk associated with the transaction in spite of the absence of certainty (e.g., when relying on the validity of a credential once an established authentication protocol has been completed). In other words, the term 'trust' in this context mainly refers to confidence in one's expectations.[9]

Establishing trust, especially in the private sphere, often proves quite difficult in practice. Making trust decisions is particularly difficult in a digital environment, when people want (or need) to interact with people or organizations they have never met, and have little time to get to know at a personal level.[10] Nevertheless, trust is a crucial aspect for many online interactions, both from a

---

[4] D.M. Rousseau, S.B. Sitkin, R.S. Burt and C. Camerer, 'Not so different after all: a cross-discipline view of trust', Introduction to Special Topic Forum, *Academy of Management* Review, 1998, Vol. 23, No. 3, p. 394.

[5] See for example D. Gollman, 'Why trust is bad for security', *Electronic Notes in Theoretical Computer Science* 2006, vol. 157, 3-9.

[6] D.M. Rousseau, et al., 'Not so different after all: a cross-discipline view of trust', l.c., p. 395. See also J. Dumortier, N. Vandezande, C. Hochleitner and K. Fuglerud, 'D.7.1 Legal Requirements for Trust in the IoT', uTRUSTit Deliverable, 2011, p. 7 et seq., available at http://www.utrustit.eu.

[7] J.C. Buitelaar, M. Meints and E. Kindt (eds.) 'D16.3 Requirements for Identity Management in eGovernment', FIDIS Deliverable, 2009, p. 13, available at www.fidis.net (hereafter: 'FIDIS 16.3').

[8] *Id.* Definition based on Lead Study Group on Telecommunication Security, Security Compendium Part 2 - Approved ITU-T Security Definitions, available at http://www.itu.int/ITU-T/studygroups/com17/def005.doc, last consulted 10 March 2009, p. 51 and L.G. Zucker, 'Production of trust: Institutional sources of economic structure, 1840-1920', in B.M. Staw and L.L. Cummings (ed.), *Research of organizational behavior*, JAI Press Inc., Londen, 1986, p. 53-111, and S. Slone (ed.), *Identity Management. A white paper*, 2004, available at http://www.opengroup.org/onlinepubs/7699959899/toc.pdf, last consulted 15, February 2009.

[9] This is essentially trust in the broadest sense of the word. See also N. Luhmann, 'Trust - a mechanism for the reduction of social complexity', in *Trust & Power - Two works by Niklas Luhmann*, UMI Books on Demand (reprint of John Wiley & Sons), Michigan, published 1993, p. 4 (original publication dates 1973 and 1975 resp.).

[10] FIDIS 16.3, *o.c.*, p. 13; Slone, S. (ed.), *o.c.*, p. 7. There are countless factors influencing trust: context, reputation, user knowledge, branding… (see e.g. E. Costante, J. den Hartog, and M. Petkovic, 'On-line Trust Perception: What Really Matters', in *Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust*, Milan, Italy, 2011, p. 53-54). Trust is also by its nature subjective. what one individual

user as well as from a service provider perspective: both parties want to be confident that the transaction will be completed to their mutual satisfaction.[11]

In recent years, several initiatives have been undertaken to develop mechanisms that might establish or enhance trust in online digital identities. Initially, these initiatives were undertaken primarily in the context of industry-led consortia and standardization fora.[12] With the rise of eGovernment, many EU Member States started to develop identity and information security management frameworks of their own[13]; often drawing inspiration from those industry-led precursors.[14] Recently, the concept of an 'identity trust framework' has emerged as a vehicle to outline the various components that are deemed necessary to establish trust in online digital identities.[15] While the stated objectives of each instantiation of the trust framework concept may vary, they often seek to promote:

1. interoperability (even in absence of a pre-existing 'trust relationship' among each of the actors involved);
2. scalability (by minimizing the need for bilateral agreements and contracts among the relevant actors);
3. a certain degree of compliance assurance (i.e. induce a certain degree of confidence that stated policies of the trust framework as well as relevant legal requirements will be complied with).

Although a myriad of definitions have been proffered, the Identity Management Legal Task Force of the American Bar Association has eloquently summarized the (identity) trust framework concept as follows:

> "*Trust Frameworks specify the requirements and rules that govern participation and outline the processes and procedures that provide mutual assurance between participants with respect to a particular functional*

considers to be an essential requirement when making trust decisions, will differ from what other individuals perceive as an essential trust requirement. Trust is also not transitive: if I trust you, and you trust person X, it does not necessarily follow that I also trust person X (but knowledge of our respective trust relationship might go a long way in establishing trust between me and person X). See also GINI D1.1, section 4.4.

[11] FIDIS 16.3, *o.c.*, p. 13; X. Huysmans and B. Van Alsenoy, 'Conceptual Framework for Identity Management in eGovernment and Requirements Study', Deliverables 1.1 and 1.3 of the IBBT project 'IDEM' (Identity Management for eGovernment), 2007, p. 103.

[12] See e.g. the Kantara Initiative (http://kantarainitiative.org) (successor of the Liberty Alliance: http://www.projectliberty.org) and the Identity Commons (http://www.idcommons.org). More recent initiatives include the Open Identity eXchange (http://openidentityexchange.org) and OASIS IDtrust (http://www.oasis-idtrust.org).

[13] See e.g. J. Deprest and F. Robben, 'eGovernment: the approach of the Belgian federal administration', 2003, available at https://www.law.kuleuven.be/icri/frobben/publications/2003%20-%20E-government%20paper%20v%201.0.pdf.

[14] Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', in Van der Hof, S. and Groothuis, M.M. (eds.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government*, Information Technology and Law Series, Volume 20, T. M. C. Asser Press, The Hague, The Netherlands, p. 258

[15] See e.g. M. Rundle (ed.), 'Open Identity Trust Framework (OITF) Model', March 2010, available at http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/oitf.aspx (last accessed 18 February 2012); The White House, *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011, Washington, p. 25, available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (last accessed 18 February 2012); DLA Piper, Sealed, Time.Lex, Price Waterhouse Coopers SG&A, 'D1.1 IAS in the European policy context' (draft version), *Study on an electronic identification, authentication and signature policy (IAS) project*, p. 3 et seq., available at http://www.iasproject.eu/docs.html.

online system. An Identity Trust Framework is just one of several types of special application trust frameworks that might be utilized in the context of an online transaction."[16]

In this chapter, we will investigate the identity trust framework concept further by analysing the key elements, actors and issues which have been associated with this concept. The purpose of this exercise is to help identify the core components of such trust frameworks, so as to enable an evaluation of areas in which the current EU regulatory framework displays certain gaps towards establishing trust in online digital identities.

2.2 Core components

Trust frameworks come in many shapes and sizes. The amorphous nature of the trust concept allows for easy integration of basically anything within the context of a trust framework: issues related to entity authentication assurance, privacy, general security practices, the availability of redress mechanisms, etc. The actual scope of any given trust framework is generally context-specific (and often closely related to what is being marketed). In practice, the actual components of a given trust framework are mainly determined by the predominant views regarding the key concerns of the various stakeholders involved. From a formal perspective, however, it is possible to discern two general categories of components which appear to be present in every trust framework, namely[17]:

1) the *technical specifications and operational rules* necessary to make the system functional and trustworthy, and
2) the *legal rules* that define the rights and legal obligations of the parties and facilitate enforcement where necessary.

In case of an identity trust framework, these two core components can be elaborated a bit further as follows:

'*An identity trust framework is the underlying [governance] structure developed for the day-to-day operation of a specific identity system, consisting of:*

- *the Technical and Operational Specifications that have been developed:*
  - *to define the requirements for the proper operation of the identity system (i.e., so that it works),*
  - *to define the roles and operational responsibilities of participants, and*
  - *to provide adequate assurance regarding the accuracy, integrity, privacy and security of its processes and data (i.e., so that the various parties are willing to participate; so it is trustworthy); and*
- *the Legal Rules that:*
  - *regulate the content of the Technical and Operational Specifications,*
  - *make the Technical and Operational Specifications legally binding on and enforceable against the participants, and*
  - *define and govern the legal rights, responsibilities, and liabilities of the participants of the identity system.*'[18]

Over the following sections, we will attempt to conceptualize the key actors (section 2.3) and issues (section 2.4) involved in the development and implementation of an identity trust

[16] ABA Identity Management Legal Task Force, 'Identity Trust Framework', Discussion Draft, June 15, 2011, 1, available at http://apps.americanbar.org/dch/committee.cfm?com=CL320041 (last accessed 15 October 2011).
[17] *Ibid*, 2.
[18] *Id.*

framework. The purpose of this exercise is to identify the key functional, legal and trustworthiness issues involved in the development of a PIM ecosystem, as well as provide an adequate basis for our subsequent discussion of the regulatory options towards the development of the PIM ecosystem envisaged by GINI (chapter 3).

2.3 Key actors

Just as there is no definitive list of the constitutive elements of a trust framework, there is also no definitive list of actors involved in the implementation of every trust framework. From a conceptual perspective, however, it is possible to distinguish among a number of actors and roles; which each have the potential of fulfilling a crucial role in the implementation of an identity trust framework. For purposes of clarity, it is useful to present these actors in terms of the '*layers*' at which they are expected to operate within a given identity ecosystem. Building on the conceptualization developed in the context of the National Strategy for Trusted Identities in Cyberspace (NSTIC) [19], three such layers can be distinguished:

1. a **governance layer**: this is the layer where the rules and policies of the ecosystem are established;
2. an **administration** (or 'management') layer: this is the layer where adherence to the rules and policies which have been established for the ecosystem is overseen, and if necessary, enforced;
3. an **operational** (or 'execution') layer: this is the layer where transactions occur in accordance with the rules of the trust framework.[20]

Each layer of an identity ecosystem comprises one or more actors, which each have their own role(s) and responsibilities. Over the following sections, we will attempt to conceptualize the basic types of actors encountered at each layer, accompanied by a brief elaboration of their role. The reader should keep in mind, however, that the number and types of actors encountered at each layer may, in practice, vary considerably among trust frameworks. The following overview merely serves to provide a basis for our later analysis.

[19] This representation of the identity ecosystem is an adaptation of the model found in the draft 'National Strategy for Trusted Identities in Cyberspace. Creating Options for Enhanced Online Security and Privacy' [NSTIC], which was issued by the US Department of Homeland Security (DHS) in June 2010, at p. 14 (currently still available at: http://www.dhs.gov/xlibrary/assets/ns_tic.pdf). This model was not retained in the final version of the NSTIC (see The White House, *National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy*, April 2011, Washington, available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf). We have chosen to retain it here as we find it is useful to describe the relationship between trust frameworks and the law (cf. *infra*; section 3.1). Kindred models to the one described here have been elaborated by other bodies such as the Kantara Initiative (see http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0), OpenID Foundation, the Information Card Foundation, and OIX (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.

[20] See also J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', *Trusted Architecture for Securely Shared Services (TAS³)*, third iteration, p. 92, available at www.tas3.eu.

2.3.1 Governance layer

The governance layer consists of the actors and interactions that *establish the rules* of an identity ecosystem.[21] In other words, it comprises those entities that act as 'rule-makers' under a particular (identity) trust framework. Such entities have been referred to collectively as 'policymakers'[22], 'governance authority'[23], or 'governance board'[24].

The role of the actors presiding at the governance layer is to define the requirements, policies and procedures that will be implemented under a trust framework. More specifically, their role is to establish and adopt inter alia[25]:

- the criteria (standards) which entities must meet if they want to exercise certain privileges within the ecosystem (e.g., participation, provisioning of a specific service);
- how these criteria will be assessed (e.g. self-assessment, gap analysis, independent audit, etc.);
- the rules which must be adhered to by the various participants when interacting with one and other within the ecosystem;
- rules, procedures and processes that must be followed by the actors charged with administration of the rules it has adopted.

The decisions adopted at the governance layer will specify the requirements for the administration and operational layers of the ecosystem (cf. *infra*). One should note that the level and nature of involvement of the actors presiding at the governance layer can also vary significantly.[26] In addition, the rules that apply to a particular ecosystem can also take on a myriad of forms. Such rules may take the form of codes of conduct, contracts, standards, legislation, etc.[27]

In case of legislation, there also exists a broad variety in the extent to which the rules are specifically designed to impact the functioning of a particular ecosystem or trust framework. For instance, the bulk of consumer protection legislation applies across sectors. Save for certain exceptions, it in principle applies regardless of whether a transaction takes place in an online or offline environment. As a result, if a particular digital ecosystem entails interaction among consumers and businesses, such legislation will in principle apply. More often than not, however,

---

[21] We do not expect that in practice there would be just one well-defined trust framework or ecosystem; but rather a plurality of frameworks and ecosystems. However, we have chosen, for purposes of simplification and conceptual clarity, to refer to "the" trust framework / identity ecosystem within this section.

[22] M. Rundle (ed.), 'Open Identity Trust Framework (OITF) Model', *l.c.*, p. 2.

[23] US Department of Homeland Security, Draft 'National Strategy for Trusted Identities in Cyberspace. Creating Options for Enhanced Online Security and Privacy', *l.c.*, p. 13.

[24] J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', *l.c.*, p. 93.

[25] Based on J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', *l.c.*, p. 93.

[26] Such actors might include private companies, legislators, regulators, self-regulatory organisations, co-regulatory organisations … who may either have power to adopt rules which shall apply to the activities that take place within the ecosystem or merely be involved in a consultative status (e.g., as members of an advisory board).

[27] In other words, the 'Legal Rules' mentioned in section 2.1 may consist of a combination of (a) existing statutes and regulations ('formal' law' or 'law on the books') and (b) self-regulation ('privately created law') (e.g. agreements between or among the participants of the ecosystem). See also ABA Identity Management Legal Task Force, 'Identity Trust Framework', *l.c.*, 3 and T. J. Smedinghoff, 'What Is an Identity Trust Framework? Addressing the Legal and Structural Challenges', available at http://meetings.abanet.org/webupload/commupload/CL320041/relatedresources/4-Trust-Framework-and-Liability-Overview.pdf (last accessed 15 October 2011), slides 7-16.

relevant legislation will not be tailored towards the implementation context of a particular trust framework. For this reason, a trust framework shall often involve one or more actors which act as additional rule-makers for the ecosystem in question, whose role consists of 'operationalizing' (at least a portion of) the relevant laws (i.e. translating the law on the books to rules which are more meaningful/readily applicable to the ecosystem in question) or complementing (or supplementing) such laws with additional rules (e.g., as needed to make the ecosystem function smoothly).[28]

Under a more narrow view of the trust framework concept, the governance layer consists only of those rule-making entities which are charged specifically with developing rules for the ecosystem to which it pertains. From this viewpoint, 'external' sources of rules (e.g., legislative bodies) would not be considered part of the governance layer of a particular trust framework as such. The entities residing at the governance layer of the trust framework would then (also) carry a de facto responsibility of 'internalizing' the relevant external requirements into the rules that they decree for the ecosystem in question (at least insofar as these external rules are directly applicable to the operations that take place within the ecosystem in question).[29]

2.3.2 Administration layer

The administration layer consists of the actors and interactions which seek to ensure that the rules decreed at the governance layer are applied and enforced within the ecosystem. Specifically, the actors involved at the administration layer are charged with ensuring that the relevant rules, policies, and procedures are observed by the actors of the operational layer.

The type and number of actors involved at the administration layer will depend on the nature of the trust framework and its implementation context. Almost all identity trust frameworks assume the presence of one or more entities that assume the following functions:

- a general **'operator' function**, which comprises activities related to the general administration and management of the trust framework[30] (e.g., ensuring appropriate implementation of rules/decisions decreed at governance layer, oversight of other actors involved at the administrative layer, etc.);

[28] The policymakers may of course be supported by any number of entities acting in an advisory capacity (e.g., advisory board, ethics committee and support staff); which may comprise relevant stakeholders who are not necessarily represented in the decision-making process through which rules are formally adopted.

[29] See also *infra*; section 3.4.1.

[30] This entity is sometimes also referred to as the 'Trust Network Operator (TNO)' (see J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', *l.c.*, p. 96); 'Federation Operator' (see J. Nigriny, R. Sabett, 'The Third-Party Assurance Model: A legal framework for federated identity management', *Jurimetrics Journal* 2010, vol. 50, p. 509); 'OITF Providers' (see M. Rundle (ed.), 'Open Identity Trust Framework (OITF) Model', *l.c.*, p. 3). or 'Trust Framework Provider (TFP)' (see e.g. Center for Democracy and Technology [CDT], 'Issues for responsible User-Centric Identity', November 2009, v 1.0, 2, available at http://www.cdt.org/paper/issues-responsible-user-centric-identity, last accessed 11 October 2011. Note however that in the CDT model the TFP also assumes rule-making and accreditation functions. In this regard it is important to note that this Operator function in principle can, but need not necessarily coincide with 'INDI Operator' role described in GINI D1.1 / D3.1. The level of involvement of the Operator in actual data processing operations may vary. Furthermore, depending on the breadth of powers that reside with the Operator, it may be necessary to appoint yet another entity that is charged with (a portion of) administration of the trust framework in order to ensure an appropriate separation of duties and to avoid conflicts of interest.

- an **accreditation function**, which comprises the activities related to validation and formal recognition of entities as being eligible (and authorized) participants in the ecosystem under the conditions of the trust framework, or as being otherwise entitled to exercise certain privileges (e.g., to display a certification of conformity)[31];
- an **oversight function**, which comprises activities related to compliance monitoring and dispute resolution for the operations that take place at the operational layer (e.g. audit of transactions, complaint handling).[32]

It is important to note that, at least in theory, each of the aforementioned functions can be concentrated within one entity, or assumed by several different entities (which could potentially either be agents of the entity assuming the operator function, or independent actors, which may or may not be directly appointed by actors presiding at the governance layer).

A second important observation pertains to the breadth and rigor with which the aforementioned functions can be exercised. For instance, participation in an ecosystem under a particular trust framework might be contingent upon validation and certification by an independent agent[33], or alternatively, be contingent upon a mere self-assertion of compliance[34]. The choice for any given implementation model will undoubtedly impact the threshold for participation and associated cost (both for prospective participants as well as for the administration of the trust framework). But perhaps more importantly, this choice is also bound to impact the overall perception of trustworthiness by (and of) the actors involved in the ecosystem (e.g., separation of duties between, on the one hand, entities involved in accreditation and, on the other hand, entities charged with ongoing compliance monitoring may influence the trust framework's credibility) (see also *infra*; section 2.4.3). As far as oversight and dispute resolution is concerned, again a variety of potential configurations are imaginable. Investments could be made to establish an independent alternative dispute resolution (ADR) mechanism, which would allow participants (end-users and/or service providers) to resolve potential issues within the context of the trust framework itself, before escalating matters with the relevant administrative or judicial authorities. On the other end of the spectrum, it could also be possible for the participants of the trust framework to rely entirely upon traditional dispute resolution mechanisms. Again the choice for either model is bound to impact the overall cost associated with the trust framework, as well as

---

[31] Such actors have been referred to as 'accreditation authority' (J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', *l.c.*, p. 99; US Department of Homeland Security, Draft 'National Strategy for Trusted Identities in Cyberspace. Creating Options for Enhanced Online Security and Privacy', *l.c.*, p. 14); 'assessors' (M. Rundle (ed.), 'Open Identity Trust Framework (OITF) Model', *l.c.*, p. 3).

[32] Such actors have been referred to as 'accountability & oversight committee' (J. Alhadeff and B. Van Alsenoy (eds.), 'Deliverable 6.2 Contractual Framework', p. 100), 'auditors' and 'dispute resolvers' (M. Rundle (ed.), 'Open Identity Trust Framework (OITF) Model', *l.c.*, p. 3).

[33] An example of such an approach was provided by the Pathfinder Privacy Projects under the APEC Privacy Framework: when a company wishes to demonstrate its compliance with the APEC Privacy Framework, they are expected to first develop a CBPR (i.e. a set of 'Cross-Border Privacy Rules'). The company is then expected to go through an application and vetting process, during which the company must complete an evaluative process related to both to the compliance of their CBPR with the Framework and their capacity to comply with their own CBPR. The accreditation and oversight of the CBPR is administered either by a local agency or authority of a participating Economy, or by an accountability agent. (J. Alhadeff, B. Van Alsenoy and J. Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', paper presented at the Privacy and Accountability conference organized by the PATS project in Berlin, 5-6 April 2011 (proceedings pending), draft version available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1933731.

[34] An example of this approach is the US Safe Harbor framework. See http://export.gov/safeharbor/ and http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm.

the degree of 'customer satisfaction' of end-users and service providers that participate in the ecosystem.[35]

2.3.3 Operational layer

The operational layer of an identity ecosystem is the layer where the actual transactions occur among the entities participating in the trust framework. Provided that the mechanisms put in place at the governance and administration layers are effective, these transactions should occur in accordance with the rules applicable within the trust framework (emanating from legislation, relevant standards, codes of conduct, …; cf. *supra*; 2.3.1).

The operational layer of the PIM ecosystem envisaged by GINI comprises multiple actors. When looking at our initial conceptualization of actors which was conducted in the context of D1.1 and D3.1[36], the following categories of actors can be distinguished:

- **INDI Users**: these are the end-users of an INDI, typically also the entities to whom the identities or other attributes relate in the context of an authentication protocol. Within the PIM ecosystem, INDI Users can act in various roles (e.g., citizen, employee, or customer). In principle, the user chooses in which role to act and whether or not to authorize the release of certain identity or attribute information.[37] The user is theoretically also able to manage its partial identities similarly with the physical world, by providing the relevant information to each situation.[38]

- **Data Sources**: these are the entities (e.g., a digital service, repository, administrative body, company) (through) which (an individual or organization) make(s) a claim(s) about some individual, organization, device or service.[39]

- **INDI Operators**: these are the entities (e.g., a service provider, software component) which provide INDI Users with the basic INDI functionality, namely the ability to disclose/present information about themselves ('claims') which is (are) maintained in one or more Data Sources, to Relying Parties.[40] The main role of the INDI Operators is to act as trust mediators. Their services are designed to provide other entities within the PIM ecosystem with the assurances they need in order to enable the disclosure and reliance upon identity information, even where the parties involved do not have pre-established trust relationships.[41]

- **Relying parties**: these are the entities (legal entities or a physical persons) with which INDI Users wish to perform one or more transactions for personal, business or official purposes. One of the most prominent functionalities of the PIM ecosystem is that it

[35] See also *infra*; section 2.3.3.

[36] See in particular section 5.3 of D1.1 and section 2.3 of D3.1.

[37] Keeping in mind of course, that the actual freedom of choice will be constrained by the requirements/expectations stipulated by the Relying Party or implementation context. In practice, failure to provide requested information will very often result in an inability to complete the envisaged transaction.

[38] See also GINI D4.1, section 3.2.

[39] *Id.* In the context of federated identity management, these entities are also often referred to as 'Identity Providers' and/or 'Attribute Providers/Authorities'.

[40] See also GINI D3.1, section 2.3.

[41] See also GINI D3.1, section 2.3.

> allows its users to present information about themselves in a verifiable fashion, i.e. in a manner which provides relying parties with appropriate assurance regarding the authenticity of the data that is presented (i.e. that the data originates from the identified source and has not been manipulated during the transmission).[42]

The extent to which a given trust framework regulates the activities of the participants to a particular identity ecosystem can vary considerably. Some trust frameworks regulate the conduct of all the participants involved in the ecosystem, including end-users.[43] Other trust frameworks, such as those governing the use of 'trust marks' or 'seals', typically focus primarily on the conduct of the entities that are displaying the trust mark or seal.[44]

Note:

The actors involved at the operational layer of the PIM ecosystem shall hereafter be referred to collectively as 'participants' in our discussion of the key issues related to the development and implementation of an identity trust framework.

2.4 Key issues

The purpose of this section is to outline the main issues for consideration in the development and implementation of an identity trust framework. Whereas the previous section provided a conceptual outline of the different types of actors and their roles, this section seeks to address the core issues that underlie an identity trust framework from a substantive perspective, i.e. in terms of the objectives it seeks to achieve and the safeguards that may be put in place in order to (reasonably) guarantee that these objectives may be realized in practice.

The reader will notice that there is a considerable overlap among the categorization of issues presented below. There are mainly two reasons for this. In first instance, this overlap is attributable to the amorphous nature of the concepts which have been used as the basis for this categorization (i.e. 'functional requirements', 'legal aspects' and 'trustworthiness'). A second reason for overlap resides in the fact that the implementation mechanisms which serve to address these issues are very often interrelated.[45] The reason why we have adopted this approach, despite the clear overlap, is to present the key issues from various perspectives. In doing so, we hope to provide a more comprehensive overview of the main functional, legal and other normative issues which need to be considered during the development of an identity trust framework.

---

[42] See also GINI D3.1, section 2.3 and GINI D4.1, section 3.2.

[43] ABA Identity Management Legal Task Force, 'Identity Trust Framework', *l.c.*, 2.

[44] *Id.*

[45] Consider the following example: the issue of whether or not a particular authentication protocol satisfies an entity authentication assurance requirement (LoA – Level of Assurance) is a 'functional' requirement. However, whether or not such a requirement is considered to be fulfilled may depend in part on whether or not there was appropriate separation of duties (e.g., between the credential issuer and the auditor), whereas this aspect is very often also categorized as a 'trustworthiness' issue. Finally, the actual rigor with which a relying party imposes a given entity authentication assurance requirement may be influenced by its ability to obtain appropriate redress in case of erroneous authentication; which is in turn dependent upon the 'legal' safeguards which are in place.

2.4.1 Functional requirements

In the case of identity trust frameworks, one of the main objectives is to establish trust in identity assertions, i.e. to provide the relevant stakeholders (relying parties in particular) with confidence that the identity assertions received are sufficiently reliable for their intended purposes.[46] However, trust and interoperability typically require more than a common understanding about the assurance levels supported by the various credentials at hand.[47] In the FIDIS project, four generic 'elements of trust' were identified, which need to be addressed within a (federated) eGovernment context.[48] These elements can in fact, for purposes of our current analysis, be generalized as core functional requirements when seeking to develop a trustworthy identity management framework. These elements are:

1. Trust in **identification, authentication and non-repudiation mechanisms**: this implies inter alia trust in the uniqueness of identifiers, credential management processes, the security ('strength') of authentication and/or signature protocols, etc.;

2. Trust in the **accuracy and integrity of data**: this trust element refers to the accuracy and integrity of assertions (or any other type of digital claim) made with regards to individual (or group of) entities (which are typically offered by so-called 'identity providers' and/or 'authoritative sources'[49]);

3. Trust in the **reliability, availability and performance** of the (identity management) systems of (and protocols executed by) other entities involved in any particular communication or transaction;

---

[46] ABA Identity Management Legal Task Force, 'Identity Trust Framework', *l.c.*, 1. In a federated environment, this is typically done by establishing and agreeing upon a certain number of entity authentication assurance levels (usually four); which each stipulate a number of technical and organizational requirements related to the authentication processes. [Note: these requirements are usually not limited to the phase of actual entity authentication (e.g., when a user 'logs on' to a system), but typically also concern initial registration (or 'enrollment'), credential management (e.g., personalization, issuance, activation), etc]. This approach is designed to help decision-makers assess what types of authentication mechanisms are appropriate for which applications, and whether or not reliance on a particular eID solution is suitable for their purposes. By agreeing upon a set of baseline requirements for each LoA, actors which do not have a pre-established trust relationship can make better informed decisions about whether or not to accept the credentials issued by a third party (See also GINI D3.1, 31-33).

[47] GINI D3.1, 32.

[48] See FIDIS D16.3, *o.c.*, 13-15.

[49] In many documents authoritative sources are also referred to as 'authentic' sources or 'authentic registers'. We have chosen to use of the term 'authoritative' as it is more in line with identity management literature and because we believe the term 'authoritative' better captures their actual role (it reflects the idea that they are seen as trustworthy within a certain context). Moreover, use of the term 'authentic' may also in the long run engender confusion with notions such as 'authentication' or 'data authenticity' in the way traditionally used in computer sciences. On the use of 'authentic' sources as part of the pan-European eIDM framework, see European Commission, Information Society and Media Directorate-General, eGovernment Unit, 'A Roadmap for a pan-European eIDM Framework by 2010', v1.0, 5, available at http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf (last accessed 26 October 2011) (Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', *l.c.*, at note 14).

4. Trust in **compliance with established policies, including data protection and privacy policies**: this element of trust refers to the expectancy that each party will properly adhere to required, agreed or stated policies such as data handling policies, access control policies, pseudonym management, etc.

There are a variety of mechanisms through which the aforementioned trust requirements can be met. The actual needs may vary dramatically according to the application envisaged.[50]

A key question, which is also related to the issue of trustworthiness (cf. *infra*; section 2.4.3), concerns the enforcement and oversight of trust framework policies which have been stipulated in relation to these functional requirements.[51] There exist, as indicated earlier, a wide range of potential implementation models to address each of these elements.[52] Finley Peter Dunne has been attributed with saying "*Trust everybody, but cut the cards*".[53] This is a different way of saying that while a basic attitude of openness and good faith is inherently good[54], one must at the same time ensure that appropriate mechanisms are in place to prevent (or at least deter) a violation of the trust that is given. Regardless of the commitments that are made by the participants of a particular identity ecosystem (be they of an operational, technical or legal nature), additional measures may be necessary to realize actual trust from the perspective of individual stakeholders.[55] One very important factor in providing assurance that the participants shall abide by their commitments and obligations is the presence of a comprehensive legal framework. The main legal issues which need to be addressed by this framework will be further elaborated in the following subsection.

[50] FIDIS D16.3, *o.c.*, 14.

[51] Or, to phrase the question in terms of the 'layers' of a particular identity ecosystem, a key issue is how the actors involved at the administration layer(s) will ensure that the rules decreed at the governance layer(s) are applied and enforced within the ecosystem. Cf. *supra*; section 2.3.2.

[52] Cf. *supra*; section 2.3.2. For instance, the satisfaction of LoA requirements may theoretically range from complete self-assertion (no external validation or oversight whatsoever) to third-party audit and certification (comprehensive validation and oversight) (See also GINI D3.1, p. 32). Similarly, the validation of adherence to the relevant requirements can take place on an ex ante (prior accreditation) and/or ex post (supervision and monitoring) basis. The breadth and rigor with which oversight and enforcement mechanisms are exercised will impact, as indicated earlier: (a) the threshold for participation; (b) the associated cost (both for prospective participants as well as for the administration of the trust framework) and (c) the overall perception of trustworthiness by (and of) the actors involved in the ecosystem.

[53] See http://en.wikipedia.org/wiki/Finley_Peter_Dunne.

[54] Luhmann eloquently summarized why trust is an inevitable component of social interaction as follows: '*In many situations, of course, man can choose in certain respects whether or not to bestow trust. But a complete absence of trust would prevent him even from getting up in the morning. He would be prey to a vague sense of dread, to paralysing fears. He would not even be capable of formulating definite distrust and making that a basis for precautionary measures, since this would presuppose trust in other directions. Anything and everything would be possible. Such abrupt confrontation with the complexity of the world at its most extreme is beyond human endurance.*' (N. Luhmann, 'Trust – a mechanisms for the reduction of social complexity', *l.c.*, p. 4.)

[55] See also *infra*; section 2.4.3. An exception to this rule shall apply where the entity making the commitments has such standing that the other stakeholders are willing to rely upon self-assertion (which may or may not be additionally contingent upon the availability and effectiveness of recourse mechanisms that would allow them to hold the asserting entity accountable in case of non-compliance).

2.4.2 Legal aspects

The implementation of an identity trust framework presents, in addition to technical and economic challenges, a number of legal challenges.[56] Smedinghoff has articulated four categories of legal risks which must be considered in the context of federated identity management.[57] This categorization will serve as the baseline for our analysis of the main legal issues presented by the PIM ecosystem in this deliverable. [58] The four categories of legal risks are[59]:

1. Privacy risk
2. Authentication risk
3. Liability risk
4. Performance risk

Each of these risks affects all participants of the PIM ecosystem, albeit in different ways. As a result, each of these actors may potentially have conflicting needs and goals with respect to how these risks should be addressed.[60] Over the following subsections, we will outline the main legal issues which need to be considered when addressing these risks, as well as the main interests of the participants of the PIM ecosystem in this respect.

2.4.2.1Privacy risk

Identity management systems, be they of a user-centric or other nature, entail processing of personal data. From a data subject's ('INDI User') perspective, the main concern in relation to privacy relates to the processing of their personal data.[61] In order to participate in the PIM ecosystem (i.e. engage in transactions with other participants), individuals will need to disclose a certain amount of their personal data. Which data is necessary for a particular transaction will generally be context-specific, but in each instance the data subject will arguably require ('some')

[56] See also T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", Draft Paper, 21 August 2009, p. 15 et seq., available at http://meetings.abanet.org/webupload/commupload/CL320041/relatedresources/Identity-Management-Legal-Background-Paper.pdf (last accessed 12 October 2011).

[57] The legal issues involved in federated identity management are largely the same as those involved in user-centric identity management (despite the fact that each model brings about its own specific considerations). In fact, every user-centric IdM solution proposed to date requires some form of federation in order for its implementation to be successful. The most notable difference between the two approaches is the emphasis on user involvement and/or control in the case of user-centric IdM.

[58] We refer the reader to GINI D3.1 for a more detailed description of the main legal barriers and gaps in relation to the development of a PIM ecosystem under the current EU regulatory framework. Several of the issues highlighted in GINI D3.1 are intertwined with the ones listed here (e.g., the authentication and liability risk are closely related to the obligations of data controllers under the Data Protection Directive; see in particular sections 4.3 and 4.8 of D3.1). However, the categorization proffered by Smedinghoff is useful to provide a more general and systematic overview of the legal issues involved in the development of a PIM ecosystem, which is why we have chosen to adopt it here. Where appropriate, references to the corresponding legal analysis in GINI D3.1 shall be made in footnotes.

[59] T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 15. Conflicting interests may also exist among the actors involved in the governance and administration layer, which is why it is important to ensure that an appropriate governance framework is in place which takes these conflicts into account. Cf. *infra*; section 2.4.3 and section 3.

[60] T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 15.

[61] *Ibid*, 16.

assurance that their data will be processed in an appropriate manner, and that recourse mechanisms will be available to them when necessary.[62]

As for the other participants to the PIM ecosystem (INDI Operators, Data Sources and Relying Parties), the privacy risk is closely related to their compliance obligations under data protection and privacy law. Each of these entities is responsible for ensuring that the processing, which takes place under their control, complies with the requirements set forth by Directive 95/46/EC (provided such processing falls within the scope of this instrument[63]). It is expected that each of the aforementioned entities shall be considered to be acting as a 'controller' in relation to several of the processing operations which take place within the context of the PIM ecosystem envisaged by GINI.[64] As a result, each of these actors may be subject to data protection obligations to a greater or lesser extent, but each have a vested interest in ensuring that the processing takes place in a compliant manner.[65] Notwithstanding these vested interests, the nature of the activities of these entities is typically such that their overall interests may conflict with the data subject's privacy interests.[66]

2.4.2.2 Authentication risk

A second legal risk category concerns the authentication risk. This risk in first instance refers to the potential adverse impact resulting from erroneous authentication of one of the actors participating in the identity ecosystem. This risk is strongly intertwined with a number of the functional requirements identified above (cf. *supra*; section 2.4.1), and is also strongly connected to the 'liability risk' (see below). However, it is important to emphasize that, in addition to the relevant functional requirements and liability risks, there are also independent legal provisions which impose upon actors a duty to appropriately authenticate entities that seek to perform a particular operation (e.g., access a particular resource, obtain attestation of a particular attribute). Data controllers, for instance, are obliged to ensure the confidentiality and security of processing.[67] This obligation entails that, whenever a resource contains personal data, the controller must put in place appropriate technical and organizational safeguards. These measures should particularly ensure that the processing capabilities (read, write, modify …) of each entity

[62] *Ibid*, 16-17.

[63] See GINI D3.1, section 4.2. For purposes of our current analysis we again make abstraction of the fact that the Relying Party may in principle also be another INDI User who may in certain instances benefit from the personal use exemption.

[64] It may reasonably be expected that both the provider (Data Source) and recipient (Relying Party) of the data shall in principle each act as a data controller in relation to their own processing operations: the storage of data by a Data Source shall in principle be the result of its own business purpose(s) or public mission. Similarly, the Relying Party to whom the data is made available will be collecting these data for its own purposes. The INDI Operators, who will fulfil primarily an intermediary function, shall in principle be considered to act as controllers in relation to the processing operations for which they exercise a determinative influence, though the actual scope of their responsibility will depend heavily on the actual implementation model. See also GINI D3.1, section 4.3.1.

[65] For an example of how these interests might play out see GINI D3.1, section 4.6.2 (describing the implications of the finality principle towards Data Sources and Relying Parties).

[66] See also T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 16. Whether and how these (potentially conflicting) are resolved under a particular identity trust framework will depend largely on the scope and breadth of the framework, which is strongly related to the issue of governance (cf. infra; *section* 2.4.3).

[67] See GINI D3.1, section 4.8.

that has the ability to access this resource are limited to that which is necessary to realize the goals of the processing.[68]

In the context of the PIM ecosystem envisaged by GINI, the obligation to ensure the security of processing shall in principle be the shared responsibility of the Data Sources, INDI Operators and Relying Parties that participate in a given transaction.[69] Again, each of these actors shall therefore have a vested interest in ensuring that authentication of participants to the PIM ecosystem takes place in a secure (and compliant) manner. From the perspective of the INDI User (data subject), the authentication risk is both a data protection (e.g., will someone be able to steal my identity?) and business concern (e.g., will I be able to complete a particular online transaction?).[70] From the perspective of Relying Parties, appropriate authentication of individual entities is (in addition to a compliance obligation) primarily a business concern (e.g., what economic harm may I suffer in case of wrongful authentication?), but also a liability concern (e.g., what is my liability exposure if I provide access to sensitive personal information, mistakenly believing that the requestor was the data subject to whom the information relates?).[71] Data Sources shall typically experience business and liability concerns similar to those experienced by Relying Parties, but may also face an additional risk of liability exposure in case of wrongful attestation of an entity's identity or attribute (see also below). Finally, the INDI Operators' concern in relation to the authentication risk will be primarily of a business nature (as part of its core business will be to maintain trust in the identity ecosystem), but they too may also face additional liability risks to the extent that it attests to the accuracy, validity and/or authenticity of an asserted claim.

It is important to note that the (legal) authentication risk is not limited to entity authentication alone. Certain transactions require the use of electronic signatures which enjoy legal validity or special legal recognition (e.g., in the context of eProcurement).[72] The authentication risk also extends to these types of transactions, but currently revolves more around the implementation of appropriate data origin authentication (rather than just entity authentication) mechanisms.[73] The main interests of the respective participants in the PIM ecosystem are however largely the same as those identified in the previous paragraph.

2.4.2.3Liability risk

There are many things that can go wrong within a PIM ecosystem. Potential liability exposure typically results from faulty identification and/or authentication, inadequate security, misuse of personal data, or, more generally, a failure to follow appropriate procedures[74] (whose normativity may result either from legal requirements, voluntarily accepted obligations and/or general standards of diligent behavior ['*bonus pater familias*']). This can lead to the following two primary harms[75]:

[68] GINI D3.1, section 4.8.1.
[69] GINI D3.1, section 4.8.2.
[70] See also T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 17.
[71] See also T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 18.
[72] Concerning the regulation of electronic signatures at EU level see GINI D3.1, section 7.
[73] Concerning the conceptual distinction between entity authentication and data origin authentication see also GINI D3.1, section 7.9.
[74] T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 21.
[75] *Id.*

1. A Relying Party and/or INDI User may suffer damages when the Relying Party acts
    a. in reliance on a false (or compromised) credential or assertion which it believed to be valid (e.g., by granting access to an impostor) or
    b. fails to rely upon a valid credential or assertion that it mistakenly believes to false or compromised

2. An INDI User may suffer damages when
    a. his or her personal data is misused or compromised or
    b. he or she is denied authorization to conduct a transaction he or she would otherwise be entitled to

From a legal perspective, a key issue is which entity will bear the liability risks (exposure) in relation to the harms mentioned above. Will the Data Source in question bear (all of) the liability exposure related to erroneous representation of an identity of an INDI User, and the subsequent harm suffered by Relying Parties and/or INDI Users?[76] In theory, a wide range of potential models are conceivable. For instance, a Relying Party could rely upon an eID solution 'as is' (without any ability of recourse even if the Data Source does not abide by the agreed upon its stated practices); the Data Source might agree to indemnify Relying Parties to a certain amount (capped liability); an objective liability of the Data Source might be installed, there might be a pooled liability scheme jointly funded by the participants in the PIM ecosystem, etc.[77] The configuration of these parameters will influence both the trust decisions of relying parties, as well as the willingness of Data Sources to make their data available to third parties (even with user authorization). Absence of (legal) certainty in this regard may pose a considerable barrier to interoperability and the development of mutual trust relationships.[78] This issue will be revisited at the end of the following subsection.

2.4.2.4Performance risk

A fourth legal risk category is performance risk. For each participant to the PIM ecosystem, the actual benefits of participation depend on each of the other participants proper performance of

[76] For a more comprehensive overview of the key liability questions see also Center for Democracy and Technology [CDT], 'Issues for responsible User-Centric Identity', *l.c.*, 7-8. For an outline of the various bases of liability exposure see T. J. Smedinghoff, 'What Is an Identity Trust Framework? Addressing the Legal and Structural Challenges', available at http://meetings.abanet.org/webupload/commupload/CL320041/relatedresources/4-Trust-Framework-and-Liability-Overview.pdf, in particular slides 20 et seq. As the issue of liability is also closely related to the question of the overall scope of a given identity trust framework, this issue shall be revisited in the context of our discussion of the key governance issues. Cf. *infra*; section 2.4.3.

[77] Numerous theories have been advanced to clarify the source and scope of potential liability exposure in relation to the harms presented above: see T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 22 (concluding that, at the end of the day, the legal liability risk remains somewhat uncertain).

[78] See also GINI D3.1, section 4.8.3. In GINI D3.1 we concluded that in case of a 'closed' system (i.e. a system which is based on voluntary agreements between a specified number of participants) the requisite legal certainty can in principle be established through contractual means. See also GINI D3.1, section 7.12. However, as will be discussed in the following subsection, current mechanisms (such as contractual frameworks) do not always appear apt to the task of appropriately balancing the (sometimes conflicting) interests of the participants to the PIM ecosystem. Cf. *infra*; section 2.4.2.4.

certain basic obligations that are fundamental to the proper functioning of the ecosystem.[79] The failure of any participant to perform one of its basic obligations could lead to substantial harm to other participants in the ecosystem.[80] While securing the performance of these obligations is strongly intertwined with the liability risk, it is worth outlining the main performance obligations which need to be fulfilled in order for the PIM ecosystem to be successful.[81] This outline will be structured according to the main performance obligations of the various participants to the PIM ecosystem (i.e. in terms of the actors involved at the 'operational layer'). The following performance obligations may be discerned[82]:

1. ***INDI User***
    a. Provide accurate information about himself/herself both during initial enrolment and subsequent transactions (to the extent that self-assertion is allowed);
    b. Protect the credentials he/she uses within the PIM ecosystem (insofar as they reside under his/her control) (e.g., by undertaking appropriate steps in case of compromise);
    c. Comply with terms of use as stipulated by other participants of the PIM ecosystem (and as agreed to by the INDI User), as well as directly applicable legal requirements.

2. ***Data Source***
    a. Implementation of appropriate identity and/or attribute management processes;
    b. Protect the credentials it uses within the PIM ecosystem (insofar as they reside under its control);
    c. Ensure that the data it maintains concerning INDI Users remains accurate and up-to-date, and only make accurate representations about INDI Users when disclosing information towards other participants of the PIM ecosystem;
    d. Accommodate data subject rights (e.g., right of access, rectification and/or blocking);
    e. Appropriately protect the privacy and security of the INDI User's personal data (as well as comply with all other obligations resulting from data protection legislation);
    f. Comply with stated policies, requirements decreed at governance layer(s) (e.g., requirements issued by the governance authority relating to assurance levels, attribute disclosure policies, etc.), as well as directly applicable legal requirements.

3. ***INDI Operator***
    a. Deliver the basic INDI functionality, i.e. facilitate disclosure/presentation of information about INDI User which is maintained in one or more Data Sources for the benefit of Relying parties (e.g., by providing (or at least identifying) the appropriate technical interface to process the user-authorized disclosure of personal data);

[79] Based on T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 23.

[80] *Id.*

[81] In GINI D3.1, we already provided a basic outline of the (trust) relationships among the various participants in the PIM ecosystem. See GINI D3.1, section 2.3. The overview provided here is based primarily Smedinghoff's risk categorization, supplemented by the findings of GINI D3.1.

[82] Most (if not all) of these performance obligations are logical extensions of the four functional requirements articulated above (cf. *supra*; section 2.4.1).

b. Properly authenticate claims and credentials coming from the participants of the PIM ecosystem (INDI Users, Data Sources, Relying Parties, other INDI Operators);
c. Protect the credentials it uses within the PIM ecosystem (insofar as they reside under its control);
d. Limit use and reliance upon identity/attribute assertions as appropriate for the circumstances (e.g. do not facilitate or otherwise enable the disclosure of personal data of INDI Users unless authorized by them or as required by a legal obligation to which the INDI Operator is subject);
e. Appropriately protect the privacy and security of the INDI User's personal data (as well as comply with all other obligations resulting from data protection legislation);
f. Comply with stated policies, as well as requirements decreed at governance layer(s) (e.g., legal requirements, requirements issued by governance authority relating to assurance levels, attribute disclosure policies, etc.).

4. Relying Party

a. Properly authenticate claims and credentials[83];
b. Protect the credentials it uses within the PIM ecosystem (insofar as they reside under its control);
c. Limit use and reliance upon identity/attribute assertions as appropriate for the circumstances;
d. Appropriately protect the privacy and security of the INDI User's personal data (as well as comply with all other obligations resulting from data protection legislation);
e. Comply with stated policies, as well as requirements decreed at governance layer(s) (e.g., legal requirements, requirements issued by governance authority relating to assurance levels, attribute use and disclosure policies, etc.).

The legal framework that governs the PIM ecosystem will need to address each of the aforementioned legal risks in an appropriate manner in order to provide a durable and scalable solution. Specifically, it will need to clearly define the obligations of each actor, and to utilize a (set of) mechanism(s) (whether they be of a statutory, (quasi-)contractual, and/or technological nature) that provide (at least 'some') assurance that the participants will perform the obligations corresponding to their role(s).[84] Where they fail to do so, appropriate redress mechanisms should be in place to mitigate the harm suffered.[85] The latter aspect is important not just from the perspective of the individual entity that actually experienced the harm, but also with a view of maintaining the overall trust in the PIM ecosystem. Traditionally, the approach towards securing adequate performance of these obligations has been primarily of a (quasi-)contractual nature (e.g., terms of use, service level agreements, certificate practice statements, etc.), which sit within the context of the existing legal framework(s) (thereby in principle ensuring remedy in case of default of e.g. a contractual commitment). However, it would appear as if the mechanisms which have

[83] Even in case of a mediated trust relationship, whereby the trustworthiness of certain claims or credentials for the Relying Party is established through the intervention of the INDI Operator, it may be expected that the Relying Party will still need to verify that the interventions which have been (allegedly) performed by a particular INDI Operator were in fact performed by this entity.

[84] T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, 24.

[85] *Id.*

been developed so far do not always provide solutions that adequately safeguard the (often competing and sometimes even conflicting) interests of the participants to the ecosystem.[86]

While the availability of legal remedy can play an important role in safeguarding participants' trust, there are many additional elements which are bound to impact their actual trust perception. Most of these elements are not strictly legal in nature. Several of them pertain to how the implementation of the trust framework is organized, and the nature of the safeguards which are in place to ensure that the system as a whole is in fact trustworthy. In the following subsection we will highlight, from a high level, some additional elements which are bound to impact the trustworthiness of a given trust framework implementation.

2.4.3 Trustworthiness

As indicated above, the main objective of a trust framework is to provide participants in a given (eco)system with adequate assurances with respect to the proper functioning of the system.[87] These assurances in turn serve to make the system 'trustworthy' to such an extent that the participants of the ecosystem will feel comfortable engaging in transactions with one and other.[88] In the previous subsections, we outlined a number of functional requirements and legal aspects which need to be addressed during the development of an identity trust framework. However, even if a given trust framework comprehensively addresses each of these issues, it may still not be sufficient to secure its trustworthiness. The reason for this is that actual trustworthiness cannot be ensured by commitments or legal obligations alone. The purpose of this section is to briefly elaborate upon a number of elements which should be explicitly considered during the development of an identity trust framework, preferably at the outset. When reviewing these elements, it is important to keep in mind that the decision of which model is appropriate for a particular context may vary. However, it is possible to identify a number of themes which will need to be addressed during the development of almost any identity trust framework (even if in some instances certain aspects are eventually considered to be 'out-of-scope' or only addressed in minimalistic fashion). In particular, the following issues need to be considered[89]:

1. **Criteria for participation**: on what basis (if any) will entities be admitted/excluded from (certain activities that take place within) the PIM ecosystem? For instance, which requirements shall be imposed upon entities that wish to act as Data Sources (e.g., adherence to specific trust framework policies such as entity authentication assurance requirements) and/or as Relying Parties (e.g., demonstration of compliance with data protection requirements, adoption of particular technological safeguards)?

[86] See T. J. Smedinghoff, 'Federated Identity Management: Balancing Privacy Rights, Liability Risks and the Duty to Authenticate", *l.c.*, p. 28 et seq. (discussing inter alia the EU E-Signatures Directive, unilateral assertion models and contractual models). For a more economic perspective on the issues relating to the quality of standards in the certification services market see J. Backhouse, C. Hsu, J. C. Tseng and J. Baptista, 'A Question of Trust - An economic perspective on quality standards in the certification services market', *Communications of the ACM* 2005, vol. 48, No. 9, 87-91.

[87] Cf. *supra*; section 2.1.

[88] The transactions for which assurance is provided, the scope of assurance, as well as the actual level of assurance proffered by a given trust framework will depend on the nature and scope of the trust framework and its implementation. For a basic outline of the (trust) relationships among the participants to the INDI ecosystem see GINI D3.1, section 2.3.

[89] Based primarily on Center for Democracy and Technology [CDT], 'Issues for responsible User-Centric Identity', *l.c.*, 7.

2. **Setting trust framework policy**: which entity or entities will actually set the 'rules' for the PIM ecosystem (e.g., specification of entity and data authentication protocols; interpretation of relevant data protection and privacy requirements for purposes of transactions that take place within the ecosystem; updating of technical and organizational requirements to ensure interoperability, etc.)? Will this be done by the participants to the ecosystem themselves? Will there be any direct involvement of governmental agencies in this rule-making process (and if so, to what extent)? Will there be any representation for (or consultation of) external or internal stakeholders (e.g., consumer protection agencies, data protection authorities, etc.)?

3. **Scope of trust framework (policies)**: what shall be the envisaged scope of applicability of the trust framework and the policies it adopts? Which type of (trans)actions does the trust framework seek to address? For instance, will it only stipulate requirements in relation to entity authentication, or will it also articulate requirements in terms of data handling (e.g., by adopting specific data protection standards)? Will such requirements only apply to defined transactions among participants to the ecosystem, or will such requirements also relate to subsequent data handling (e.g., further processing by the Relying Party once it has received the data)?

4. **Accreditation, oversight and enforcement**: Will there be a formal intake and accreditation process for entities that wish to participate in the ecosystem? With which amount of rigor will the criteria for participation be validated? What will be the impact of formal accreditation? For instance, will there be an ecosystem-wide list of recognized Data Sources? If so, which warranties will accreditation entail (if any)? Will there be any internal oversight ('policing') for the ecosystem? Will participants be expected to demonstrate compliance on an ongoing basis? If so, how? (e.g., use of online compliance testing (OCT) mechanisms, on-site auditing, self-assertion/notification)?[90]

5. **Separation of duties**: How will an appropriate separation of duties among the actors involved at the respective layers be ensured? Should the trust framework define certain restrictions to avoid conflicts of interest (e.g., by restricting the ability of actors involved at the operational layer to also be involved in tasks of the administrative or governance layer)?

6. **Nature of the relevant (legal) instrument(s)**: what should be the nature of the legal instrument(s) that bind the participants to the ecosystem to adhere to the trust framework policies and requirements? What should be the nature of the legal instrument that binds the entities involved at governance and/or administrative layer (e.g., statute, articles of incorporation, contracts, memoranda of understanding, …)?

7. **Accountability mechanisms**: what mechanisms shall be put in place to ensure that each of the participant's abide by its obligations and stated practices? For instance, will transparency-enhancing mechanisms be put in place to allow verification of compliance by individuals? Will an independent body be entrusted with compliance verification, or will the participants "police themselves"?

8. **Conflict resolution**: should any additional dispute resolution mechanisms be put in place to allow for (initial) internal mediation of complaints? On what basis will conflicts be resolved (e.g., verification of audit trail)? How will redress be organized?

[90] See also *supra*; section 2.3.2.

3 Regulatory tools at EU level

The overall objective of this deliverable is, as mentioned in the introduction, to outline areas in which further regulation or other policy initiatives may be needed in order for

1. an operator-driven[91] infrastructure across EU borders to be established and function smoothly
2. in a manner that guarantees privacy, gives choices to individuals, and
3. allows institutional actors to oversee the respect and enforcement of legal rules to the benefit of the public interest and the private interests of individuals.

It is beyond the scope of this deliverable to advance a definitive normative position as to which type of regulatory intervention is best suited to realize the GINI vision. There are several reasons for this. The first reason is that such a position, as will become apparent over the following subsections, requires a detailed examination of the underlying market conditions and the interests of the relevant market players.[92] Second, much will depend on the (subjective) perception regarding the extent to which a particular regulatory strategy may be seen as effective in aligning reality with a given public policy objective. Third, many of the issues highlighted in the previous section are not strictly legal in nature. Rather, they concern policy and/or business decisions which need to be considered by the designers of a particular trust framework. Finally, as highlighted throughout this deliverable, the choice for any particular implementation model will generally depend on context-specific elements (e.g., is the Data Source a governmental agency?, what is the nature of the data that will be processed within the ecosystem/transaction in question?).

Notwithstanding these considerations, we do consider that there is merit in further exploring the regulatory tools and policy options that exist, particularly those available to EU policy-makers. The purpose of this section is to outline the logical steps to be completed when evaluating the need for regulation, as well as to articulate a number of principles that may help guide decision-makers to select the appropriate policy option. Once this analysis has been completed, we will proceed to provide an outline of the main areas in which regulatory is deemed appropriate in our chapter on Recommendations (chapter 4).

---

[91] The PIM ecosystem envisioned by GINI is based on a network of Operators. The main role of these ('INDI') Operators is to act as trust mediators. Their services are designed to provide other entities within the PIM ecosystem with the assurances they need in order to enable the disclosure and reliance upon identity information, even where the parties involved do not have pre-established trust relationships. As described in GINI D3.1, the INDI Operator is to be seen as a 'logical entity', which could in principle both be a separate legal entity which is charged with performing certain processing operations, but it could also be a purely technical application (e.g. a software component which runs locally on a device controlled by the INDI User). Naturally, the choice for either implementation model will have substantial privacy ramifications. See also GINI D3.1, section 2.2.

[92] See also Ofcom (UK Office of Communications), 'Initial assessments of when to adopt self- or co-regulation - Consultation', 27 March 2008, p. 9, available at http://stakeholders.ofcom.org.uk/binaries/consultations/coregulation/summary/condoc.pdf (last accessed 10 January 2011).

In its White Paper on European Governance[93], the European Commission put forward certain principles which should be taken into account whenever the adoption of regulation is being considered. It outlines three major steps which need to be completed when evaluating the need for regulatory intervention, which shall be further elaborated over the following sections[94]:

1. **Step 1: Assess the need for (and impact of) regulation.** This question should be answered based on the analysis of its impact, costs and benefits. As the European Commission put it:

   "*Proposals must be prepared on the basis of* ***an effective analysis*** *of whether it is appropriate to intervene at EU level and whether regulatory intervention is needed. If so, the analysis must also assess the potential economic, social and environmental impact, as well as the costs and benefits of that particular approach*".[95]

2. **Step 2: If regulatory action is required, select the appropriate policy instrument.** One of the starting points of the aforementioned White Paper was the idea that the European Community should follow a less top-down approach and complement its policy tools more effectively with non-legislative instruments.[96]As the European Commission put it

   "***[L]egislation is often only part of a broader solution*** *combining formal rules with other non-binding tools such as recommendations, guidelines, or even self-regulation within a commonly agreed framework. This highlights the need for close coherence between the use of different policy instruments and for more thought to be given to their selection*".[97]

3. **Step 3: Determine which actors should be involved in the regulatory process.** The White Paper emphasizes that wide participation throughout the policy chain is crucial.[98] The involvement of civil society, effective and transparent consultation, and dialogue are considered key elements to achieve this. This principle has gained importance, particularly in environments where the addressees of (possible) regulation are numerous, widespread and very active.

[93] Commission of the European Communities, 'European Governance – A White Paper', COM (2001) 428 final, 25 July 2001.

[94] The White Paper on European Governance also outlines additional steps and principles, of which the main elements have, for purposes of conceptual clarity, been incorporated in the subsequent sections.

[95] Commission of the European Communities, European Governance – A White Paper, *l.c.*, p. 20 (original emphasis).

[96] *Ibid*, p. 4.

[97] *Ibid*, p. 20 (original emphasis). The OECD has similarly stressed that "*[r]egulators should carry out, early in the regulatory process, an informed comparison of a variety of regulatory and non-regulatory policy instruments, considering relevant issues such as costs, benefits, distributional effects, and administrative requirements*". (OECD, Recommendation of the Council on improving the quality of government regulation, 1995, available at http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=128&InstrumentPID=124&Lang=en&Book=False (last accessed 9 January 2012).

[98] Commission of the European Communities, European Governance – A White Paper, *l.c.*, p. 10.

3.1 Assessing the need for (and impact of) regulation

Before adopting regulation, policymakers should carefully consider the questions of 'whether regulation is necessary' and 'what to regulate exactly'.[99] In market regulation, *evidence-based* approaches have been promoted for several years, which require legislators and regulators to carefully consider whether there is a market failure which needs to be addressed and, if so, whether a legislative or regulatory intervention is the best way to deal with the concern.[100]

In deciding whether to adopt regulations, legislators at EU level expected to examine the potentials costs and benefits of such an intervention, by means of so-called '*regulatory impact assessments*' (RIAs).[101] In the Interinstitutional Agreement on Better Lawmaking (IABL), the use of impact assessments is put forward as positively contributing to the improvement of the quality of Community legislation.[102] In 2009, the European Commission published their '*Impact assessment guidelines*'.[103] The guidelines define an impact assessment as

> '*a set of logical steps to be followed when you prepare policy proposals. It is a process that prepares evidence for political decision-makers on the advantages and disadvantages of possible policy options by assessing their potential impacts*'.[104]

They key analytical steps to be executed in the course of an RIA are:

1. Identifying the problem
2. Defining the policy objectives
3. Developing main policy options
4. Analyzing the impact of the options
5. Comparing the options

---

[99] As the OECD put it in 1995: "*Government intervention should be based on clear evidence that government action is justified, given the nature of the problem, the likely benefits and costs of action (based on a realistic assessment of government effectiveness), and alternative mechanisms for addressing the problem*". (OECD, Recommendation of the Council on improving the quality of government regulation, 1995).

[100] In its Smart regulation in the European Union Communication, the European Commission stated that evidence-based policy making is considered good practice. (European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Smart regulation in the European Union, COM (2010) 543 final, 8 October 2010, p. 2.)

[101] RIAs can also lead to the 'evidence' required in an evidence-based regime. See OECD, 'Draft recommendation on regulatory policy and governance', *l.c.*, p. 12: "*Improving the evidence base for regulation through ex ante impact assessment of new regulations is one of the most important regulatory tools available to governments*"; "*RIA improves the use of evidence in policy making, allows for a proportionate response to an identified problem and reduces the incidence of regulatory failure arising from regulating when there is no case for doing so, or failing to regulate when there is a clear need*".

[102] European Parliament, Council, and Commission, Interinstitutional agreement on better law-making, 2003/C 321/01, *OJ* 31.12.2003, C 321, paragraph 28. The OECD has also recommended to "Integrate regulatory impact analysis into the development, review, and revision of significant regulations, and use RIA to assess impacts on market openness and competition objectives; support RIA with training programmes, and with ex post evaluation to monitor quality and compliance; include risk assessment and risk management options in RIAs. Ensure that RIA plays a key role in improving the quality of regulation, and is conducted in a timely, clear and transparent manner". (OECD, 'Guiding principles on regulatory quality and performance', 2005, p. 4, available at http://www.oecd.org/dataoecd/24/6/34976533.pdf) . This was emphasized again in its most recent Draft recommendation on regulatory policy and governance (p. 5).

[103] European Commission, Impact assessment guidelines, 15 January 2009, , available at http://ec.europa.eu/governance/impact/index_en.htm.

[104] European Commission, Impact assessment guidelines, *l.c.*, p. 4.

6. Outlining policy monitoring and evaluation

The guidelines also provide detailed descriptions of how to implement each of these steps.[105]

Without going into further detail on each of the analytical steps which EU institutions need to complete in the context of an RIA, it is worth emphasizing that the first option for decision-makers to consider is to simply not undertake any (additional) regulatory action. According to the Commission's Regulatory Impact Assessment Guidelines '*the option of 'no EU action' must always be considered as a viable option, except in cases where the Treaties lay down a specific obligation to act*'.[106] This requirement stems from two basic principles of EU law, namely the principles of subsidiarity and proportionality (see art. 5 TEU). These principles entail that both (a) the choice of the level at which action is taken (from EU to local) and (b) the selection of the instruments used must always be in proportion to the objectives pursued.[107] As a result, decision-makers must, before launching an initiative, systematically check
(1) if public action is really necessary,
(2) if the European level is the most appropriate one, and
(3) if the measures chosen are proportionate to those objectives.[108]

EU policymakers should particularly refrain from regulatory intervention where:
1. markets are able to deliver required outcomes (i.e. citizens and consumers are empowered to take full advantage of the products and services and to avoid harm)[109] or
2. national regulation by Member States provides a satisfactory result, without posing an obstacle to EU policy objectives (e.g., free movement of goods and services within the internal market).

3.2 Choosing the appropriate option

Once the need for regulation has been established, policy-makers then need to consider which type of regulatory measure would be most appropriate to address this need. Regulation can take many different forms. The purpose of this subsection is to elaborate further on the range of initiatives which might be taken at EU level, together with a number of considerations that may help guide decision-makers to select the appropriate option. For the purposes of our current discussion, we distinguish between two general of categories of measures available to EU policymakers: legislative measures and non-legislative measures.[110] The reader should note that the use of the term 'legislative' does not mean that all of the relevant rules are developed by a legislative or regulatory body alone. It merely signifies that such measures have a stronger nexus with the legislative framework, in that they imply the adoption of one or more legally binding instruments by a governmental body.

[105] See European Commission, Impact assessment guidelines, *l.c.*, p. 21 et seq..
[106] European Commission, 'Impact assessment guidelines', *l.c.*, p. 30.
[107] Commission of the European Communities, 'European Governance – A White Paper', *l.c.*, p. 10-11.
[108] *Id.*
[109] Ofcom, 'Initial assessments of when to adopt self- or co-regulation - Consultation', *l.c.*, p. 7.
[110] There exists a vast body of academic theory concerning regulation, with many different types of categorization (see E. Lievens, *Protecting Children in the Digital Era – The Use of Alternative Regulatory Instruments*, Martinus Nijhoff Publishers, International Studies in Human Rights, Leiden, 2010, p. 143 et seq.)

3.2.1 Non-legislative measures

There exists a wide variety of non-legislative measures available to EU policymakers. Article 288 TFEU mentions two types of non-legislative instruments (recommendations and opinions), but there are far more such instruments in use.[111] The following subsections provide a (non-exhaustive) overview of non-legislative measures used by EU institutions and how they can be applied.

3.2.1.1 Instruments

Recommendations are measures which, even as regards to the entities to whom they are addressed, are not intended to produce binding effects. [112] They are generally adopted by EU institutions[113] when they do not have the power under the Treaties to adopt binding measures or when they consider that it is not appropriate to adopt more mandatory rules.[114] *Opinions* are also non-legislative acts, very often preparatory acts which form one step in the procedure leading to the adoption of a definitive act.[115] Additional non-legislative instruments employed at EU include: *notices*, *communications*, *guidelines, frameworks*, *action plans* and *white papers*.

3.2.1.2 Use

Each of the aforementioned instruments may serve a variety of purposes: to articulate objectives, to spur relevant stakeholders towards action, to describe the kind of Member State measures to be compatible with Community law in a given area, to present legislative proposals or areas of future legislative action, etc.[116]

A specific form of non-legislative Community Action which merits further elaboration is the so-called '*Open Method of Co-ordination*' (OMC). OMC is a form of policymaking which consists of the development of (non-binding) political targets, which are accompanied by benchmarks and monitoring mechanisms to evaluate the progress towards achieving those targets.[117] It is a way of

---

[111] P. J. G. Kapteyn, A.M. McDonnell a.o. (eds.), *The Law of the European Union and the European Communities*, Alphen a/d Rijn, Kluwer law international, 2008, fourth revised edition, p. 290 (in reference to ex Article 249 TEC).

[112] See also K. Lenaerts and P. Van Nuffel, *European Union Law*, London, Sweet & Maxwell, 2011, p. 919 (citing ECJ, Case C-322/88 *Grimaldi* [1989], E.C.R. 4407, paras 13 and 16.

[113] Recommendations are adopted by the Council or, in the specific cases provided by the Treaties, by the Commission or the European Central Bank (see art. 292 TFEU).

[114] K. Lenaerts and P. Van Nuffel, *o.c.*, p. 919. Recommendations do not create rights upon which individuals may rely before a national court as such. However, the ECJ has stipulated that national courts are bound to take recommendations into consideration when deciding disputes (in particular where they cast light on the interpretation of national measures adopted in order to implement them or when they are designed to supplement binding Union provisions). (*Id.*)

[115] P. J. G. Kapteyn, A.M. McDonnell a.o. (eds.), *o.c.*, p. 290. However, opinions are sometimes also used as a means to provide guidance to Member States or other entities, in which case it may stand alone as a definite act (with or without legal effect). See e.g. the opinions adopted by the Commission in the context of Directive 2006/95/EC: http://ec.europa.eu/enterprise/sectors/electrical/documents/lvd/guidance/opinions/index_en.htm.

[116] P. J. G. Kapteyn, A.M. McDonnell a.o. (eds.), *o.c.*, p. 292. See e.g. Commission of the European Communities, 'Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)', Brussels, 2 May 2007, COM(2007) 228 final.

[117] See P. Craig and G. de Búrca, *EU Law – Text, Cases and Materials*, Oxford, Oxford University Press, 2007, Fourth Edition, p. 150 et seq.; S. Borrás and K. Jacobsson, 'The open method of co-ordination

encouraging co-operation and the exchange of best practice among Member States.[118] Use of OMC is perceived as being particularly useful under conditions of local and regional diversity and under conditions in which problems are volatile.[119] Use of OMC may also provide the basis for determining whether legislative or programme-based action is needed to overcome particular problems highlighted.[120]

The *promotion of self-regulation* is another type of policy measure which can be used at EU level. Self-regulation covers a large number of practices, common rules, codes of conduct and voluntary agreements by which economic actors, social players, NGOs and other organised groups establish themselves voluntarily to regulate and organise their activities.[121] While self-regulation, by definition, implies a voluntary accord among the actors involved, EU institutions may nevertheless play an important role in stimulating self-regulatory initiatives.[122]

Self-regulation is often heralded by proponents for its flexibility, its higher degree of incorporated expertise, lower cost, greater incentives towards compliance, and that it might be better suited to address global issues.[123] Opponents criticize self-regulatory mechanisms for reasons including: lack of effective enforcement (mild sanctions, if any, and reluctant enforcement); low level of transparency, accountability, proportionality and consistency; advancement of private over public interests; and that it may lead to cartel-like agreements that close markets.[124] It has also been characterized as 'a cynical attempt by self-interested parties to give appearance of regulation (thereby warding off more direct and effective government regulation) while serving private interests at the expense of the public'.[125] Whether or not self-regulation is an appropriate option to consider in practice largely depends on the existence of bodies and processes to support self-regulation, as well as their ability to build consensus amongst market players and to impose

---

and new governance patterns in the EU', *Journal of European Public Policy* 2004, 185–208 and A. Héritier, 'New Modes of Governance in Europe: Policy-Making without Legislating?', Renner Institut, Max Planck Project Group, 2001, available at http://www.renner-institut.at/download/texte/heritier.pdf (last accessed 17 January 2012).

118 Commission of the European Communities, 'European Governance – A White Paper', *l.c.*, p. 21.

119 A. Héritier, 'New Modes of Governance in Europe: Policy-Making without Legislating?', *l.c.*, p. 5.

120 Commission of the European Communities, 'European Governance – A White Paper', *l.c.*, p. 22.

121 European Commission, 'Part III: Annexes to the Impact Assessment Guidelines', 15 January 2009, p. 24, available at http://ec.europa.eu/governance/impact/commission_guidelines/docs/ia_guidelines_annexes_en.pdf (last accessed 18 January 2012). See also *supra*; section 3.2.1.

122 See Commission of the European Communities, 'Communication from the Commission: Action plan "Simplifying and improving the regulatory environment"', Brussels, 5 June 2002, COM(2002) 278 final, p. 11: "The Commission can consider it preferable not to make a legislative proposal where agreements of this kind already exist and can be used to achieve the objectives set out in the Treaty. It can also suggest, via a recommendation for example, that this type of agreements be concluded by the parties concerned to avoid having to use legislation, without ruling out the possibility of legislating if such agreements prove insufficient or inefficient." See also L. Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?', ECJL 2005, vol. 9.1, available at http://www.ejcl.org/91/art91-3.html#N_1_ (last accessed 17 January 2012). Article 27 of the Data Protection Directive explicitly calls upon the Member States and the Commission to 'encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.'

123 E. Lievens, *o.c.*, 203-204.

124 *Ibid*, 205-206.

125 *Ibid*, 206, citing N. Gunningham and J. Rees, 'Industry self-regulation: an institutional perspective', *Law & Policy* 1997, vol. 19, no. 4, p. 370.

effective monitoring and enforcement mechanisms.[126] Additional success factors to be considered are: operational objectives and clearly defined responsibilities, transparent regulatory processes and measurable results, defined fall back scenarios in case of malfunction, adequate sanction powers, periodical reviews and external control by the general public and the state, and participation possibilities for interested stakeholders.[127]

Finally, the Commission's RIA Guidelines also highlight *better enforcement and implementation* as means to achieve the desired policy objective.[128] Where legislation already is in place, creating a new instrument may not be the best remedy.[129] Alternatively, the relevant institutions (e.g., data protection authorities) could issue additional guidance to help steer private or public actors towards the desired outcome.

3.2.2 Legislative measures

In the previous subsection we outlined a number of non-legislative measures available at EU level. Each of those measures may be characterized as 'soft law', in that they have no direct binding legal effect vis-à-vis the entities addressed in and of themselves. The purpose of this section is to briefly elaborate upon the range legislative measures available to EU decision-makers. As indicated earlier, the use of the term 'legislative' does not mean that all of the relevant rules are developed by a legislative or regulatory body alone – merely that they imply the adoption of one or more legally binding instruments by a governmental body.[130]

---

[126] European Commission, 'Part III: Annexes to the Impact Assessment Guidelines', *l.c.*, p. 24. See also Ofcom, 'Initial assessments of when to adopt self- or co-regulation - Consultation', *l.c.*, p. 4:
'*Self-regulation is more likely to be effective in those markets where:*
- *companies recognise that their future viability depends not only on their relationship with their current customers and shareholders, but also they operate in a environment where they have to act responsibly within the societies in which they operate; and*
- *companies recognise and acknowledge the identified problems which may cause harm or market failure that impede citizens or consumers; and*
- *companies individually and collectively acknowledge the need to reduce the identified harm or market failure, since this will improve the ability of those companies to determine the interests of citizens or consumers and, potentially, society as a whole.*

This is more likely to be where citizens or consumers and all other individuals share common views as to the merits of regulating the activities of companies to achieve a particular social objective. A market environment with an active industry participation and/or cohesiveness is most likely to administer effective self-regulation as industry participants are more likely to commit financial resources, consult with stakeholders and monitor the effectiveness of self-regulation. Thus, self-regulation is less effective where there is a broad spread of smaller businesses that do not communicate with each other and have little resources to commit.'

[127] M. Latzer, 'Trust in the industry – Trust in the users: self-regulation and self-help in the context of digital media content in the EU, Report for working group 3 of the Expert conference on European media policy "More trust in content – The potential of co- and self-regulation in digital media", Leipzig 9-11.05.2007, p. 56.

[128] European Commission, 'Impact assessment guidelines', *l.c.*, p. 30.

[129] *Id.*

[130] See also *infra*; section 3.4.

3.2.2.1Instruments

Article 288 TFEU mentions three types of legislative instruments: regulations, directives and decisions. Each of these instruments may in principle serve as (1) legislative acts, (2) acts implementing legislative acts or (3) acts implementing other implementing acts.[131]

A *regulation* has general application, is binding in its entirety, and is directly applicable in all Member States (art. 288, § 2 TFEU).[132] The fact that regulations by definition have a general scope of application differentiates it from a decision which may have an individual scope.[133] They differ from directives in the fact that they are binding in their entirety, as directives are in principle only binding as to the result to be achieved.[134] Use of regulations is deemed appropriate in cases where there is a need for uniform application and legal certainty across the Union.[135]

Directives are binding as to the result to be achieved, upon each Member State to which it is addressed, but leave national authorities the choice of form and methods on how to achieve this result (art. 288, § 3 TFEU). By leaving the Member States a certain amount of discretion in how to achieve the intended result within the national legal system, directives also reflect the idea of subsidiarity.[136] They are perceived as appropriate instruments for introducing EU rules which call for existing national provisions to be amended or fleshed out before the new rules can be applied.[137]

A *decision*, like a regulation, is binding in its entirety. However, unlike regulations, decisions may also be addressed to specific entities. A decision which specifies to whom it is addressed is only binding upon them (art. 288, § 4 TFEU).[138] Decisions can be used to adopt individual administrative acts, in which case they serve to apply Community law in a specific case.[139] They can however also have a general scope.[140] Decisions may be addressed to individuals and Member States alike.[141]

---

131 K. Lenaerts and P. Van Nuffel, *o.c.*, p. 885. This provision also gives an incomplete picture of the range of legal instruments which are used in practice in the EU. Most of the other types of instruments in use are of a non-legislative nature (cf. *supra*), however some of them do have binding force (see P. J. G. Kapteyn, A.M. McDonnell a.o. (eds.), *o.c.*, p. 276) In principle the EU institutions are free to choose which instrument to use, as long as they act in accordance with treaty provisions (i.e. on the basis of conferred powers). In certain instances a Treaty provision may prescribe use of a certain type of instrument (see P. J. G. Kapteyn, A.M. McDonnell a.o. (eds.), *o.c.*, p. 275).

132 'General application' means that it is "applicable to objectively determined situations and involves legal consequences for categories of persons viewed in a general and abstract manner". (K. Lenaerts and P. Van Nuffel, *o.c.*, p. 893, citing ECJ, Case 6/68 *Zuckerfabrik Watenstedt v Council* [1968] E.C.R. 409, at 415.

133 *Ibid*, p. 894. While a regulation may, in practice, despite its general scope of application, affect only a limited number of entities, it will not lose its character as regulation 'as long as there is no doubt that the measure is applicable as the result of an objective situation of law or of fact which it specifies and which is in harmony with its ultimate objective' (*Id.*)

134 P. J. G. Kapteyn, A.M. McDonnell a.o. (eds.), *o.c.*, p. 280.

135 Commission of the European Communities, 'European Governance – A White Paper', *l.c.*, p. 20.

136 K. Lenaerts and P. Van Nuffel, *o.c.*, p. 886.

137 *Id.*

138 K. Lenaerts and P. Van Nuffel, *o.c.*, p. 915.

139 P. J. G. Kapteyn, A.M. McDonnell a.o. (eds.), *o.c.*, p. 287.

140 K. Lenaerts and P. Van Nuffel, *o.c.*, p. 916.

141 *Ibid*, 917.

3.2.2.2 Use

Each of the aforementioned legislative instruments can be used in a variety of ways. The RIA guidelines outline the following types of legislative initiatives[142]:

1. *'Cross-cutting' legislative action*, such as regulations and directives that address broad issues and are likely to have significant impacts on a wide range of stakeholders across different sectors (e.g., the Data Protection Directive);
2. *'Narrow' legislative action* in a particular field or sector, and unlikely to have significant impacts beyond the immediate policy area;
3. *Expenditure programmes*: decisions to establish or renew spending programmes (e.g., the Decision to establish the IDABC programme[143]);
4. *Comitology decisions*: different executive initiatives defined by the procedure of adoption (e.g., Commission Regulation implementing Directive 2005/32/EC with regard to ecodesign requirements for external power supplies).

Annex 7 to the RIA Guidelines additionally considers the use of legislative instruments for purposes of establishing a framework for *co-regulation*.[144] Co-regulation combines binding legislative action with actions taken by relevant stakeholders.[145] It implies involvement of both governmental authorities and other stakeholders (e.g. industry, civil society) in the regulatory process. Within the EU context, co-regulation has been defined as

> '*a mechanism in which a Community legislative act entrusts the attainment of the objectives defined by the legislator to parties which are recognized in the field (such as economic operators, the social partners, non-governmental organisations, or associations)*'.[146]

This approach implies the adoption of a legislative instrument which sets forth a regulatory framework, in which typically the deadlines and mechanisms for implementation, the methods of monitoring the application of the legislation and any sanctions are set out.[147] In addition, the co-regulatory framework should[148]:

---

[142] European Commission, 'Impact assessment guidelines', *l.c.*, p. 15.

[143] Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC), 18 May 2004, L 181, p. 25-35.

[144] European Commission, 'Part III: Annexes to the Impact Assessment Guidelines', *l.c.*, p. 26 et seq.

[145] Commission of the European Communities, 'European Governance – A White Paper', *l.c.*, p. 21. See also supra; section 3.2.1.

[146] Paragraph 18 of the IABL. Most authors consider co-regulation as a special type of self-regulation, whereby the self-regulatory framework is 'anchored' within the regulatory framework (public sector regulations) in one of two ways: (a) either a public authority provides a legal basis for the self-regulatory framework so that it can begin to function ('top-down approach'), or (b) it integrates (part of) an existing self-regulatory system within the regulatory framework ('bottom-up approach'). (C. Palzer, 'European provisions for the establishment of co-regulation frameworks', in Nikoltchev, S. (ed.), *Co-regulation of the media in Europe*, IRIS Special, Strasbourg, European Audiovisual Observatory, 2003, p. 4; C. Palzer, 'Co-regulation of the media in Europe: European provisions for the establishment of co-regulation frameworks', *Iris Plus 2002*, No. 6, p. 4. See also E. Lievens, o.c., 208-214.) The definition of co-regulation contained in the IABL however seems to only reflect the top-down approach. See also T. Prosser, 'Self-regulation, co-regulation and the Audio-Visual Media Services Directive', *Journal of Consumer Policy* 2008, vol. 31, no. 1, p. 107.

[147] European Commission, 'Part III: Annexes to the Impact Assessment Guidelines', *l.c.*, p. 26.

[148] E. Lievens, o.*c.*, p. 227 and p. 215-216 (with reference to Hans-Bredow-Institut and EMR, Study on co-regulation measures in the media sector: Final report', Study commissioned by the European Commission, June 2006, available at

1. carefully lay down the structure and procedures of the co-regulatory process;
2. safeguard 'process values' such as transparency, adequate participation (representativeness), independence and accountability;
3. put in place proportional regulatory enforcement (establishment of effective sanctions and appropriate supervisory mechanisms) to ensure the system has 'teeth'.

Co-regulation is seen by many as combining the advantages of legislation (e.g., legal certainty, democratic guarantees and more efficient enforcement) with the advantages of self-regulation (e.g., greater flexibility, greater expertise, higher commitment to compliance).[149] However, not all commentators are equally optimistic regarding the benefits of this approach.[150] In the end, the success of such an approach will depend mainly on the underlying market conditions and whether or not adequate safeguards are in place.

An interesting example of how co-regulation may look in practice is provided by the Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards.[151] This resolution outlined a number of basic principles, commonly referred to as 'The New Approach', whereby:

1. (legislative) harmonization is limited to essential safety requirements (or other requirements of general interest) which are defined in an EU directive;
2. the task of drawing up the technical specifications needed for the production and placing on the market of products conforming to these essential requirements is entrusted to organizations competent in the standardization area;
3. conformity with those standards is not mandatory but national authorities are obliged to recognize that products manufactured in conformity with the relevant standards are presumed to conform to the 'essential requirements' established by the Directive (rebuttable presumption of compliance with the requirements of the law).[152]

While traditionally speaking the 'New Approach' has been limited to fields of health, safety, environmental or consumer protection, many directives have been adopted which incorporate

---

http://ec.europa.eu/avpolicy/docs/library/studies/coregul/final_rep_en.pdf) (last accessed 8 January 2012).

149 See E. Lievens, *o.c.*, p. 225-226; Commission of the European Communities, 'Interim report from the Commission to the Stockholm European Council: Improving and simplifying the regulatory environment, COM (2001) 130 final, 7 March 2001, p. 7 and Commission of the European Communities, 'Communication from the Commission – Simplifying and improving the regulatory environment, COM (2001) 726 final, 5 December 2001, p. 8.

150 See e.g. T. Prosser, 'Self-regulation, co-regulation and the Audio-Visual Media Services Directive', *l.c.*, p. 103, pointing out that, in certain circumstances, co-regulatory systems do not offer the best of both worlds but the worst, 'in which neither [private or public interests are] respected and any values are subjected to unprincipled bargaining between state and private interests'.

151 O.J.-136, 4 June 1985, p. 1–9.

152 For more information see H. Schepel and J. Falke, Legal aspects of standardisation in the Member States of the EC and EFTA. Volume 1 – Comparative Report, Luxembourg, Office for official publications of the European communities, 2000, p. 22 et seq.; European Commission, 'Guide to the implementation of directives based on the New Approach and the Global Approach', 2000, available at http://ec.europa.eu/enterprise/policies/single-market-goods/files/blue-guide/guidepublic_en.pdf (last accessed 18 January 2012). For a discussion on the viability of technical standards as a means for promoting data protection see J. Winn, 'Technical Standards as Data Protection Regulation', in S. Gutwirth and Y. Poullet (eds.), *Reinventing Data Protection*, Springer, 2009, 191-206. A revised version of this paper is available via SSRN at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1118542 (last accessed 25 December 2011).

this approach or elements of it.[153] For instance, Directive 1999/93/EC on E-Signatures is considered to have incorporated several elements of the New Approach.[154]

3.3 Participation and consultation

The previous sections have illustrated that the state no longer holds a monopoly position as regulator, as regulatory instruments in which other actors are involved have gained importance. The European Commission has repeatedly stressed the importance of wide participation from policy conception to implementation.[155] Consultation of different parties is considered crucial in attaining wider participation in policymaking.[156]

However, throughout the policy documents it is not always clear which stakeholders should be consulted or are considered valuable participants in the regulatory process. A wide variation in terminology is used, including: 'stakeholders', 'users', 'citizens', 'civil society', 'public', 'consumers', etc. In principle, consultation may be open to the general public, restricted to specific categories of stakeholders, or limited to a set of designated individuals or organizations.[157] As a general rule however, all target groups and sectors which will be significantly affected by the regulatory measure, or involved in its implementation, should be consulted (including those residing outside of the EU). Organizations and bodies whose stated objectives give them an interest in the policy area in question should also be considered.[158]

In the context of GINI, we believe that, in addition to researchers and experts, the following three categories of stakeholders should be consulted prior to the adoption of any policy measure:

1. Civil society (e.g., consumer advocacy groups, activists, academia, and other experts);
2. Governmental entities (not only those traditionally involved in policy-making, but also those that may be affected by the envisaged policy measure, i.e. during implementation);
3. ICT industry (particularly those companies and fora involved in the design and deployment of identity solutions, without limiting oneself the large scale operators).

For these stakeholders, proper consultation will require that they are actively engaged in the policy process from early on. This is partly because of the presence of significant information problems in the domain at hand, but also because the extent to which markedly improved outcomes can be achieved will much depend on their direct involvement. The costs of unsatisfactory (or altogether missing market conditions) are spread thinly on large numbers of

[153] See http://www.newapproach.org.

[154] See SEALED, DLA Piper and Across communications, 'Study on the standardization aspects of eSignature', Study for the European Commission (DG Information Society and Media), 22 November 2007, p. 13, available at http://ec.europa.eu/information_society/eeurope/i2010/docs/esignatures/e_signatures_standardisation.pdf.

[155] See e.g. Commission of the European Communities, 'Communication from the Commission: Towards a reinforced culture of consultation and dialogue - General principles and minimum standards for consultation of interested parties by the Commission', Brussels, 11.12.2002, COM(2002) 704 final, p. 4.

[156] See also OECD, 'Guiding principles on regulatory quality and performance', 2005, 5: *"Consult with all significantly affected and potentially interested parties, whether domestic or foreign, where appropriate at the earliest possible stage while developing or reviewing regulations, ensuring that the consultation itself is timely and transparent, and that its scope is clearly understood"*.

[157] European Commission, 'Part III: Annexes to the Impact Assessment Guidelines', *l.c.*, p. 14.

[158] *Id.*

unaware users that face difficulties to organize themselves effectively to defend their interests. This is a well-known phenomenon in markets that are one-sided (in the sense that the costs of rectifying a particular imperfection fall disproportionately on a small number of well-informed actors, whereas the benefits of such action are spread thinly on large numbers of less informed users). This issue also presents itself when many of those who stand to pay for the absence of orderly market conditions belong to future generations, who have not yet been born (or whose members are too young today to make themselves heard in the political process). These considerations also apply for the lack of orderly frameworks for handling identity management in digital communication, since everyone suffers (often in small unknown doses) from the resulting problems in security, privacy, lack of trust, and inflated transaction.

Furthermore, since users' awareness and behavior will be interdependent with what options they are confronted with, and the incentives for different service providers to engage in efforts to, e.g., develop better privacy protection, will depend on the actions of other service providers as well as how users will respond, the drive for developing solutions will much depend on what active interface can be achieved between users, service providers and various kinds of public authorities and policymakers. There is a case not only for activating appropriate representatives of the latent "silent majority" to have a say on what needs to be done, but to initiate a process of continuous collaboration, entailing improved awareness-creation as well as concrete problem-solving, between the key actors that need to be part of a viable solution.

On this basis, we propose that the preparations for launching an INDI architecture and/or INDI services should be accompanied by the establishment of a consultation and communication platform. Whereas public authorities and the ICT industry would thereby obtain a forum for actively "working with" representatives from their broad customer base in developing and testing solutions, civil society would gain a mechanism to raise complaints against current malpractice, push for innovations and exercise a reality check of new products and methods that are under way in the market place or conceived of by policymakers. Such a forum could be developed on a European basis, or it could be global in nature (or extend to other parts of the world from a European base). This is important both because the global nature of the digital exchange means that technical, market and policy developments in any single region can affect other parts of the world, and also because this would facilitate the much needed exchange of information what works and what does not work under varying circumstances, and to help identify best practice. It is not least import to support a more widespread understanding and agreement what measures are required for attaining solutions that are both effective in the short term and susceptible to innovation and gradual improvement over time.

Various bodies have already developed and proposed relevant standards and protocols for the web related issues/developments around identity management. Examples in this regard are, e.g., the Organization for the Advancement of Structured Information Standards (OASIS), the Liberty Alliance (Kantara Initiative), the World Wide Web Consortium (W3C), and the Global Trust Center (GTC). Each of these may be expected to champion their perspectives and model approaches. However, the range of possible tracks and institutional building blocks should be taken into account when developing regulatory frameworks to help ensure they become conducive to diverse and yet consistent offerings of INDI operators.

Finally, there is the need of putting in place other mechanisms for more effective policy coordination at the global level, beyond what we see in today's multilateral organizations such as ITU, ICANN or the OECD, in support of consistency and interoperability in identity management solutions. An active multi-stakeholder consultation and communication platform can however help articulate the demand and help push for such collaboration.

3.4 Relationship regulatory tools – trust framework(s)

In the previous chapter we provided an introduction to the trust framework concept, the actors involved, as well as an overview of the key issues which need to be addressed. Now that we have also identified the range of regulatory tools available to EU policy-makers, the question arises how such measures might relate to the development of a particular trust framework in practice. Given the wide range of regulatory instruments available, it is impossible to provide, in the context of this report, a detailed analysis of how each type of instrument might impact the development of a given trust framework. Nevertheless, we consider that there is merit in further exploring, at a conceptual level, the potential interactions between trust frameworks and different forms of regulation outlined above.[159]

In section 2.2, we outlined three 'layers' at which the actors involved in the implementation of a particular trust framework can reside: governance, administration and operational layer. The relationship between the regulatory measures outlined in the previous sections and trust frameworks will mainly hinge upon how such measures determine the *level of involvement of governmental authorities in the setting and administration of a trust framework's policies*. In addition, regulatory measures adopted by policy-makers may also be instrumental in providing *incentives* and *co-ordination* to either promote the emergence of one or more trust frameworks and/or align their functioning with one or more policy objectives. Each of these considerations shall be further elaborated over the following subsections.

3.4.1 Trust framework policies

The policies (or 'rules') of a given trust framework are defined by the actors residing at the governance layer. As indicated earlier, the rules that apply to a particular ecosystem can take on a myriad of forms.[160] To the extent that the legal instruments which bind the participants of a particular ecosystem have been decreed by a governmental authority, the trust framework's policies may be seen as an extension (or part) of the regulatory framework. Conversely, if the setting of trust framework policies is observed entirely by private sector actors, the interaction between regulation and trust frameworks shall be more indirect in nature. Even though, in such circumstances, the 'rule-makers' (entities residing at the governance layer) may enjoy considerable latitude in setting trust framework policies, they will still need to take into account the relevant (mandatory) legal requirements (e.g., data protection law, competition law). In practice this will require them to 'internalize' the relevant legislation within the policies of the trust framework; which shall apply in conjunction with any additional rules decreed by the entities residing at the governance layer.[161] In other words, even where regulatory measures are not tailored to address a particular trust framework, existing or new regulation (particularly regulation which has a broad scope, such as data protection legislation) is bound to impact its policies and practices.

The nature and extent of regulatory intervention by public actors will inevitably determine 'margin for manoeuvre' of private sector actors, and thus also for self-regulation. In this regard, it

[159] Regulation can take many different forms. Trust frameworks, whether they emerge through the acts of governments and/or private sector entities, always seek to have a 'regulatory' effect (in the sense that they seek to impose certain constraints on or alter the behaviour of the participants in a particular ecosystem). However, we use the term 'regulatory' in more narrow sense here. Specifically, we use this term to refer to the measures available to EU policy makers, i.e., the 'policy options' identified in the preceding subsections.

[160] Cf. *supra*; section 2.3.1.

[161] See also *supra*; section 2.3.1.

is important to keep in mind the following considerations. No regulatory instrument, whether it has been drafted by public or private actors, can reside in a legal vacuum. While the degree of discretion of private actors in determining the scope of their respective rights and obligations may vary, there will always be certain boundaries imposed by mandatory law. Conversely, it is unfathomable that governments would regulate the relationships among private actors in their entirety: while it may set certain standards from which private actors may not deviate, it would be impossible for them to micro-manage each and every aspect of their mutual relationships. An appropriate balance needs to be sought, in line with the principles of subsidiarity and proportionality, whereby both the nature and extent of regulatory intervention are tailored to address the problems and objectives identified in the course of the regulatory impact assessment.

3.4.2 Oversight

Oversight of trust framework policies is a second area in which regulatory measures and trust frameworks are bound to interact with one and other. As indicated earlier, almost all identity trust frameworks assume the presence of an oversight function, which comprises activities related to compliance monitoring (e.g., audit of transactional records).[162] This supervisory function could in theory be observed by both private sector (e.g., auditing company) and/or public sector authorities (e.g., national data protection authorities). In any event, it is important to keep in mind that no agreement among private actors can detract from the jurisdictional authority of a public sector body which has been established by law. Similar considerations also apply in relation to dispute resolution mechanisms. No trust framework policy shall be able to diminish the participants' fundamental right of access to an independent and impartial tribunal established by law where the dispute concerns their civil rights (art. 6 ECHR).[163] For example, where a dispute among participants implicates the privacy rights of INDI Users, the individuals concerned shall always have the right of recourse through the traditional judicial and/or administrative authorities. In other words, the implementation of ADR mechanisms will not negate the ability of individuals to file complaints with either the courts or data protection authorities, but can merely serve as a supplementary form of dispute resolution.

3.4.3 Accreditation

Another area in which regulatory measures and trust framework(s) may interact concerns the accreditation of ecosystem participants. A trust framework may for example stipulate a requirement of formal recognition as a prerequisite to the performance of one or more activities within the context of the ecosystem (e.g., validation of security practices before being authorized to act as an identity service provider or relying party) or to enjoy certain benefits (e.g., the right to display a certain 'trust mark' or 'seal'). While accreditation may be observed by private sector bodies, public sector bodies may also be involved in this process to a greater or lesser extent. An example of an instance where public sector actors may be involved in the accreditation of service providers is the voluntary accreditation scheme under the E-Signature Directive.[164] Depending on how a Member State transposed article 3, 2 of the E-Signature Directive, it is possible that the

[162] Cf. *supra*; section 2.3.2.

[163] For more information see E. Lievens, *o.c.*, 323-327 and 411-418.

[164] Article 3, 13 of the Directive defines 'voluntary accreditation' as '*any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification-service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body*'. See also GINI D3.1, section 7.7.

accreditation of certain types of certification services within its territory is observed (in whole or in part) by a public sector body. It is worth noting that the existence of an accreditation function in practice also implies the existence of one or more standards ('rules') with which the applicant must comply in order to receive accreditation. The accreditation function under a particular trust framework will therefore always be closely related to the rules adopted by the governance layer, which may or may not involve governmental authorities (cf. *supra*; section 3.4.1).

3.4.4 Incentives and co-ordination

Policymakers can use regulatory measures not only to constrain the activities of private and public actors, but also to provide incentives and ensure necessary co-ordination. For instance, through spending programmes, legislative measures can be used to stimulate further research and/or development in a particular field of technology (e.g., attribute-based credentials or other privacy enhancing technologies). However, incentives need not necessarily take the form of direct financial intervention. By providing certain benefits of a non-financial nature (e.g., formal accreditation, presumption of compliance), relevant actors might also be encouraged to meet the standards set forth by policymakers.

EU policymakers can also try to steer relevant actors in the desired direction through co-ordination. In addition to the use of OMC and the promotion of self-regulation, EU policy makers may also consider the use of different forms of public-private partnership to achieve their objectives. In this regard, it is worth taking note of the approach adopted in the US with regards to the implementation of NSTIC: having outlined the basic vision of the strategy, NSTIC called for the establishment of an interagency office, to be known as the 'National Program Office' (NPO).[165] This NPO is to be charged with achieving the goals of the Strategy, by leading the day-to-day coordination of NSTIC activities. Specifically, the NPO is expected to:

1. *Promote private-sector involvement and engagement;*
2. *Support interagency collaboration and coordinate interagency efforts associated with achieving programmatic goals;*
3. *Build consensus on policy frameworks necessary to achieve the vision;*
4. *Identify areas for the government to lead by example in developing and supporting the Identity Ecosystem, particularly in the Executive Branch's role as a provider and validator of key credentials;*
5. *Actively participate within and across relevant public- and private-sector fora; and*
6. *Assess progress against the goals, objectives, and milestones of the Strategy and the associated implementation activities.*[166]

In conclusion, we reiterate that the actual relationship between regulatory measures and a trust framework will mainly depend on the nature and role of the actors involved in the articulation and administration layer of trust framework policies. Trust frameworks are social systems which, like legal systems in general, aim to stabilize the expectations of participants in a particular ecosystem.[167] To the extent that their governance and/or administrative functions are observed

[165] The White House, 'National Strategy for Trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy', *l.c.*, p. 39. This interagency office is established within the Department of Commerce

[166] *Id.*

[167] According to Luhmann, the sole function of the legal system is the *maintenance (stabilization) of expectations despite disappointments (counterfactual examples)* (R. Nobles and D. Schiff, Introduction to Luhmann's 'Law as a Social System', Oxford University Press, New York, 2004, p. 14): *"Concretely, law deals with the function of*

by governmental authorities, they shall be integrated in whole or in part within the regulatory framework. However, in practice the aforementioned functions will rarely be observed by governmental authorities alone. Rather, it may be expected that trust frameworks shall operate as subsystems within the broader legal system, whereby the actual degree of proximity (or overlap) with the regulatory framework may vary.

The evaluation of which type of regulatory instrument is best suited to attain a particular policy objective needs to be made on a case-by-case basis.[168] More often than not, the optimal approach will lie in a combination of different regulatory instruments. In the following section we shall further elaborate upon a number of areas in which some form of regulatory intervention may be required in order for the PIM ecosystem envisaged by GINI to emerge. Where appropriate, we shall point to the different forms of intervention that may be considered to address the identified problems and objectives.

the stabilization of normative expectations by regulating how they are generalized in relation to their temporal, factual, and social dimensions. Law makes it possible to know which expectations will meet with social approval and which not. […] One can afford a higher degree of uncertain confidence or even mistrust as longs as one has confidence in the law. Last but not least, this means that one can live in a more complex society, in which personal or interaction mechanisms no longer suffice." (N. Luhmann, *Law as a Social System*, Oxford University Press, New York, 2004, p. 148 (translation by K. A. Ziegert). As elaborated earlier, the overall aim of a trust framework is to '*provide mutual assurance between participants with respect to a particular functional online systems*'. (cf. *supra*; section 2.1.) Thus the social function, of both legal systems and trust frameworks, is to enable individual entities to maintain certain (normative) expectations with regards to the behaviour of other entities (at least insofar as this behaviour falls within the scope of the framework in question). Fulfilling this function should in turn, at least theoretically, allow the relevant entities to engage in transactions with one and other even where they do not have complete confidence that the other party (or parties) to the transaction will hold up their end of the bargain. A prerequisite for such trust, however, is a trust in the framework itself (confidence in the legal system or confidence in the trust framework respectively). In other words, the object of trust ('what or who needs to be trusted') is shifted, at least in part, from the counterparty to a particular transaction to the framework(s) that govern(s) that transaction.

[168] See also E. Lievens, *o.c.*, p. 229-230.

4 Recommendations

The purpose of this section is to identify areas in which some form of regulatory intervention is recommended in order for the PIM ecosystem envisaged by GINI to emerge. These recommendations are based on:

1. the GINI vision as outlined in GINI D1.1;
2. the legal gaps and barriers identified in GINI D3.1;
3. additional insights gained through stakeholder engagement; and
4. discussions within the project consortium.

In the previous chapter we elaborated upon the range of regulatory instruments available to EU policymakers. Over the following sections, we will outline how these instruments may be used in order to overcome the main gaps between the current situation and the PIM ecosystem envisaged by GINI. While a more detailed analysis of underlying market conditions is required to specify in detail which approach is best suited to address a particular issue, we shall explore whether use of legislative and/or non-legislative measure instruments is appropriate.

4.1 Data protection and privacy

4.1.1 Privacy enhancing technologies

The first essential component of the GINI vision is the availability of a variety of privacy-enhancing services from which individuals can choose when sharing their identity information with relying parties. The availability of such services requires the development and adoption of privacy enhancing technologies (PETs), i.e. technologies which seek to

(a) reduce the risk of contravening privacy principles and data protection legislation;
(b) minimize the amount of personal data being processed; and/or
(c) provide individuals increased control and/or transparency over the processing of their personal data.[169]

Studies have shown that large-scale adoption of many PETs is still lacking, for a variety of reasons.[170] Companies often have insufficient incentives to invest in and/or implement certain PETs because they seldom provide a direct commercial advantage. Moreover, use of some PETs may limit the future functionality of the data they collect (e.g., by limiting a company's ability to cross-reference user-provided data with data from other sources referring to the same users).

[169] Based on London Economics, 'Study on the economic benefits of privacy-enhancing technologies (PETs)', Final Report to The European Commission DG Justice, Freedom and Security, July 2010, p. 7, available at http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm (last accessed 2 March 2012).

[170] *Ibid*, p. 29-46. See also J. Borking, 'Why adopting Privacy Enhancing Technologies (PETs) Takes So Much Time', in S. Gutwirth, Y. Poullet, P. De Hert and R. Leenes (eds.), *Computers, Privacy and Data Protection: An Element of Choice*, Springer, 2011, p. 309-341; S. Fischer-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg, and M. Waidner, 'Online Privacy: Towards Informational Self-Determination on the Internet' (Dagstuhl Perspectives Workshop 11061), *Dagstuhl Manifestos* 2011, vol. 1, issue 1, p. 11, available at http://www.dagstuhl.de/en/program/calendar/semhp/?semnr=11061 (last accessed 12 March 2012).

PET adoption often also requires modification of business (processing) models, which entails additional costs. So from a company's perspective, adopting PETs often implies costly investments without short-term monetary benefit.[171] The main motivation for most companies to invest in and adopt privacy enhancing practices or technologies appears to be compliance.[172] However, it is often unclear which implementations do fulfill the relevant legal requirements, which does not encourage the investment in better solutions, that on the short term are often more complex and expensive to adopt.

In light of the foregoing considerations, regulatory intervention promoting the development and adoption of PETs appears to be warranted.[173] Given that compliance is one of the more prominent drivers for PET adoption, one might infer that use of legislative measures would be the most appropriate policy option (e.g., by introducing additional provisions in the legal data protection framework which require the use of anonymization or pseudonymization technologies). However, there are significant limitations to this approach, particularly if it were to be adopted in isolation. The main reason is that enforcement of any legal provision aimed at stimulating the use of PETs shall always be constrained by the state of the art and the costs of implementation.[174] In absence of successful large-scale implementations and reasonably priced, 'off-the-shelf' solutions, it is difficult to imagine a generally enforceable legal obligation to adopt PETs (save for specific instances). Conversely, should a particular PET be adopted on a large scale and become available at a reasonable price, the enforcement of such a provision could become much more straightforward.[175]

This being said, it is also clear that the current data protection framework places far greater emphasis on ex-post securing of data rather than on ex-ante elimination of privacy risks (e.g., through data minimization or 'privacy by design').[176] While existing data protection principles already impose upon data controllers an obligation to take preventative measures to ensure compliance, explicit incorporation of 'data minimization' and/or 'privacy by design' principles would arguably help promote their actual enforcement[177], which could in turn stimulate the

---

[171] See also London Economics, 'Study on the economic benefits of privacy-enhancing technologies (PETs)', *l.c.*, p. 61.

[172] Bramhall, Pete; Hansen, Marit; Rannenberg, Kai; Roessler, Thomas (Eds.) (2007): User-Centric Identity Management – New Trends in Standardization and Regulation. In: IEEE Security & Privacy, Vol. 5 No. 4, pp. 84-87.

[173] See also London Economics, 'Study on the economic benefits of privacy-enhancing technologies (PETs)', *l.c.*, p. 154.

[174] This point is illustrated by article 17, 1 of Directive 95/46/EC, which provides that *"[…] the controller must implement appropriate technical and organizational measures to protect personal data against […] and against all other unlawful forms of processing. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."* [emphasis added] While other provisions of the Directive, e.g. the principles relating to data quality, do not explicitly reference cost or state of the art, the assessment of compliance shall depend on what are considered to 'reasonable measures to safeguard these principles' that may be expected from any controller in similar circumstances.

[175] In other words, the slow rate of PET adoption appears to explainable, at least in part, as a 'catch 22' or 'chicken-or-egg-problem'.

[176] See S. Fischer-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg, and M. Waidner, 'Online Privacy: Towards Informational Self-Determination on the Internet', *l.c.*, p. 11-12.

[177] See also European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 2010/C 280/01, paragraph 39 and S. Gürses, C. Troncoso and C. Diaz, 'Engineering Privacy by Design', in *Computers, Privacy & Data Protection* (CPDP Conference 2011), 25 pages (pre-print), 2011, p. 3-4 available at http://www.esat.kuleuven.be/scd/person.php?view=2&persid=400.

adoption of PETs.[178] However, as we just indicated, merely adopting such provisions without additional measures is not likely to deliver the desired outcome. Rather, a combination of legislative and non-legislative measures is bound to be most effective, whereby the following forms of regulatory intervention should additionally be considered[179]:

1. **Stimulating further research and development**: EU policy-makers should continue to support PETs development through direct or indirect funding, and particularly the research and development of solutions that address the technological gaps identified in GINI D2.2.

2. **Leading by example**: governments have, in light of their public policy objective, a specific role to play in the promoting the adoption of privacy-enhancing practices. Their decision to incorporate certain PETs (or failure to do so) may impact future assessments as to what measures may reasonably be expected from private data controllers (benchmarking role).[180] In addition to 'practicing what they preach', EU policy-makers should also continue to promote benchmarking and exchange of best practices among Member States (e.g., by use of the OMC).[181]

3. **Enhancing accountability**: even if the legal provisions and technical developments are in place to stimulate PETs adoption, actual adoption will arguably only take place if there is effective oversight and enforcement of data controllers' operations; in combination with sanctioning mechanisms that provide sufficient incentives for adoption. EU policy-makers should ensure that both national and European Data Protection Authorities are provided with sufficient resources in terms of manpower, expertise, and investigational competencies to ensure meaningful accountability of data controllers.[182]

4. **Increasing awareness**: poor awareness among data controllers is an important factor contributing to low levels of PETs adoption.[183] Data protection authorities in particular have a key role in broadly communicating the benefits of PETs, which types of PETs are available and what purpose they may serve, etc. However, other stakeholders, such as self-regulatory organizations and other public sector entities, may also play an important role in bringing the availability and desirability to the attention of data controllers and the public at large.

5. **Promoting further standardization and recognition of PETs**: EU policy-makers should also be a driving force in the further development of technical standards which

[178] The European Commission has explicitly incorporated provisions to this extent in its EU data protection reform proposals; see e.g. the proposed articles 5 (c) (data minimization) and 23 (data protection by design and by default) of the 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', Brussels, 25 January 2012, COM(2012) 11 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, last accessed 13 March 2012.

[179] Similar recommendations were also articulated in the Study on the economic benefits of privacy-enhancing technologies (PETs), *l.c.*, 153-154.

[180] In addition, due to the scale of their operations, the adoption of a certain PET by governmental authorities (even if its use is limited to certain application areas) has the ability to prove this technology's maturity as part of the 'state of the art' if this wasn't already accepted.

[181] Cf. *supra*; section 3.2.1.2.

[182] See also *infra*; section 4.1.3.

[183] S. Fischer-Hübner, C. Hoofnagle, I. Krontiris, K. Rannenberg, and M. Waidner, 'Online Privacy: Towards Informational Self-Determination on the Internet', *l.c.*, p. 11.

support data protection principles.[184] Additional initiatives should also be considered to promote recognition of PETs, e.g. in the forms of voluntary accreditation[185] or official endorsements[186] by regulators.

In conclusion, it is worth underlining that each PET has its own characteristics, so the appropriate policy response may vary. For some PETs, adequate incentives for adoption may emerge naturally, whereas for other PETs there may be a stronger need for investment, co-ordination and stimulation by policymakers.[187]

4.1.2 Data portability

A second essential component of the GINI vision is data portability. While this term has been defined in a variety of ways, it is typically used to denote the ability of individuals to transfer and re-use their personal information across (interoperable) services.[188] Under the GINI vision, data portability comprises three dimensions. First, it means that individuals shall have the ability to present their data, which is held by one or more Data Sources, to one or more Relying Parties.[189] An individual might wish to do this in order to meet transactional requirements (e.g., access control conditions set by a Relying Party) or to improve the perception of her trustworthiness (e.g., when selling a car). The basic assumption is that Relying Parties will have greater confidence

---

[184] European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union', November 2010, Brussels, COM(2010) 609 final, p. 16, available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdfEC. See also European Commission, 'Communication from the Commission to the European Parliament, the Council and the Economic and Social Committee: A strategic vision for European standards: Moving forward to enhance and accelerate the sustainable growth of the European economy by 2020', COM(2011) 311 final, Brussels, 1 June 2011, p. 9, available at http://ec.europa.eu/enterprise/policies/european-standards/files/standardization/com-2011-311_en.pdf (last accessed 13 March 2012). The European Commission (EC) in particular, as the supranational representative of 27 countries and initiator of regulatory change at EU level, can play an important role in the standardisation process as intermediary between the respective stakeholders (industry, research, regulators and consumers).

[185] As indicated earlier, one of the ways in which regulatory frameworks and trust frameworks can interact is at the level of accreditation of ecosystem participants (cf. *supra*; section 3.4.4). In theory, use of voluntary accreditation mechanisms can be stimulated is through 'New Approach' mechanisms (comp. *supra*; section 3.2.2.2). While some commentators have advocated for application of this approach in the context of data protection (see e.g. P. Van Eecke and M. Truyens (eds.), 'The future of online privacy and data protection', EU study on the Legal analysis of a Single Market for the Information Society – New rules for a new age?', DLA Piper, November 2009, p. 64, available at http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=7022); others have questioned whether this approach can successfully be adapted to the dynamic and volatile ICT markets in all instances (see J. Winn, 'Technical Standards as Data Protection Regulation', *l.c.*, 191-206.). In a later section we will elaborate upon the use of voluntary accreditation mechanisms in the context of the re-use of personal data held by governmental bodies (cf. *infra*; section 4.2)

[186] For an example see London Economics, 'Study on the economic benefits of privacy-enhancing technologies (PETs)', *l.c.*, p. 150.

[187] *Ibid*, p. 72.

[188] See e.g. European Commission, 'A comprehensive approach on personal data protection in the European Union', *l.c.*, p. 16; http://en.wikipedia.org/wiki/DataPortability.

[189] Instead of actually disclosing the data an individual might also present the Relying Party with a link to the information which is being held by the Data Source. See GINI D1.1, section 5.3.5.

in the attributes asserted by an individual if they are confirmed by an independent entity, which is perceived as maintaining high-quality information.[190] The second dimension of data portability under the GINI vision is verifiability of authenticity. This dimension entails that, when presenting their data, individuals shall be able to do so in a manner that provides Relying Parties with appropriate assurance as to its authenticity.[191] This dimension of data portability is arguably critical to the first, because without it the data will only be accepted in instances involving very low assurance requirements (i.e., where self-assertion by the individual concerned is deemed sufficient by the Relying Party).[192] Finally, data portability under the GINI vision also means that individuals shall be able to transfer their data seamlessly across INDI Operators, so as to facilitate greater competition among these entities.[193]

Under the current state of play, individuals rarely have the means to control, in a positive sense, the exchange of their personal information. Because the organizations collecting and storing personal information are (in one way or another) 'consumers' of this information, the exchange of this data is typically structured in an 'organization-centric' fashion. While data protection laws endow individuals with a set of rights as data subjects[194], the current framework does not provide them with any 'affirmative' rights which enable them to initiate an exchange of information at their own discretion.[195] A fortiori, individuals also lack the right to request that their personal data be made available in a way which enables easy re-use and/or verification by other entities.

There are several reasons to believe that the aforementioned deficits shall not be remediated by the market itself. First, making data available at the request of the data subject will always entail certain costs (e.g., authentication of the data subject, retrieval of requested information, making it available in re-usable format, etc.), which do not necessarily have a corresponding short-term benefit. Second, personal data is typically perceived as a valuable asset, which a Data Source may not want to share with its competitors. A third reason why Data Sources may be reluctant to divulge personal data to third parties is a fear of liability. This being said, it also clear that certain Data Sources do perceive economic benefits in supporting data portability, particularly where it:

4. directly contributes to their core business model[196];
5. enables them to gain efficiencies[197]; and/or

[190] See also GINI D3.1, section 2.1.

[191] See GINI D1.1, section 5.

[192] In addition to the need for assurance regarding the source of the data (which should either be a Data Source or claims handler trusted by the Relying Party such as an INDI Operator), there is also the issue of reliability. While the former is dependent on the means used to secure the authenticity of the data (e.g. digital signatures), the latter depends mainly on the data verification and management practices of the Data Source (e.g., when registering attributes about individuals for the first time).

[193] Regarding the role of the INDI Operator see GINI D1.1, section 5.3 and GINI D3.1, section 2.2.

[194] See GINI D3.1, section 4.9.

[195] See also M. Rundle (ed.), 'At a Crossroads: "Personhood" and Digital Identity in the Information Society', *STI Working Paper 2007/7*, Information and Communication Technologies, OECD, Directorate for Science, Technology and Industry, 29 February 2008, p. 28, available at www.oecd.org/dataoecd/31/6/40204773.doc (last accessed 23 March 2012), stating that '*[t]he [OECD] Privacy Guidelines have a strong focus on protecting a person's data against inappropriate treatment by other actors; however, they place the individual in a rather passive role and so fail to provide him with the proactive right to use his own identity information as he sees fit.*'

[196] While this is clearly the case for service providers whose core business is certification (e.g. a CA in a PKI scheme), other scenarios are also possible. For instance, an internet service, whose business model is based on (the facilitation of) behavioural advertising, might actively promote re-use of the credentials it has issued in order to enrich its dataset on its users (as it might put them in a position to learn more about the Relying Parties with which its users interact).

6. is perceived as a valuable addition to their service offering.

However, even in instances where Data Sources do perceive an economic benefit, the incentives to support data portability shall typically be limited to specific subsets of the information it maintains. Comprehensive data portability will therefore require some form of regulatory intervention before it becomes a reality.

The European Commission has already undertaken to provide data subjects with a general right of data portability in its proposals for the reform of the data protection framework.[198] Specifically, art. 18, 1 of the proposed Regulation specifies that

> *'The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.'*

The second paragraph of article 18 supplements this right by an additional right, in cases where the data subject has provided the personal data and the processing is based on consent or on a contract, to transmit those personal data to another automated processing system. The rationale behind these proposals is two-fold:

7. to further improve access of individuals to their personal data[199]; and
8. to enable individuals to withdraw their data, from one application or service, and transfer it to another application or service, without hindrance from the data controllers (as far as this is technically feasible).[200]

As a precondition for the effective exercise of this right, article 18 provides the right to obtain from the controller those data in a structured and commonly used electronic format.[201] The third paragraph of article 18 delegates to the Commission the authority to specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2.[202]

When comparing article 18 of the proposed Regulation to the concept of data portability as envisioned by GINI, it is clear that a number of gaps still remain. First, article 18 only affords individuals a right to transmit their personal data from one processing system to another in cases where the data subject has provided the personal data and the processing is based on consent or

---

[197] For instance, in the context of e-payment, portability of billing data (e.g., from service providers to banks, with or with the intervention of an intermediary) provides greater convenience to customers, but also enables greater efficiencies for service providers.

[198] See European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', Brussels, 25 January 2012, COM(2012) 11 final, p. 9, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, last accessed 13 March 2012.

[199] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)', *l.c.*, p. 9.

[200] European Commission, 'A comprehensive approach on personal data protection in the European Union', *l.c.*, p. 8.

[201] *Id.*

[202] Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

on a contract.[203] This implies that individuals shall not enjoy a right to data portability where the processing is based on a different legitimate basis, such as a legal obligation to which the controller is subject (which would arguably exclude important Data Sources including public authorities[204]). Second, article 18 does not, by itself, require verifiability of authenticity and/or reliability. Data controllers are prevented from hindering the withdrawal and transfer of data, but are not required to 'package' this data in a way that would allow third parties to establish its origin and integrity (or otherwise corroborate its reliability).[205] As a result, the potential added value of this right consists mainly of greater convenience when changing service providers, rather than providing data subjects with a means to prove certain attributes.[206] A third area in which the proposed right of data portability may show itself lacking concerns the ability to designate recipients. While Data Sources should not learn the identity of Relying Parties where this is not necessary, the data subject should also be able to request from the controller that he sends his or her data to a third party of his or her choosing (e.g., an INDI Operator).[207]

It is beyond the scope of this deliverable to make a normative recommendation on how to best bridge these outstanding gaps. Before one can do so, further research is necessary to elaborate upon both the economic and legal aspects of data portability, which should take into account the following issues:

1. **Interoperability**: what costs are there for Data Sources to provide data in a format which differs from the format in which the data is currently being processed? Is there a viable business model for supporting data portability as a service; which would enable interoperability while allowing Data Sources to minimize expenses? Or is it sufficient that a limited number of standardized formats are imposed upon all Data Sources?

2. **Verifiability**: can a generally enforceable right of data portability be created which allows data subjects to convincingly demonstrate the authenticity of the data they present (or which is presented on their behalf)? Or must alternative forms of regulation be adopted to (incrementally) achieve this goal (e.g., by stimulating market-based solutions through a combination of legislative and non-legislative measures)?

3. **Reliability**: in which ways can appropriate assurance regarding the accuracy of information be realized? For instance, is it sufficient that Data Sources are subject to a

[203] While article 18 does not actively limit data portability to those scenarios, it only prevents controllers from posing an obstacle to such portability in those two instances (which in turn implies that the right of data portability shall only then be enforceable as such).

[204] Regarding re-use of information held by public sector bodies see also *infra*; section 4.2.

[205] It is in principle not excluded that the Commission, by way of an implementing act, specifies standards or modalities which would support verifiability of authenticity and reliability. However, such an act might also be considered *ultra vires* as the text of article 18 seems to be mainly aimed at removing artificial barriers towards re-use rather than supporting verifiability.

[206] The use of the word 'prove' here does not refer to the provisioning of evidence in the legal sense, but rather to the conveyance of assurance by virtue of the authority enjoyed by the Data Source and its data management practices.

[207] From a privacy perspective, it is in principle undesirable that a Data Sources has the ability to keep track of the Relying Parties with whom their data subjects interact. However, certain individuals might wish to entrust the management of their data with a third party (e.g. a service provider acting as INDI Operator); rather than manage the exchange themselves. This could in principle also be realized through delegation by the data subject of its right of access (see GINI D3.1, section 4.9.2). However, it would appear difficult to then scope the agent's rights in such a way that he or she does not more information than strictly necessary.

general obligation to maintain the accuracy of the information they process (cf. art. 6, 1, d of Directive 95/46/EC)? Or must they formally subscribe to standardized practices which would allow Relying Parties to ascertain the corresponding assurance levels? Or will Data Sources simply be trusted or not by virtue of their informal authority rather than on the basis of their data management practices (e.g., citizen register vs. social network profile)? How important is the context in which the data is being processed by the Data Source? Are qualified statements (e.g., outlining the purpose for which the information is being processed) necessary?

4. **Liability**: when data is transferred from one entity to another, how should the liability risk be apportioned among the parties involved? Does the duty of care in maintaining data accuracy, which is imposed upon all data controllers, extend to third party use? Is there a need to adopt additional legislative measures which define the liabilities of Data Sources and Relying Parties respectively? Or may this simply be left to contract and tort law?

4.1.3 Accountability[208]

A third essential component of the GINI vision is the accountability of actors involved in the PIM ecosystem. GINI envisions a regulatory framework in which institutional actors are able 'to oversee the respect and enforcement of legal rules to the benefit of the public interest and the private interests of individuals.' After first explaining what we mean by accountability in this context, we will outline different forms of regulatory intervention that may help realize accountability.

Accountability is a concept with many dimensions.[209] It has been characterized by scholars as being an 'elusive' and even 'chameleon-like' concept, because it can mean very different things to different people.[210] In its most basic meaning, it refers to the obligation of an entity to explain ('give an account of') how it has acquitted itself of certain responsibilities or why it has acted in a certain way. In order for an actor to be considered 'accountable', a number of constitutive elements must be present. First, accountability implies the presence of one or more *norms* against which the behaviour of the entity in question will be assessed. Second, implicit in the concept of accountability is the assumption of a *relationship* between an entity that is answerable (the 'accountor') and another entity that is being answered to (the 'accountee' or 'forum').[211] Although the nature of this relationship and the actors involved also varies, the accountee shall typically be

[208] Portions of this subsection consist of extracts of a forthcoming publication: J. Alhadeff, B. Van Alsenoy and J. Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', paper presented at the Privacy and Accountability conference organized by the PATS project in Berlin, 5-6 April 2011 (proceedings pending), draft version available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1933731.

[209] See e.g. J. Koppell, 'Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"', *Public Administration Review* 2005, vol. 65, p. 94-99; R. Mulgan, '"Accountability": an ever-expanding concept?', *Public Administration* 2000, vol. 78, p. 555-556.

[210] A. Sinclair, 'The Chameleon of Accountability: Forms and Discourses', *Accounting, Organizations and Society* 20 (1995): 219; M. Bovens, 'Analysing and Assessing Accountability: A conceptual Framework', *European Law Journal* 2007, vol. 13, p. 448.

[211] See also M. Bovens, 'Analysing and Assessing Accountability: A conceptual Framework', *l.c.*, 449-450. Bovens defines accountability as a (social) '*relationship between an actor and a forum, in which the actor has an obligation to explain and justify his or her conduct, the forum can pose questions and pass judgment, and the actor may face consequences*'.

able to call upon the accountor to explain and/or justify its actions.[212] Finally, several authors argue that the *possibility of sanctions* is also a constitutive requirement for accountability.[213] While this view is contestable (on the grounds that it goes beyond the notion of merely 'giving an account')[214], it stands to reason that a relationship in which information is shared without any risk of (unfavorable) consequences whatsoever does not constitute an accountability relationship.[215]

Accountability is a basic principle of data protection law.[216] Recently, this principle has received renewed attention in discussions concerning the future of data protection regulation in the EU.[217] In this context, the principle of accountability has been put forward as a means of ensuring that data controllers 'put in place effective policies and mechanisms to ensure compliance with data protection rules'.[218] The introduction of an explicit provision on accountability would serve mainly two purposes. In first instance, it would serve to reaffirm the responsibility of controllers towards the processing of personal data.[219] In addition, controllers would also be required to demonstrate, upon request, that they have in fact implemented appropriate and effective data protection measures.[220] Under this approach, data protection authorities would have an immediate cause of action if a controller fails to demonstrate that it has implemented such measures.[221] The novelty of this approach would mainly be that, if a controller fails to demonstrate that it has implemented appropriate measures, this would be grounds for a separate enforcement action, independently of an alleged violation of data protection principles.[222]

Enhanced accountability of data controllers can contribute to the realization of the GINI vision in several ways. First, it can contribute to the trustworthiness of the PIM ecosystem in general, by providing additional assurance of compliance with basic data protection norms. This may in turn

---

212 A. Sinclair, 'The Chameleon of Accountability: Forms and Discourses', *l.c.*, 220-221; R. Mulgan, '"Accountability": an ever-expanding concept?', *l.c.*, p. 555-556 (referring to 'rights of authority'); M. Bovens, 'Analysing and Assessing Accountability: A conceptual Framework', *l.c.*, 450.

213 See M. Bovens, 'Analysing and Assessing Accountability: A conceptual Framework', *l.c.*, p. 451; R. Mulgan, '"Accountability": an ever-expanding concept?', *l.c.*, p. 556; A. Schedler, 'Conceptualizing accountability' in A. Schedler, L.J. Diamond and M.F. Plattner (eds.), *The self-restraining state: power and accountability in new democracies*, Rienner, Boulder, 1999, p. 16.

214 R. Mulgan, '"Accountability": an ever-expanding concept?', *l.c.*, p. 556.

215 See also M. Bovens, 'Analysing and Assessing Accountability: A conceptual Framework', *l.c.*, p. 452.

216 Data protection laws institute of a variety of procedural safeguards designed to protect individuals' privacy and to promote accountability by both public and private actors in relation to personal data processing (P. De Hert and S. Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', in E. Claes, A. Duff and S. Gutwirth (eds.) *Privacy and the Criminal Law*, Antwerpen/Oxford Intersentia, 2006, p. 77). Obligations of transparency towards data subjects and oversight authorities are clear examples of such safeguards. In other words, even in instruments where accountability is not called out as a separate data protection principle, many of its substantive provisions are in fact designed to enable accountability.

217 See e.g. Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173, 13 July 2010, 3, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf, last accessed 8 February 2011; European Commission, 'A comprehensive approach on personal data protection in the European Union', *l.c.*, p. 12.

218 *Ibid*, 11. See also Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', *l.c.*, 3.

219 See Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', *l.c.*, 8-9. In this respect the Working Party highlights that that most of the requirements set out in the envisaged provision already exist, albeit less explicitly, under existing laws. (*Ibid*, 10.)

220 *Ibid*, 10.

221 *Ibid*, 16.

222 *Id.*

make individuals more confident that their personal data will not be processed inappropriately by other participants to the PIM ecosystem. It may similarly instil greater confidence in other participants that have a vested interest in ensuring that the processing takes place in a compliant manner.[223] Second, more effective oversight and enforcement of data controllers' operations can help to provide additional incentives for the adoption of PETs, which are also a key component of the GINI vision.[224] A third reason why accountability of data controllers is important concerns the legitimacy and proportionality of processing. Data portability implies data availability. Where an individual is actually free to decide whether or not to consent to a particular processing operation, user control can serve as a privacy enhancement. However, in practice consent can also be used to 'legitimize' excessive data processing.[225] While controllers are obliged to respect the principle of proportionality regardless of whether the user has consented to the processing, additional oversight and enforcement may be needed to ensure that controllers do not overstep their boundaries.

Accountability relationships can take on a myriad of formats. The provisions which have been proposed as part of the data protection reform mainly seek to enhance the accountability of data controllers vis-à-vis data protection authorities. However, the trust framework policies that apply within the PIM ecosystem shall in practice encompass other components than just data protection. Even though many of these components have a nexus with data protection regulation[226], additional accountability mechanisms may (or may not) be needed to secure participant's confidence in their execution. As indicated earlier, there exists a spectrum of mechanisms which can be used to monitor and enforce compliance of the operations that take place within the PIM ecosystem.[227] Strictly speaking, establishing accountability does not require additional regulatory intervention per se: private actors can voluntarily submit themselves to external scrutiny (e.g., through a self-regulatory certification scheme); or existing accountability mechanisms (e.g., regulatory oversight in certain areas, possibility of legal recourse through judiciary) may be sufficient. Finally, it is worth noting that the appropriate level of accountability might also be reached through a mixture of public and private sector accountability mechanisms. These mechanisms can work either in parallel (where participants need to answer to multiple public and/or private sector accountees) or supplementary towards each other (whereby a public sector entity oversees private sector accountees).[228]

It is impossible, at this stage, to determine 'the right formula' of accountability mechanisms that should be in place within the PIM ecosystem envisioned by GINI. The answer to this question is inevitably context-specific, and depends on factors such as:

a) **nature of the trust framework policies** (e.g., were the policies in question decreed by a governmental entity? if not, what is the relationship of these policies vis-à-vis existing regulations and oversight mechanisms?);
b) **scope of the trust framework policies** (e.g., what is the potential harm which may result from failure to comply with the policies in question? what is the sensitivity level of the

[223] See also *supra*; section 2.4.2.1.

[224] Cf. *supra*; section 4.1.1.

[225] See also O. Tene and J. Polonetsky, 'To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising', *Minnesota Journal of Law, Science & Technology*, vol. 13, n° 1, p. 335 et seq.

[226] Cf. *supra*; section 2.4.

[227] Cf. *supra*; sections 2.3.2 and 3.4.2.

[228] For example, within the APEC Pathfinder Privacy Projects the accreditation and oversight of the CBPR is administered either by a local agency or authority of a participating Economy, or by an accountability agent. (see J. Alhadeff, B. Van Alsenoy and J. Dumortier, 'The accountability principle in data protection regulation: origin, development and future directions', *l.c.*, p. 12-13.

transactions involved? how many individuals are affected by the policies? what is the financial value of the resources involved?);

c) **economic interests of participants** (e.g., which incentives do the participants have to forego compliance? do certain participants stand to gain more than others?);
d) **technical safeguards** (e.g., have established technologies been deployed which mitigate the risks of certain forms of misbehavior?);
etc.

As far as data protection and privacy is concerned, it would seem as if the accountability mechanisms currently provided by Directive 95/46/EC have thus far failed to achieve the desired result.[229] Meaningful accountability of actors involved in the PIM ecosystem may therefore also require both legislative (e.g., additional regulatory authority and/or resources for data protection authorities) and non-legislative measures (e.g., increased enforcement). As noted by the JRC report concerning the state of the electronic identity Market:

> "*Interviewees expressed the opinion that (with some exceptions) many EU Member States do not enforce sufficiently rigorously existing regulations, which would encourage the growth or operation of trusted eID. For instance, Directives encouraging organisations to use Privacy Enhancing Technologies (PETs) seem to have no mandatory requirement and no associated penalties, and are perceived as floundering. Moreover, Data Protection Commissioners lack, or choose not to use, the means and powers they need to enforce compliance with data protection regulations. The role, operation and powers of Data Protection Commissioners in regulating eID and ensuring a 'level playing field' across all borders and sectors is fundamental in the success of interoperable eID deployment.*"[230]

4.2 Re-use of PSI

4.2.1 Current enablers, barriers and gaps

Governments maintain a vast amount of information about their citizens. While in practice the quality of this information may vary, it is often presumed to be trustworthy. Many European governments assume the role of primary identity provider (through the issuance of ID cards, be they electronic or paper-based) and/or act as the 'official' source for many basic attributes such as date of birth, current address, marital status, current occupation etc. As a consequence, leveraging the corresponding data registries could enhance the credibility and trustworthiness of the digital identities used within the PIM ecosystem. Relevant data might for instance be included in population, company, vehicle or credit registers, or registers maintained by employment agencies.

In GINI D3.1, we reviewed Directive 2003/98/EC on the re-use of public sector information in order to identify the enablers, gaps and/or barriers it presents for the re-use of personal data held

[229] See e.g. Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173, 13 July 2010, p. 3, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf (last accessed February 8, 2011).

[230] T. Stevens, J. Elliott, A. Hoikkanen, I. Maghiros and W. Lusoli, 'The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies', *JRC Scientific and Technical Reports*, EUR 24567, 2010, at p. 71 (own emphasis).

by public sector bodies within the PIM ecosystem envisioned by GINI.[231] In terms of enablers, we noted:

a) the principle of non-discrimination and the prohibition of exclusive arrangements when making public sector information available for re-use (articles 10 and 11);
b) the transparency obligations of public sector bodies regarding the information they make available for re-use, as well as any applicable conditions (article 7);
c) the requirements for the processing of requests (with regards to time-frame, motivation in case of refusal, specification of means of appeal and redress) (article 4); and
d) the restrictions concerning the conditions under which the PSI is disclosed (articles 5, 6 and 8).

In terms of gaps, we noted the absence of an obligation for Member States to make their documents available for re-use.[232] This entails that in many Member States a great deal of PSI remains unavailable for further for re-use within the PIM ecosystem. We also highlighted the legal barriers which result from the restrictions contained in Directive 95/46/EC, article 8 of the European Convention of Human Rights and articles 7 and 8 of the European Charter. The combined effect of these provisions, together with general principles of public law, is that public sector bodies require a legal mandate before they can release personal data to another entity.[233] As a result, consent of the data subject does not, in and of itself, constitute a valid basis for the disclosure of personal data held by public authorities. While certain Member States have, in their national legislation, explicitly provided that data subjects can authorize the disclosure of PSI relating to them, other Member States have yet to adopt comparable provisions.[234] Finally, we also noted that certain practical barriers exist, which are caused mainly by a general lack of awareness of the public sector about the benefits and risks of opening up their data for re-use.

4.2.2 Regulatory reform

The PSI Directive is currently under review. In December of 2011, the European Commission proposed a number of amendments to the Directive, together with a number of non-legislative measures.[235] Perhaps the most important element of the reform is the requirement that, *as a general principle, all existing documents held by public sector bodies in the EU shall be made available for re-use*.[236] While several important exceptions would still remain[237], this amendment would effectively

[231] See section 5 of GINI D3.1.

[232] Only if Member States (or their public bodies) choose to do so, will they have to comply with the obligations of the PSI Directive and the transposing national legislation.

[233] See GINI D3.1, section 5.2.5.

[234] See C. Dos Santos, C. De Terwangne, et al., 'WG 2 Policy Recommendation 1: Need to complete PSI Directive regarding data protection & privacy provisions', Working draft 4, LAPSI project, November 2011, available at http://www.lapsi-project.eu/wiki/index.php/Policy_recommendation_on_privacy.

[235] See European Commission, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Open data: an engine for innovation, growth and transparent governance', COM(2011)882 final, 12 December 2011 (available at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/opendata2012/open_data_communication/en.pdf) and European Commission, 'Proposal for a directive of the European Parliament and of the Council Amending Directive 2003/98/EC on re-use of public sector information, COM(2011)877 final, 12 December 2011 (available at http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/en.pdf).

[236] See proposed article 3 (1): 'Subject to paragraph (2) Member States shall ensure that documents referred to in Article 1 shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.'

reverse the status quo.[238] For purposes of GINI, the practical impact of this amendment would be that, once implemented in national law, public sector bodies would receive the statutory authority they need in order to make personal information available for re-use. Two important limitations remain however. First, public sector bodies would still need to comply with the aforementioned data protection and privacy requirements (but shall in principle be enabled to disclose personal data on the basis of data subject consent). Second, article 1, 2 c) of the PSI-Directive (which would be retained under the proposed amendments) specifies that this Directive shall not apply to 'documents which are excluded from access by virtue of the access regimes in the Member States'. This restriction could prove to be quite significant, seeing as several registers containing relevant data (cf. *supra*) may prove to be indirectly be excluded from re-use.[239]

Although not directly related to the gaps identified in D3.1, two additional amendments proposed by the Commission are worth mentioning. First, the Commission considers that public sector bodies should be obliged, where possible and appropriate, to make the data available '*in machine-readable format and together with their metadata*'.[240] 'Machine-readable' means that digital documents 'are sufficiently structured for software applications to identify reliably individual statements of fact and their internal structure'.[241] This would not mean that the public sector bodies have an obligation to create or adapt their documents to a machine-readable format in order to comply with a request. However, if such a format is available, it would be deemed the preferred option for making the data available. Both these elements are bound to facilitate the re-use PSI in the context of the PIM ecosystem envisaged by GINI. The final amendment worth mentioning explicitly here is the requirement for an *independent authority* 'that is vested with specific regulatory powers regarding the re-use of public sector information and whose decisions are binding upon the public body concerned'.[242]

The Commission also announced that it will continue to stimulate activities to open up government data through its funding programmes.[243] In particular, the Commission will continue to give financial support to research, development and infrastructure initiatives in the field of open data. Finally, the regulatory reform package also outlines a number of coordinating

---

[237] See revised articles 1, 2 and 3, 2. For instance, one exception to this general principle is made for documents for which libraries (including university libraries), museums and archives have intellectual property rights. For this information, the Member States or the institutions involved can still decide themselves whether they choose to allow re-use or not. If they decide to do so, re-use must be possible for commercial and non-commercial purposes in accordance with the conditions of the directive. This exception does not apply to documents in the public domain held by libraries, museums and archives. These documents fall under the general right of re-use.

[238] Under the current framework Member States have complete discretion in deciding whether or not to allow re-use of public sector documents. Only if re-use is allowed, must they ensure that the documents can be re-used for commercial and non-commercial purposes under the conditions set out in the Directive.

[239] For instance, the Belgian Company Register is publicly accessible online (via http://kbopub.economie.fgov.be/kbopub/zoekwoordenform.html), whereas the National Registry can only be accessed with authorisation from a Sector Committee within the privacy authority by particular organisations for the performance of a public task (see Wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, B.S. 21 april 1984).

[240] See the proposed revisions to article 5, 1.

[241] See proposed article 2, 6.

[242] See revised article 4, 4.

[243] European Commission, 'Open data: an engine for innovation, growth and transparent governance', *l.c.*, p. 9.

measures at Member State and EU level to facilitate exchange of good practice, information and knowledge sharing.[244]

4.2.3 Open issues

While the measures proposed by the EC have the potential to address – at least partially – the gaps and barriers identified in GINI D3.1, several important issues remain. These issues will eventually require additional regulatory intervention before all personal data held by public authorities can be re-used in the context of a PIM ecosystem. In particular, the following issues still need to be considered:

1. **Existing restrictions to access rights**: which national registers shall remain unavailable for re-use 'by virtue of the access regimes within the Member States'? To what extent are the data subjects themselves able to authorize access, notwithstanding the absence of a general right of access/re-use? Is the data in question perhaps rendered accessible through other means (e.g., eID cards/services)?

2. **Data portability for PSI**: should the right of data portability, as defined earlier[245], be extended to cover information held by public sector bodies pursuant to a legal obligation? Would it be reasonable to demand from Member States that their public sector bodies issue electronically signed attestations which enable verifiability of authenticity?[246] Should such a right perhaps be introduced incrementally (e.g., by attribute or sector)?

3. **Regulation of identifiers of general application**: how can national restrictions upon the use of identifiers of general application be accommodated? Given that a harmonized approach to this issue across Member States is unrealistic in the short or medium term, which technical and organizational approaches can be used to ensure that national identifiers are not used by unauthorized entities?[247]

4. **Legal and technical safeguards**: what legal and technical safeguards should be put in place when allowing re-use of PSI constituting personal data? Is a licensing scheme sufficient? Should recipients be required to demonstrate their capacity to comply with certain privacy requirements (e.g., under an accreditation scheme)? Should such requirements vary in light of the role of the recipient (e.g., information broker vs. relying party)? Can the incentive provided by the ability to leverage PSI justify the imposition of a higher standard of data protection?

5. **Verification of compliance of envisaged re-use**: should governments be notified in advance of the finality pursued by the recipients appointed by data subjects, or would this present a greater privacy risk (by providing governments with more information on the types of transactions the citizen is involved in)? Would it be sufficient for governments to receive appropriate assurance of consent by the data subject? Which entity should assess the proportionality of the information disclosure: the source, the recipient, an independent regulator, or a combination of these entities?

---

[244] *Ibid*, 10-11.

[245] Cf. *supra*; section 4.1.2.

[246] The other open issues identified in relation to data portability in general (i.e. interoperability, reliability, liability) also apply here.

[247] See also GINI D3.1, section 4.10.

6. **Accountability and harmonization**: should a dedicated regulator be created at the level of each Member State to oversee re-use practices? Or should such oversight be observed by existing regulatory authorities (e.g., DPAs)? How will consistency in decision-making be ensured across Member States in order to prevent fragmentation?

The open issues highlighted here illustrate the absence of any (detailed) alignment between the data protection and PSI frameworks respectively. These issues should be tackled through regulatory intervention at EU level.[248] Several of these issues might be addressed through non-legislative measures (e.g., by issuing additional guidance).[249] Others, such as the possibility of a general right of data portability for PSI (notwithstanding restrictions to access in national legislation), are likely to require legislative measures if one wishes to ensure a more uniform and consistent approach across Member States (as the relevant national legislations will otherwise continue to be fragmented).

4.3 E-Signatures

4.3.1 Current enablers, barriers and gaps

In GINI D3.1, we reviewed Directive 1999/93/EC on a community framework for electronic signatures[250] in order to identify the enablers, gaps and/or barriers it presents for the realization of the GINI vision. There we concluded that the 'certification services' envisaged by GINI shall in principle fall outside the current scope of this Directive. Even if it were accepted that certain participants to the PIM ecosystem act as certification service providers within the meaning of this Directive, the practical relevancy of this conclusion would still be limited. This is because the existing provisions of the E-Signature either

(a) deal only with electronic signatures as a legal concept;
(b) only regulate the activities of CSPs issuing qualified certificates;
(c) have similar counterparts in other regulatory instruments (e.g., in the E-commerce Directive); or
(d) impose requirements which are an integral part of the GINI vision (e.g., reliance upon consent).[251]

We did not observe any immediate legal gaps. We concluded that the need for additional regulation (through legislative measures) of the services envisaged by GINI would primarily arise to the extent that there would be:

- a specific need to derogate from the contractual freedom of parties in order to attain a legitimate policy objective; or
- a rationale arises for policymakers to increase the trustworthiness of services envisioned by GINI in order to stimulate their acceptance in an 'open' environment.[252]

[248] See also European Data Protection Supervisor, 'Opinion on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents', 18 April 2012, available at http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/478 (last accessed 20 April 2012).

[249] See also See C. Dos Santos, C. De Terwangne, et al., 'WG 2 Policy Recommendation 1: Need to complete PSI Directive regarding data protection & privacy provisions', *l.c.*, section V.

[250] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, *O.J.* 19 January 2000, L 13/12-20.

[251] See GINI D3.1, section 7.11.

4.3.2 Regulatory reform

In 2010, the EU Commission announced a revision of Directive 1999/93/EC on electronic signatures as one of the key actions of its Digital Agenda. The goal of this revision would be 'to provide a legal framework for cross-border recognition and interoperability of secure eAuthentication systems'.[253] This policy objective was echoed in a subsequent communication, in which the Commission announced its intention to propose legislation to "provide a common legal base for mutual recognition of e-authentication and electronic signatures across borders".[254]

In 2011, the 'Feasibility study on an electronic identification, authentication and signature policy (IAS)' was launched. The aim of this study is to evaluate '*the feasibility of a comprehensive EU legal framework that would gather all the identification-related electronic credentials needed to secure electronic transactions as well as the ancillary services needed to use them: electronic identification, authentication, signature, seals, certified delivery and a voluntary official email address.*'[255] It shall also assess '*which provisions of the current e-signature framework established by Directive 1999/93/EC could be adapted or expanded to cover wider IAS requirements*'. In its first public report, the IAS study team outlined the following policy options for further consideration:

- no regulatory intervention;
- a single comprehensive legal framework (an 'IAS Directive', with national 'IAS supervisory bodies' and European generally recognized 'IAS standards');
- a lighter, simpler eSignatures framework (e.g., based on the 2001 UNCITRAL Model Law on Electronic Signatures), at the exclusion of any other IAS services;
- a light IAS framework based on the New Approach regulatory style;
- making only minimal changes to the E-Signatures Directive to address some of the shortcomings mentioned above, but without further touching upon other IAS services;
- adopting (a mixture of) separate directives (or other regulatory instruments) for each IAS service to be covered as the need is recognized (an E-Signatures Directive/Decision, an eID Directive/Decision, a Timestamping Directive/Decision, etc.).[256]

Regulation of identification and authentication services as is being considered in the context of the E-Signature review has the potential to impact many of the 'certification' services envisaged by GINI. In the following section we will consider arguments for and against the additional regulation of these services, in particular those provided by the INDI Operator.

---

[252] See GINI D3.1, section 7.12. This conclusion was based on the fact that the trust model in the PIM Ecosystem envisioned by GINI is an operator-based trust model (i.e. a 'brokered' trust relationship). In order to connect to the INDI infrastructure/network, an entity must have a contractual relationship with at least one INDI Operator. This contractual relationship should be sufficient for reaching the whole INDI space. In other words, the PIM Ecosystem envisioned by GINI is a 'closed system', which allows the relevant parties to specify the terms and conditions under which the services shall be offered..

[253] European Commission, 'A Digital Agenda for Europe', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 19 May 2010, COM(2010) 245, p. 11, available at http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

[254] European Commission, 'A roadmap to stability and growth', Communication from the Commission, Brussels, 12 October 2011, COM(2011) 669 final, p. 6

[255] Tender Specification of 'Feasibility study on an electronic identification, authentication and signature policy (IAS), public tender nr. SMART 2010/0008 p. 3 (own emphasis), available at http://www.iasproject.eu/attachments/File/admin/ias_study_tender_spec_final.pdf.

[256] DLA Piper, Sealed, time.lex, PriceWaterhouseCoopers, SG&A, 'IAS in the European policy context, Deliverable D1.1, draft version, 28 September 2011, p. 68-69, available at http://www.iasproject.eu/docs.html.

4.3.3 Regulation of INDI Operators?

The PIM ecosystem envisioned by GINI is based on a network of INDI Operators. The main role of these operators is to act as trust mediators. The services are designed to provide other entities within the PIM ecosystem with the assurances they need in order to enable the disclosure and reliance upon identity information; even where those parties involved do not have pre-established trust relationships. Such assurances might extend to: the identity of the entities involved in a transaction (individual end-user - Data Source – Relying Party), authorization by the individual end-user (data subject consent), authenticity and/or reliability of data presented towards relying parties, etc.[257]

Discussions with stakeholders have revealed that arguments can be made both for and against regulation of INDI Operators at EU level. The most contentious issue is whether or not use of additional *legislative* measures is deemed necessary in order to realize the GINI vision. Over the following paragraphs, we shall provide an overview of the main arguments made either in favour or against the regulation through legislative measures. This initial overview seeks to be descriptive only (i.e., it does not evaluate the merits of each argument). After this overview is completed we shall outline our position on what we believe to be the best way forward.

The main arguments advanced in favour of legislative measures regulating the services of INDI Operators are that such regulation could:

1. **Promote interoperability/Internal Market**: by decreeing trust framework policies at EU level, a European legal framework could reduce fragmentation and subsequent interoperability barriers among (national, regional, sectorial, …) trust frameworks (e.g., because otherwise assurance levels might be defined in a totally proprietary way); which will in turn contribute to a smoother functioning of the Internal Market.

2. **Ensure fairness**: by participating in the definition of trust framework policies, EU policymakers could help ensure that these policies appropriately balance the various interests at stake (e.g., by providing a fair allocation of responsibilities among the participants to the Ecosystem, by defining adequate security levels, by imposing a baseline quality of service, etc.)

3. **Improve legal certainty**: provided it is drafted in a clear and unambiguous manner, the legal framework could provide participants to the ecosystem with greater confidence with respect to the (il)legality of policies/operations within the ecosystem, the liability exposure of each participant[258], the evidentiary value of records maintained, etc.

[257] See GINI D3.1, section 2.2 – 2.3.

[258] See also T. Stevens, J. Elliott, A. Hoikkanen, I. Maghiros and W. Lusoli, 'The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies', *JRC Scientific and Technical Reports*, EUR 24567, 2010, at p. 72: "*One of the obstacles to eID growth has been determining who – or which organisation – is responsible for what happens when things go wrong. Where interoperability is established, emerge issues of dispute resolution (agreeing the authority that has the ultimate decision on resolving problems) and liability management (a legally binding framework to ensure that all parties understand who will recompense what level of loss arising from failures in the system). If these issues are not addressed, trust in interoperability will eventually be eroded as disputes grow. A central European authority to resolve disputes and enforce liability decisions would become a powerful force in encouraging interoperable eID growth*".

4. **Enhance trust(worthiness)**: provided effective accreditation and/or oversight mechanisms are put in place, the legal framework could provide ecosystem participants with greater confidence that fellow participants shall behave in accordance with trust framework policies. For instance, end-users might feel more confident knowing that the activity of the INDI Operator is regulated and monitored more strictly than other services. Similarly, Data Sources and Relying Parties might feel more confident that the INDI Operator is in fact acting on behalf of a particular data subject.

5. **Promote a common eID infrastructure:** one of the main reasons why the eID services envisaged by GINI are yet to flourish is the absence of a harmonized, interoperable and shared eID infrastructure. This causes barriers for both market development and entry (e.g. high up-front costs, insurmountable diversity) which shall be removed once the requirements and policies for these services have been defined at EU level ('if you build it, they will come').

On the other hand, there are also a number of arguments that can be used to advocate against the adoption of legislative measures regulating the services of INDI Operators:

1. **'Closed' system**: the PIM Ecosystem envisioned by GINI is a 'closed system', in which each entity has at least one contractual relationship with an INDI Operator. Parties are therefore in principle able to agree upon trust framework policies as they see fit (e.g., through contractual frameworks); in light of the services involved and the context in which they are provided.

2. **Market considerations**: the business case for user-centric identity management solutions as stand-alone services remains uncertain. At this stage, it is better to limit regulatory intervention to generic, high-level requirements (e.g., as contained in data protection legislation) and allow the market to develop before introducing specific legislative measures.[259] Otherwise one might risk 'regulating the market to a standstill' before it is actually operational.[260]

3. **'One size does not fit all'**: the security needs of each application are by definition context-specific. Top-down regulation, even if it provides considerable flexibility, runs the risk of disregarding 'local' needs with respect to identification and authentication. Security should remain a risk-driven rather than compliance-driven exercise: safeguards should serve the actual needs of an application rather than satisfy centrally defined policies which may add burdens without having a commensurate benefit.

[259] See also T. Stevens, J. Elliott, A. Hoikkanen, I. Maghiros and W. Lusoli, 'The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies', *JRC Scientific and Technical Reports*, EUR 24567, 2010, at p. 73: "*The majority of eID systems in use today are specific to particular applications, communities, or nations. In the absence of a well-defined and accepted business case that proves the value in harmonisation and interoperability of eID, no organisation or government is willing to speculatively invest in the necessary standards and 'pump priming' to catalyse the eID market.*"

[260] See also Ian Walden, 'Regulating Electronic Commerce: Europe in the global e-conomy', *European Law Review* 2001, vol. 26, at p. 546-547: "*One principle that would seem to stand the test of time, however, is that of allowing law to lag behind developments, rather than try to anticipate markets. The focus of the Electronic Signatures Directive on certification services, as the basis of a trust industry perceived critical to the mass take-up of electronic commerce, seems, to date, to be an example of how policy-makers can effectively regulate a market to a standstill.*"

4. **Regulation should be used to enable, not to micro-manage**: EU policymakers should limit themselves to ensuring that undesirable (internal) market barriers are removed; and refrain from defining prescriptive requirements which may potentially stifle the development of innovative practices, policies and services. To date, there is no national legislation which poses a barrier to the free movement of services envisaged by GINI within Internal Market, so there is no need for intervention at EU level.

While each of these arguments is endowed with practical considerations, many of them also seem to reflect different ideological viewpoints. Most of the arguments against legislative measures support a more liberal economic ("laissez-faire") approach; whereas the arguments in favor seem to suggest that the market will deliver a sub-optimal result in the absence of legislative measures (e.g., lack of interoperability or competitive market for user-driven eID services). The latter category of arguments also seems to implicitly assume a positive role for government as an enhancer of trust (e.g., through oversight, the provisioning of legal backstops) and/or as a market enabler (e.g., by putting in place a common eID infrastructure).

In our view, realization of the GINI vision does not require regulatory intervention through legislative measures per se, at least not towards the private sector. A strong case may, however, be made for other forms of regulatory intervention in order to ensure the necessary building blocks emerge. For the public sector, the situation is slightly different, and regulatory intervention through legislative measures may indeed be appropriate. Each of these elements shall be elaborated further over the following paragraphs.

Much of the legal framework that is necessary to enable the realization of the GINI vision is already in place. The Data Protection Directive contains most of the requirements necessary to secure fair processing of end-users' data, and has put in place a framework which enables oversight and enforcement by regulatory authorities. It is true that there are areas for improvement; both in terms of the rights of data subjects and data controller obligations (cf. *supra*; section 4.1). However, these elements are situated at a higher level of abstraction and are of broader applicability than the provisioning of services by INDI Operators. The E-Commerce Directive, from its part, has put in place a framework which allows information society services to move freely within the internal market by instituting the 'country of origin' principle and by restricting Member States from subjecting the provisioning of such services to prior authorization.[261] While practical issues towards the realization of the GINI vision still exist (e.g. in terms of interoperability, viable business cases, etc.), these matters are better resolved through non-legislative measures or simply left to the market. For example: real interoperability across organizations is something which requires a mutual understanding on many different elements: the technical standards to be used, proper alignment of business processes, semantic interoperability, etc. The level of detail and specificity at which this mutual understanding must be reached makes it ill-suited for top-down regulation through legislative measures. As a result, we believe that the legislative framework should limit itself to minimum harmonization of high-level requirements (e.g. as contained in the Data Protection Directive) and removal of actual legal barriers on a sectorial level, rather than prescribe detailed requirements for the provisioning of INDI services in general.

The actual legal barriers towards the realization of the GINI vision are limited. These barriers all revolve around two main issues. The first issue is the absence of a regulatory framework which enables and promotes the re-use of PSI pursuant to a data subject request.[262] Legislative measures

[261] Articles 3 and 4 of the E-Commerce Directive. See also GINI D3.1, section 6.3-4.
[262] See also GINI D3.1, section 5.4.

at EU level may be necessary in order to ensure that relevant identity data held by public sector bodies can be leveraged effectively throughout the EU.[263] A second reason to consider adoption of legislative measures towards the public sector bodies is to ensure that they receive the legal mandate they need to participate in the PIM Ecosystem. This mandate should not only comprise the ability to make available PSI to authorized recipients, but also enable them to interoperate with eID credentials other than those issued by their own national governments.[264] From a practical perspective, it may be more effective to elaborate these frameworks around specific use cases, rather than imposing a uniform approach which would apply across sectors. Legislative measures would then be directed at enabling and securing the involvement of Member States in a given application; whereby the corresponding technical and organisational components are developed in parallel at EU level (which must in turn be accompanied by a comprehensive legal framework).[265]

While a legal framework dedicated to the provisioning of INDI services may not be needed, other forms of regulatory intervention (in addition to those highlighted in the previous sections) should be considered. In particular, EU policy makers should consider committing resources towards[266]:

1. **Co-ordination:** through use of OMC, raise consensus with stakeholders regarding the key objectives for eID schemes, exchange best practices, disseminate information about successful business practices concerning user-driven identity management solutions;

2. **Standardization:** promote the consistent use of open standards by Member States, commit resources towards the development of standards that help make the various components of identity trust frameworks operational and interoperable, preferably at an international level;

3. **Large-scale pilots:** encourage the development of pan-European user-centric identity services through large scale pilots; possibly in the form of public-private partnerships.

[263] The open issues to be addressed in this respect were highlighted earlier in this deliverable: cf. *supra*; section 4.2.1.

[264] For instance, Austria has already adopted a legal basis for the recognition of foreign eIDs. See also GINI D3.1, section 4.8.3.

[265] A successful example of such an approach is provided by the Internal Market Information system (IMI). While the Professional Qualifications and Services Directives provides the necessary legal bases to secure Member States' involvement, the common infrastructure to make these provisions operational was designed at EU level. For more information see http://ec.europa.eu/internal_market/imi-net. See also Van Alsenoy B., Kindt, E. and Dumortier, J., 'Privacy and Data Protection Aspects of e-Government Identity Management', *l.c.*, p.266-273.

[266] See also T. Stevens, J. Elliott, A. Hoikkanen, I. Maghiros and W. Lusoli, 'The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies', *l.c.*, 79-80.

5 Conclusion

Establishing and maintaining trust in online digital identities can become quite complex as soon as one attempts to extend their scope of application beyond their initial boundaries. Many variables need to be accounted for, each of which has the potential to either enhance or undermine the trust of the entities concerned. In recent years, the concept of an 'identity trust framework' has emerged as a vehicle to outline the various components that are deemed necessary in order to establish trust in online digital identities. From a practical perspective, the main objective of a trust framework is to provide participants in a given (eco)system adequate assurances with respect to the proper functioning of the system. These assurances in turn serve to make the system 'trustworthy' to such an extent that the participants of the ecosystem will feel comfortable engaging in transactions with one and other.

Trust frameworks display considerable similarities with certain forms of regulatory intervention. For instance, 'rule-making' and 'oversight' are functions typically associated with legislative, executive and judicial branches of government. However, provided they do not contravene provisions of mandatory law, private actors are free to organize their mutual relationships as they see fit. As a result, the relationship between regulatory measures and a given trust framework may vary. It may be expected that trust frameworks shall operate as subsystems within the broader legal system, whereby the actual degree of proximity (or overlap) with the regulatory framework may vary. In practice, regulatory measures can be used to influence trust frameworks in mainly two ways. In first instance they may constrain the behavior of the private and or public actors involved. Second, the may be used to provide incentives and/or co-ordination in order to either (a) promote the emergence of one or more trust frameworks and/or (b) align their functioning with one or more policy objectives. The evaluation of which type of regulatory instrument is best suited to attain a particular policy objective needs to be made on a case-by-case basis. More often than not, the optimal approach will lie in a combination of different regulatory instruments.

Much of the legal framework that is necessary to enable the realization of the GINI vision is already in place. The Data Protection Directive contains most of the requirements necessary to secure fair processing of end-users' data, and has put in place a framework which enables oversight and enforcement by regulatory authorities. While it is true that there are areas for improvement within the current framework, these issues are situated at a higher level of abstraction and are of broader applicability than the provisioning of services by INDI Operators alone. Recommended areas of regulatory intervention include: privacy enhancing technologies, data portability, and accountability of data controllers. Both legislative and non-legislative measures shall be necessary in order to secure effectiveness of these interventions.

The actual legal barriers or gaps towards the realization of the GINI vision are limited. These barriers and gaps all revolve around two main issues. The first issue is the absence of a regulatory framework which enables and promotes the re-use of PSI pursuant to a data subject request. Legislative measures at EU level may be necessary in order to ensure that relevant identity data held by public sector bodies can be leveraged effectively throughout the EU. The second legal barrier concerns the absence of a legal mandate for public sector bodies to participate in the PIM Ecosystem. If created, such a mandate should comprise both the ability to make available PSI to authorized recipients, as well as the ability to interoperate with foreign eID credentials. From a practical perspective, it may be more effective to elaborate these frameworks around specific use

cases, rather than imposing a uniform approach which would apply across sectors. While a comprehensive legal framework dedicated to the provisioning of INDI services as such may not be needed in the short or medium term, EU policy makers should consider committing further resources towards the co-ordination, standardization and piloting of user-centric, privacy enhancing identity management services in both private and public sectors.