SEVENTH FRAMEWORK PROGRAMME
Challenge 1
Information and Communication Technologies

Trusted Architecture for Securely Shared Services

Document Type:	Deliverable
Title:	**Requirements: Privacy, governance and contractual options**
Editors:	Joseph Alhadeff, Brendan Van Alsenoy
Work Package:	WP6
Deliverable Nr:	D6.1
Dissemination:	PU
Preparation Date:	December 31, 2010
Version:	3.0

The TAS³ Consortium

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

Contributors

	Name	Organisation
1	Joseph Alhadeff	ORACLE
2	Brendan Van Alsenoy	KUL (ICRI)
3	Griet Verhenneman	KUL (ICRI)
4	David Chadwick	KENT
5	Luc Vervenne	SYN
6	Quentin Reul	VUB

Contents

1 Executive Summary

TAS3 is designed to provide a secure and trusted architecture that is compliant with applicable privacy requirements. TAS3 goes beyond traditional privacy by design to include design of privacy in not only in the technical design, but also in business processes, organizational policies and in a privacy enabling contractual framework from the outset. The TAS3 architecture thus combines the four elements of technology, business, policy and legal requirements to provide a privacy-enabled ecosystem.

The focus of this deliverable is to identify the privacy requirements that are set forth in the European Directive and national implementations that support the fundamental right of privacy. TAS3 D6.2, which sets forth the Contractual and Policy Frameworks, will incorporate and build on these requirements. . As part of this design approach we also review the "7 laws of embedded identity", as developed by Information and Privacy Commissioner Ann Cavoukian in furtherance of Kim Cameron's first published seven Laws of Identity.

The purpose of this deliverable is to translate the broad legal requirements related to privacy and governance into concepts that can provide technical and organizational guidance. Annex 1 provides a comparative review of the major instruments on which EU privacy law is founded as well as the laws of countries in which TAS3 may take place. From those documents common principles are distilled. The deliverable then maps the application of those principles and related terms of art to new technologies to illustrate the challenges that are emerging. Then, before concentrating on the specific requirements of the Directive, we review emerging global and EU trends in accountability and accountable systems. More detailed legal requirements are then identified and cross-referenced to TAS3 functions and practices (Summarized in Annex 3). Finally an overview of requirements and their operational relevance is given.

In order to maintain the currency of the document, periodic annexes will be included to provide updates on trends and emerging concepts related to privacy requirements. The provision of annexes also helps readers focus on developing trends that may impact the requirements. As these developments become more established, or codified, the will be integrated into the paper.

This document represents the beginning of an iterative process, which will continue throughout the TAS3 project by way of refinement and supplement. Apart from tracking changes in actual law and the application of existing law, more detailed research will be performed related to relevant sectoral laws, which may also impact privacy requirements (e.g. employee privacy rights; regulations impacting electronic health records).

2 Introduction

TAS3 is designed to provide a secure and trusted architecture that is compliant with applicable privacy requirements. This concept, often referred to as "privacy by design", has been an important topic in recent years within privacy and technology development communities. 'Privacy by design' typically focuses on building privacy protections into technology at the design stage. TAS3 goes beyond traditional privacy by design to include from the outset the design of privacy compliant business processes and organizational policies, which are in turn also supported and bound by a privacy enabling contractual framework. The TAS3 network thus combines the four elements of technology, business, policy and legal requirements to provide a privacy-enabled ecosystem.

The focus of this deliverable is to identify the privacy requirements that are set forth in the European Directive and national implementations that support the fundamental right of privacy. One of the purposes of this deliverable is to describe a common set of obligations in a way that is accessible to different stakeholder communities: end-users, system developers, businessmen and policymakers. As part of explaining these obligations, we will also present them in a context that is relevant to our global information society, as well as the challenges it creates towards individuals for the exercise of their rights; and towards governments in the enforcement of their laws. The TAS³ Contractual and Policy Frameworks (D6.2), will incorporate and build on these requirements.

It is important to have a deliverable dedicated to the analysis of legal privacy requirements for TAS3, as this is a field of significant activity. Within the EU, the Data Protection Directive is currently under review. New concepts of accountability are being considered both as part of that review, as well as in a number other projects that have been undertaken by various data protection authorities. Consideration is also being given on how to develop accountable systems that provide greater privacy and security which may in turn enhance trust. This work is considered essential to deal with the ever-increasing globalization of information flows and seamless introduction of technology into our daily lives. The increasing complexity of information flows, processing and value chains makes it more difficult for individuals to understand how to exercise their privacy rights. A design approach geared to embedding support for security and privacy in the technical architecture, legal contracts, and policy requirements can enhance trust by creating a privacy-enabled ecosystem. TAS3 among other projects of FP7 serve as test beds for ideas, processes, policies, contracts, and of course, technology related to the development of accountable systems.

3 Privacy fundamentals

Since the time of the philosophers of ancient Greece, people have been trying to define privacy and to differentiate public from private life. In 1967 Alan Westin published an influential study on privacy entitled 'Privacy and Freedom'[1] in which he reviewed many anthropological studies of societal approaches to personal information and proposed that privacy was:

> *"[…] the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."*

This definition of privacy has been influential in that it clearly identified some of the control parameters, which have become the hallmark of today's major legal instruments on privacy.

In the EU, the concept of privacy was taken up in a slightly broader context, namely the fundamental right of "data protection". The five main documents that create the foundation of data protection in the EU today are:

- The Council of Europe's European Convention on Human Rights 1950 ["ECHR"], and in particular, article 8 on the right to privacy,[2]
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) ["OECD Guidelines"][3],
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.I.1981)[4] ["COE Convention"]
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[5] ["Directive"]
- EU Charter of Fundamental Rights of the European Union; Article 7 [EU Charter][6]

It should be noted that both the OECD Guidelines and Directive 95/46/EC are currently under review and may be revised within the next couple of years[7].

The concept of data protection as used in these main foundation instruments considers privacy one of the fundamental freedoms that are to be protected. The document most relevant to our current analysis, the Directive, built upon the previous documents and embodies a pan-European set of privacy requirements. The Directive must be, and has been, implemented into the national law of each

[1] A. Westin, 'Privacy and Freedom', New York, Athenaeum Press, 1967, p.7
[2] http://conventions.coe.int/treaty/EN/Treaties/html/005.htm
[3] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[4] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
[5] Directive 95/46/EC on the protection of individuals with regards to the processing of personal data and on the free movement of such data, Official Journal of the European Union, n° L 281, 23 November 1995. pp. 31-50. See also http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
[6] O.J. 18 December 2000, C 364/1-22, available at http://www.europarl.europa.eu/charter.
[7] See Infra: Annex V 2009 Privacy Update at p. 61

of the Member States of the EU[8]. As such, there are variances in the national implementations and interpretations among Member States, with the Directive serving as the benchmark for review. The variability of this process entails that the requirements defined at the national level can be more detailed, and in some cases even more restrictive, than those initially set forth by the Directive.

The UK and the Netherlands, the Member States focused on in the TAS[3] architecture, have both implemented the EU Privacy Directive in the following national laws:

- Data Protection Act 1998 1998 CHAPTER 29[9]
- Personal Data Protection Act (Wet Bescherming Persoonsgegevens, or the 'WBP') 2001[10]

In both cases, there is great commonality in the adoption of the EU Privacy Directive with greater and lesser details specified in the drafting. A high-level comparison of major principles and requirements of all five instruments mentioned above is provided in Annex 1.

The importance of the ECHR and European Charter is that they anchor the more privacy specific rights articulated in the Directive and COE Treaty into the fabric of fundamental and human rights. The OECD Guidelines, COE Treaty and Directive were all passed as a reaction to increased automation in data processing, which also entailed the movement of more data across borders. At the time, most of that processing was carried out in the form of Electronic Data Interchange (EDI) that involved simple batch processing and point-to-point transfers of information across borders. Company A in country A would send information to Company B in Country B, which would return it when the processing was complete. All of the documents outlined above also share three main goals:

- The protection of privacy and other fundamental rights in these new automated processing environments,
- Harmonization of requirements, and
- Enabling the free flow of information; as there was recognition of the benefits of these transfers if done responsibly.

As is evidenced by the matrix in Annex 1, Apart from sharing general objectives, the Foundation documents referenced above, also shared a common set of principles/concepts ("Common Privacy Principles"):

1. Personal data should only be collected/processed for fair and lawful business purposes.
2. The purpose(s) for processing personal data must be clearly specified.

[8] All members of the Council of Europe are also expected to abide by Article 8 of the ECHR.
[9] Data Protection Act of 16 July 1998, 1998 Chapter 29, available at http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.
[10] Wet van 6 juli 2000 houdende regels inzake de bescherming van persoonsgegevens ('Law of 6 July 2000 containing rules concerning the protection of personal data'), available at http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp.shtml?refer=true&theme=purple.

3. The collection of personal data related to those purposes must be relevant, non-excessive and maintained in identifiable form only as long as needed to accomplish the specified purpose
4. Retention of data must only be for the limited time needed to accomplish the purpose(s) of collection
5. Personal data must be accurate and, where needed, up-to-date.
6. Use, and subsequent use, of personal data cannot be incompatible with the purposes specified and should be with the consent[11] of the data subject
7. Appropriate security (technical and organizational) measures against unauthorized/unlawful/accidental access; modification, disclosure, destruction, loss or damage to personal data must be in place.
8. Controllers and processors have duties to maintain the confidentiality of personal data.
9. Processing of sensitive data may be subject to greater restrictions.
10. Data subjects have the right to know what types of data are being maintained and have the right to access and demand correction of their personal data, as well as object to further processing.
11. Transfers of data outside of the EU may be subject to controls, limitations (adequacy) and requirements of accountability[12].

It should be noted that while the notion of accountability are inherent in all of the documents referenced above, the Directive and the national laws that implement it have focused on the need to have so-called "adequacy findings" (a finding at governmental level that the law of the place of processing is "adequate"). Adequacy as a concept is primarily relevant in case of transfers outside of the EU, so this deliverable will not focus in great detail on the adequacy requirement; except when describing future trends (see section 4).

3.1 Definitions

The Foundation documents mentioned above have also spawned their own language of privacy. Since this deliverable is focused on legal requirements within the EU, we shall focus on the most important definitions of the Directive.[13]

It remains to this day difficult to find a meaning of privacy that is not significantly bound to a particular subjective or cultural perspective. For example, privacy in some Asian cultures, which tend to focus more on the collective, appears to place great emphasis on the preservation of reputation rather than on individual rights as such. Notwithstanding such difficulties, the governmental authorities charged with the enforcement of privacy rights[14]

[11] It should be noted that consent often bears important adjectives of clear, unambiguous or explicit. From a technical point of view, this requires that the user "opt in" to the collection of personal information.
[12] Please note that while this issue is perhaps the most contentious and important in the global/multinational context it is less relevant to TAS[3] and will not be the subject of significant discussion.
[13] See art. 2 of Directive 95/46/EC. For all of the definitions referenced in this section.
[14] These governmental agencies may include, Data Protection Authorities, Information Commissioners and Data Protection Supervisors; Data Protection Officers may supplement them at the organizational level.

needed to concur on what data required protection. Within the EU and specifically under the Directive, personal data is defined as:

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

While this definition appears to be relatively straightforward, its application to more contemporary technologies has introduced significant challenges. For instance, considerable debate emerged with regards to the question of whether this definition of personal data also included technical elements such as IP Addresses. The Article 29 Working Party has provided guidance in its opinion on data protection issues related to search engines and has found that IP addresses can be considered personal data in some circumstances.[15] Whether use of an IP address is permissible is a determination contingent on the type of processing, nature of the data, the type of entity performing the processing, and whether it's based on consent. These contingencies also provide a summary of other important terms defined in the directive.

"Processing" of personal data under the Directive is understood as:

> "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*"

The definition of processing is important to consider because the list of examples of what may constitute a processing activity provides a substantial breadth of the types of activity to which the Directive may apply.

The next natural term to define is that of "processor" which in the Directive is defined as:

> "*a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller*"

This is a somewhat circular definition, as it refers to undertaking any of the acts defined as processing on behalf of an entity called a controller. A "controller" under the Directive is in turn defined as

[15] Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines, 00737/EN WP 148, 4 April 2008, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf. The Article 29 Working Party has since then also issued a more comprehensive opinion on the concept of personal data: see 'Opinion 4/2007 on the concept of personal data', 01248/07/EN WP 136, 20 June 2007, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf.

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

Read in conjunction, the controller is the party deciding on the means or purposes of the processing. A number of issues are raised with these terms and their applicability to modern business transactions and information flows, like outsourcing[16]:

> "*It is often difficult to determine in practice which party is the controller and which is the processor, although it is a fundamental issue. The Data Protection Directive (EC/95/46) characterises the test of a controller in terms of the degree of discretion or decision-making authority exercisable by that party in relation to the data it processes. The party which decides the purposes and means of the processing will be the controller.*
>
> *The difficulty many organisations face in practice is that their business operations are dynamic. Businesses operate in an increasingly collaborative manner and the nature of relationships changes over time. A party that was once merely a processor might, over a period, assume a greater degree of responsibility in relation to the data. This might occur as a result of additional services being added or new technology being deployed. More subtly, as the relationship develops, the processor may simply be entrusted with greater discretion in relation to the data.*"

Lastly, but also of significant relevance, both within the Directive and towards the TAS[3] network is the concept of "consent". As defined in the Directive, consent means:

> "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*"

Under the Directive, consent is a mechanism of central importance, which enables data subjects to exercise their rights. The hallmarks of consent are that it be freely given and informed. Interestingly, consent is also being challenged as an effective way to exercise one's privacy rights. The Article 29 Working Party has called into question whether consent in employment and other scenarios can be freely given because of the potential for negative consequences and the imbalance in power that exists between employers and (prospective) employees.[17] TAS[3] may be of some assistance in levelling the playing field and re-enabling consent. The user-centric nature of TAS[3] coupled with the ability to support anonymity and partial identities within a legal and governance framework

[16] Treacy, Bridget, 'Lessons from SWIFT: the 'controller' vs 'processor' dilemma", Complinet, 9 January 2008, available at http://www.hunton.com/files/tbl_s47Details/FileUpload265/2103/Treacy_SWIFT_1.08.pdf

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

designed to enhance privacy compliance, may help alleviate some of the concerns related to whether consent is freely given.

4 Privacy and the Information Society in Context

As noted in Alan Westin's definition of privacy, how, when and what control should be exerted are critical elements of consideration. This concept of control has also been credited as a partial source of today's greater focus on user-centric systems that enhance user control. Today, previous notions of control are being reconsidered in light of the information society we live in, in which more and more aspects of everyday life are being integrated in a digital environment. Information about people is more widely available through search engines, social networks, and the near-ubiquity of technology. The EU is currently working on Guidance related to the so-called 'Internet of Things'[18]– looking to a future where objects, services and people are all interconnected. Information flows are ever more global and the concept of point-to-point access to information has been replaced by the concepts of 24x7x365 service and global access to information that allow global companies to support global corporate clients and increasingly mobile individual customers.

A small group of researchers at the World Wide Web Consortium (W3C) has been working on models of information accountability and use-based controls as tools to remedy the limitations of the current notice and consent based models in the age of ubiquitous computing. The main concern is that so much information exists beyond the direct control of the data subject, and even the traditional data controllers, that notice and choice models that rely on consent are no longer sufficient.[19] Use-based control models supplement notice and choice by imposing limitations on the use of information, which might cause harm or create adverse impacts to the data subject.

4.1 Accountability

In light of the growing realization that the notice and consent model has limitations in the Information Society, there is growing interest in the concept of accountability. While Accountability is a principle inherent in the OECD guidelines, it clearest articulation has been made in PIPEDA[20] (the Canadian privacy law):

> *"An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."*

[18] Santucci, Gerald, *From Internet of Data to Internet of Things*, Paper for the International Conference on Future Trends of the Internet, 28 January, 2009, http://ec.europa.eu/information_society/policy/rfid/documents/Iotconferencespeech012009.pdf

[19] Weitzner, Abelson, Berners-Lee et al., Information Accountability Communications of the ACM, June 2008/Vol 51, No 6

[20] http://laws.justice.gc.ca/PDF/P-8.6.pdf

This concept of accountability is also the organizing principle for the APEC (Asia Pacific Economic Cooperation) Privacy Framework[21].

> *"A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."*

While it is contemplated that many APEC Economies will continue to require consent related to the collection and use of information, there was a deliberate use of the word "or" to provide a potential alternative rationale for transfer and processing - to use due diligence and reasonable steps to ensure the consistent treatment and processing of the information. At the heart of accountability is the concept that *obligations flow with the information*.

In recent guidance on obligations related to cross border data transfers, the Canadian privacy Commissioner highlighted the rationale for accountability and differentiated it from the EU approach of adequacy[22]:

> *"As the legislation itself states, PIPEDA is intended to 'support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances…' This acknowledges that proper protection of personal information both facilitates and promotes commerce by building consumer confidence. Today's globally interdependent economy relies on international flows of information. These cross-border transfers do raise some legitimate concerns about where personal information is going as well as what happens to it while in transit and after it arrives at some foreign destination. Consumer confidence will be enhanced, and trust will be fostered, if consumers know that transfers of their personal information are governed by clear and transparent rules.*
>
> *There are different approaches to protecting personal information that is being transferred for processing. European Union member states have passed laws prohibiting the transfer of personal information to another jurisdiction unless the European Commission has determined that the other jurisdiction offers "adequate" protection for personal information.*
>
> *In contrast to this state-to-state approach, Canada has, through PIPEDA, chosen an organization-to-organization approach that is not based on the concept of adequacy. PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However, under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement.*"

[21] See also APEC, 'Privacy Framework', 2005, available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf.

[22] http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm

4.2 Accountability developments in the EU

Concepts of accountability are better suited to an environment in which information is more distributed and its location less predictable. If one cannot be sure where information will be needed at a later time and for what purpose(s), it is difficult to ensure that the needed administrative finding of adequacy will be in place. In light of these considerations, the concepts of accountability outlined in the previous section are being considered in the EU as well. To be clear, at present these concepts are not expected to replace the notion of adequacy but rather to serve as concepts which could complement the adequacy requirement.

In the following paragraphs we provide some examples of other instances in which the accountability approach outlined above is reflected:

Rand Study In 2008, the UK Information Commissioner sponsored a study by Rand Europe to review the EU Data Protection Directive in advance of its formal review by the Commission. The study recommended an approach that was based on principles, focusing on use limitations, security, transparency, individual participation (the ability to effectively exercise rights) and accountability[23]. The approach outlined was also meant to be risk-based with a focus on preventing harm. While it is unlikely that the Directive will be changed so radically, other Data Protection Authorities are also considering how to use such notions of accountability.

The Galway Project[24]: The Data Protection Commissioner of Ireland has hosted 2 meetings with privacy experts to "develop a draft document that sets out the essential elements necessary for organizations to establish and demonstrate accountable management of personal information in a compliant and respectful manner, and for enforcement agencies to confidently determine which organizations should be trusted to manage and move personal data in a flexible manner." The OECD and the Business and Industry Advisory Committee (BIAC) to the OECD have been participants, and the results of the drafting process will be submitted by BIAC to the OECD for information and consideration as appropriate.[25]

Barcelona Process – International Privacy Policy Standard/Framework/Principles[26] The Barcelona process has its roots in the 30th International Conference of Privacy and Data Protection Commissioners in Strasbourg (2008), where the Commissioners adopted a resolution on the need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection. As

[23] http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf, p 49.

[24] See Infra: Annex V, 2009 Privacy Update at p. 66

[25] Both the Galway Project and the Barcelona Process were expert groups convened by the Irish and Spanish data Protection Commissioners, respectively. A member of WP6 participated in his expert capacity, but neither project is ready for a public distribution of their work. In both cases, publications are expected by or at the Spanish data protection commissioners' conference in November.

[26] See Infra, Annex V, 2009 Privacy Update at pp. 62-64

the Spanish Data Protection Authority will host the 31st International Conference of Privacy and Data Protection Commissioners in November 2009, they have convened a working group of data protection authorities and privacy experts that first met in Barcelona in January. While no public paper is available at present, concepts related to accountability are clearly referenced in the working drafts.

The Edinburgh DPA Meeting. At the recent European Conference of Privacy and Data protection Commissioners held in Edinburgh, the conference declaration affirmed that[27]:

> *"The conference will continue to promote the need for high standards of data protection in all areas of life, in particular as regards developing technologies, the online world and law enforcement activity.*
>
> *The conference encourages the development and improvement of comprehensive data protection legislation that will:*
>
> - *guarantee and promote fundamental rights and freedoms;*
> - *build on the existing Data Protection Principles;*
> - *focus on effectiveness in achieving desired outcomes in practice;*
> - *encourage organisations to adopt best practice, including privacy by design;*
> - *address the risks of adverse effects faced by individuals and by society at large;*
> - *avoid burdens which cannot be justified; and*
> - *provide for effective enforcement.*
>
> *[…] With this declaration, the conference acknowledges the evolving landscape of data protection and privacy both in Europe and beyond, and the need to continue our work to promote data protection and privacy standards while adapting to the world in which we now find ourselves."*

At the same meeting, Commissioner Thomas from the UK delivered a speech where he focused on promising themes for reform. Among one of the most important themes was the notion of accountability. He set out an argument, captured in the accompanying diagram, that showed how elements of business process, technology, policies and contracts are essential elements of an accountability and governance framework[28]:

---

[27] European Privacy and Data Protection Commissioners' Conference Edinburgh, 23-24 April 2009: Declaration on leadership and the future of data protection in Europe, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_EU/09-04-23_Edinburgh_Declaration_LeadershipDP_EN.pdf

[28] Thomas Richard, Data Protection in the European Union, Promising Themes for Reform, European Privacy and data Protection Commissioners' Conference, Edinburgh, 24 April 2009 http://www.privacycommission.be/nl/static/pdf/seminarie-privacyrichtlijn/data_protection_in_the_eu_nl.pdf

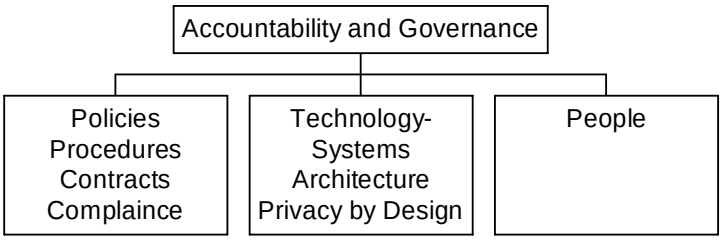


Figure 1: Accountability and Governance Model proposed by Richard Thomas

He also highlighted the need to consider how people interact with the system (usability) and capacity building (skills development/training). These elements are essentially the same elements that are incorporated in the TAS[3] governance model: Policies, Procedures, Contracts and Technology.

4.3 Towards Accountable Technology

When the W3C team was looking at use-based models and concepts of information accountability, they highlighted the increased importance of technology in assuring privacy in the information society. In defining what technical architectures should look like in these new accountability models, the major requirements were related to policy-aware tools, including transactions logs, language frameworks and perhaps most importantly policy-reasoning tools.

The increased level of identified transactions, which occur on-line across all aspects of life, and the rise of identity theft and other similar crimes have also heightened concerns of accountability across information flows. Personal data breaches have become a common part of the lexicon and are now defined in the revised e-Privacy Directive as[29]:

> *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community"*

Issues of Identity and privacy have also received increased attention as concerns over identity theft have continued to grow. In 2005, Kim Cameron first published his 'Seven laws of identity' in his blog[30]. These laws provide a useful foundation for placing identity and privacy in context. Since then, Ann Cavoukian, the Information and Privacy Commissioner for Ontario, has built on the 7 laws in a paper entitled "The Case for Privacy Embedded Laws of Identity

[29] See Art. 2, 2 c) of Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, O.J. 18 December 2009, L-337/29.

[30] http://www.identityblog.com/352/#lawsofiden_law1

in the Digital Age[31]. Commissioner Cavoukian is also known for her work on promoting the concept of privacy by design[32] - the idea that privacy is built into the technology at the design stage, not bolted on after deployment.
A review of the Seven Laws of identity as enhanced for privacy is informative, because like the TAS[3] approach, Commissioner Cavoukian goes beyond the technical elements of privacy by design. A comparison table between the 7 Laws of Identity and the 7 laws of embedded Identity has appeared as follows:

f

The 7 Laws of Identity	**7 Privacy-Embedded Laws of Identity**
LAW #1: USER CONTROL AND CONSENT	**LAW #1:** PERSONAL CONTROL AND CONSENT
Technical identity systems must only reveal information identifying a user with the user's consent.	Technical identity systems must only reveal information identifying a user with the user's consent. Personal control is fundamental to privacy, as is freedom of choice. Consent is pivotal to both. Consent must be invoked in the collection, use and disclosure of one's personal information. Consent must be informed and uncoerced, and may be revoked at a later date.
LAW #2: MINIMAL DISCLOSURE FOR A CONSTRAINED USE	**LAW #2:** MINIMAL DISCLOSURE FOR LIMITED USE: DATA MINIMIZATION
The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution.	The identity metasystem must disclose the least identifying information possible, as this is the most stable, long-term solution. It is also the most privacy protective solution. The concept of placing limitations on the collection, use and disclosure of personal information is at the heart of privacy protection. To achieve these objectives, one must first specify the purpose of the collection and then limit one's use of the information to that purpose. These limitations also restrict disclosure to the primary purpose specified, avoiding disclosure for secondary uses. The concept of data minimization bears directly upon these issues, namely, minimizing the collection of personal information in the first instance, thus avoiding the possibility of subsequent misuse through unauthorized secondary uses.

[31] Cavoukian, Ann, 'The Case For Privacy Embedded Laws of Identity in the Digital Age', available at http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf
[32] http://www.ipc.o n.ca/images/Resources/up-2007_09_17_UofT.pdf; See also infra, Annex V, 2009 Privacy update at p.64

The 7 Laws of Identity	7 Privacy-Embedded Laws of Identity
LAW #3: JUSTIFIABLE PARTIES	**LAW #3:** JUSTIFIABLE PARTIES: "NEED TO KNOW" ACCESS
Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.	Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. This is consistent with placing limitations on the disclosure of personal information, and only allowing access on a "need-to-know" basis. Only those parties authorized to access the data, because they are justifiably required to do so, are granted access.
LAW #4: DIRECTED IDENTITY	**LAW #4:** DIRECTED IDENTITY: PROTECTION AND ACCOUNTABILITY
A universal identity metasystem must support both "omnidirectional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.	A universal identity metasystem must be capable of supporting a range of identifiers with varying degrees of observability and privacy. Unidirectional identifiers are used by the user exclusively for the other party, and support an individual's right to minimize data linkage across different sites. This is consistent with privacy principles that place limitations on the use and disclosure of one's personal information. At the same time, users must also be able make use of omnidirectional identifiers provided by public entities in order to confirm who they are dealing with online and, thereby ensure that that their personal information is being disclosed appropriately. To further promote openness and accountability in business practices, other types of identifiers may be necessary to allow for appropriate oversight through the creation of audit trails.
LAW #5: PLURALISM OF OPERATORS AND TECHNOLOGIES	**LAW #5:** PLURALISM OF OPERATORS AND TECHNOLOGIES: MINIMIZING SURVEILLANCE
A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers.	The interoperability of different identity technologies and their providers must be enabled by a universal identity metasystem. Both the interoperability and segregation of identity technologies may offer users more choices and control over the means of identification across different contexts. In turn, this may minimize unwanted tracking and profiling of personal information obtained through surveillance of visits across various sites.

LAW #6: HUMAN INTEGRATION	**LAW #6:** THE HUMAN FACE: UNDERSTANDING IS KEY
The identity metasystem must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.	Users must figure prominently in any system, integrated through clear human-machine communications, offering strong protection against identity attacks. This will advance user control, but only if users truly understand. Thus, plain language in all communications used to interface with individuals is key to understanding. Trust is predicated on such understanding.
LAW #7: CONSISTENT EXPERIENCE ACROSS CONTEXTS	**LAW #7:** CONSISTENT EXPERIENCE ACROSS CONTEXTS: ENHANCED USER EMPOWERMENT AND CONTROL
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.	The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies. We return full circle to the concept of individual empowerment and informed consent. Clear interfaces, controls and options that enhance an individual's ability to exercise control across multiple contexts in a reliable, consistent manner will serve to enhance the principle of informed consent.

Figure 2: Table Comparing 7 Laws of Identity and 7 Privacy Embedded laws of Identity[33]

This privacy articulation of the seven laws provides a useful roadmap for the application of technology and the consideration of privacy in context. In today's world of continuously expanding information flows and uses, privacy must be considered in a larger context than just the enterprise or the transaction. It must be considered at the ecosystem level and across its lifecycle. This approach has been adopted by TAS[3]. In future iterations of this deliverable, we will use the applicable portions of the 7 embedded laws as part of an evaluation metric to see how successful we are in deploying a privacy by design identity management implementation.

In looking at ecosystem concepts, Commissioner Cavoukian also saw the need to develop new tools to assess privacy, and to that end, in conjunction with the Liberty Alliance, her office has developed a paper entitled: **Building Privacy and Trust-enabled Federation: Federated Privacy Impact Assessment (F-**

[33] Cavoukian, Ann, 'The Case For Privacy Embedded Laws of Identity in the Digital Age', available at http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf, p. 14-15.

PIA)[34]. It is informative to consider the approach to accountability (the basis of PIPEDA, the Canadian privacy law) that is incorporated in this paper:

> "*Finally, the collection of personal information entails a duty of care for its protection. Obligations related to all relevant privacy-related policies and procedures should be documented and communicated as appropriate, and assigned to a specified individual within an organization. When transferring personal information to third parties, organizations should seek equivalent privacy protection through contractual or other means. Further, in order to ensure the accountability of federation members, the principles of openness and transparency should be adopted. That is to say, information about the policies and practices relating to the management of personal information should be made readily available to the individuals whose data is being held.*
>
> *Organizations should also establish compliance and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Compliance with privacy policies and procedures should be monitored, evaluated and verified on an ongoing basis.*
>
> *The combination of these factors leads to the concept of accountability, in which information is appropriately secured and protected across both the scope of federated enterprises and the life cycle of the information. This concept not only forms the basis of Canadian privacy laws, but also is found in the OECD Guidelines, and is the defining principle of the APEC Privacy Framework.*"

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

5 Legal requirements for TAS³

The requirements outlined in the summary of privacy principles, as well as in the 7 Embedded Laws are not defined in a manner that provides sufficient technical guidance, particularly because they lack details of operational relevance. As we delve into the operational requirements, it becomes clear that the principles summarized above are both interdependent and overlapping. Since our goal is to provide guidance and not a legal treatise, the following sections will address these issues within the context of how relationships and interactions occur. For the technical and business community this presents more of a workflow concept; for the data subject this represent more of the intuitive path through which a relationship with an organization or a number of organizations may develop.

Part of the challenge which TAS³ is addressing, is the need to address privacy and security within an ecosystem, not just within a particular enterprise. Requirements will thus contemplate both the workflow between individual entities as well as needs of the ecosystem. Since one of the main objectives of TAS³ is the assurance of privacy and security, we will also look at the role of policies and other legal instruments in assuring that security and privacy are enabled in an environment of trust supported by a governance framework.

The following table (Figure 3) highlights the basic data protection requirements mandated in the Directive. In order to help define their operational relevance, these requirements have been divided into 4 categories: collection, processing, operation and accountability.

Requirements at time of collection
• Information must only be collected for specified, explicit and legitimate purposes (this also can encompass related compatible purposes). • Collected information must be limited to information relevant to the specified purpose. • Data subjects must be provided notice which includes: o Identity of controller o Purpose(s) of processing o Information on recipients of data o Nature/consequences of information collection o Available access/correction rights and methods o Any other information required to assure fairness of processing. o Where Information is not collected directly by controller or will be shared, notice must be given at time of collection or prior to sharing including: o Identity of controller o Purpose(s) of processing o Information on recipients of data o Nature/consequences of information collection o Available access/correction rights and methods o Any other information required to assure fairness of processing.

Processing Requirements

- A legitimate basis for the processing must be ensured
- Unambiguous consent is required, unless
  - Processing is necessary to accomplish the purpose of collection
  - Processing is needed to protect vial interest of the data subject or in the public interest
  - Processing is required by legitimate business needs of controller or third party relating to the service they are providing if they are not inconsistent with fundamental rights of privacy (general obligations…)
- No processing of personal information revealing/concerning
  - Racial/ethnic origin
  - Political opinions
  - Religious/philosophical belief
  - Health
  - Sex life
  - Without/Unless:
    - Explicit consent (unless still prohibited by law)
    - Necessary for a legally authorized purpose of a controller in the field of employment law
    - To protect the vital interest of the data subject to other person not able to provide consent
    - In the normal course of business of a non-profit with political, philosophical, religious or trade union aim where processing is of member of group
    - Made public by the data subject
- Limitation does not apply where:
  - Processing is needed for purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
  - Processing of national identifier information as prescribed by Member State

Operational Issues: Accuracy, retention, security

- Accuracy of information collected must be maintained; kept up-to-date where needed and all reasonable steps taken to ensure correctness and completeness of the data.
- Data may only be maintained as identifiable data only as long as needed to accomplish the purpose of collection.
- Data must be secured by physical, logical and administrative controls that are at the level of the current state-of-the-art and appropriate to the risks represented by the processing and nature of the data. Appropriate technical and organizational measures must be defined to protect personal data against:
  - Accidental/unlawful destruction
  - Unauthorized access or disclosure

Accountability: Access, oversight and compliance
Data subjects have the right to access their information at reasonable intervals and without excessive delay or expense and have the right to: • Receive confirmation as to whether there is data being processed; including category/type, purpose, and who their has been shared with (if applicable) • Have such information provided in an intelligible fashion • Information about automated processing that could result in decisions impacting the data subject • Where appropriate, request rectification, erasure or blocking of data not consistent with Directive obligations as well as notification of same to third parties where reasonable. Implicit in the requirements of the Directive are the need to have processes to enable individuals to exercise these rights. Issues such as complaint handling, audit, oversight and redress mechanisms are necessary elements to enable proper execution of the user rights. Some of these would also have operational utility in terms of security or be required as part of collection or processing of information. We call them out under accountability because of their importance to proper oversight and compliance.

Figure 3: Summary Table of TAS³ Data Protection Requirements

Note: As TAS³ develops greater detail will need to be provided with regards to the specifics and nuances of both the laws at the national level as well as the implementations of any supporting regulations, and the relevant decisions of the data protection authorities. There will also be need for specific guidance related to sectoral applications of both the relevant data protection laws as well as specific sectoral laws related to security and/or data protection. For now, the development of a high level compendium of requirements is essential to allow developers to better grasp the nature of requirements which must be met.

5.1 Applying Privacy Concepts in practice

A workflow approach to privacy and security requirements first starts at the moment an individual enters a system/ecosystem. As we proceed with the workflow analysis it will become increasingly clear why we have to think of both system and ecosystem needs.

5.1.1 Notice/use

The first introduction of a person to a system may be in person, on the phone, via documents or online. In all cases, the individual has a right to know certain things:

- Who is controlling the collection of information;
- What personal information is being collected (both in the event of directl and indirect collection);[35]
- For what purpose is the information is being collected
- How the information will be used
- Who the information will be shared with[36]
- That the information will be appropriately secured.
- How to request access to the information for correction/review.
- That the information will only be retained (in identifiable form) for a period of time relevant to the purposes of collection.

A number of these questions are essential to allowing an individual to determine whether they wish to consent to the collection and use of the information. In considering these questions, it is essential to understand all the possible purposes of collection and uses of information by both the collecting entity and any downstream/ecosystem entity with which the information may need to be shared. The consent of the data subject to the collection and use of information is limited to those purposes specified. Thus, if an enterprise only specifies the limited uses of information that it currently engages in, but then desires to share the information with other parties, or use the information for other purposes, a new notice and consent would be required[37].

[35] The notice obligation does not only cover situations in which the data subject knowingly provides certain information, but also extends to instances in which information is collected in less obvious ways, e.g. on-line or on the phone. In employment and health cases issues of video surveillance, audio-taping, and email surveillance also come into play. Depending on the jurisdictions there may be specific notice requirements. Issue of third party information sources used to supplement information obtained directly are also covered.

[36] At least in terms of types/categories

[37] There are some uses/sharing that are permitted within the original collection – those purposes not incompatible with the purposes of the collections/processing or needed to accomplish the transaction. Good practice would favour listing those uses explicitly in the initial notice provided to the data subject.

5.1.2 Technical/business considerations[38]

- Need to develop a notice strategy across all channels of communication
  - Explore short-form notice options[39] to address form factor issues
  - Explore timing of online notice presentation[40]
- Understand/identify what personal data elements are going to be needed
- Identify the persons/organizations that may get access to the information
- Consider how the various data elements will be used by the system and the ecosystem

5.2 Collection limitation/Data minimization/Least means access

Collection limitation concepts come into play at the very outset of any transaction. At the same time an organization considers what information it needs for its business purposes, it must consider the extent of information that is permissible. Once the appropriate notice has been provided specifying the purposes, uses and sharing of information, and the data subject has provided the personal information, data minimization and least means access come into play. The concepts are related and are predicated on the concept that what isn't collected or shared is much less likely to be compromised.

Collection limitation, which is closely related to the requirement of data minimization, refers to the need to assure that only the minimum amount information needed to accomplish the purposes of the processing is collected. This is a question that requires guidance from those using the information, not just those developing systems, as they may not be aware of the possible uses and all aspects of data required.

Data Minimization is the broader concept of assuring that only the information needed to accomplish the specific business need is accessed, and also that data is not kept in a form which permits identification for longer than is necessary to achieve the purposes of the processing. Data Minimization may best be explained by an example. A shipping department may need to access customer information to deliver a product, but may not require access to credit or other financial information. As soon as the collected information is no longer necessary to achieve the purposes of the processing, the shipping department should remove that information from its databases.

'Least Means Access' complements the previous principles by requiring controls to the access of information. From a security perspective this may be interpreted as only providing access to information on a need-to-know basis. Only those with

[38] This is where the overlapping and interdependent nature of the requirements comes into play; some elements that must be addressed are more suitably discussed under other topics.
[39] Article 29 Working Party, 'Opinion 10/2004 on More Harmonised Information Provisions', WP100, 25 November 2004, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.
[40] Laws require notice at or before time of information collection, which sometimes becomes more problematic, e.g. with regards to the processing of IP addresses (cf. supra).

a need to know may be provided with access to personal information. Similarly, individual entities should only be accorded further processing privileges (delete, edit, …) to the extent that it is necessary to fulfil their role towards the processing

Taken together, the three concepts require organizations to limit information collection to those personal data elements needed to accomplish the specified purposes, to then limit use of those personal data elements according to their legitimate business which were specified as purposes and to also limit access to those data elements to employees on a need-to-know basis. Additionally, data management life cycles must also be in place to ensure that data is not kept in identified form for longer than is necessary.

We recognize that the need-to-know and need-to-share requirements set forth in the Directive help create a framework for enabling responsible information flows. One reason why the TAS³ work is so important is the increased need to share information. Concepts of information portfolios managed throughout a lifetime by their very nature imply the purpose of sharing information, whether it is through subsequent transfers or delegated access. The need to both maintain control related to sharing in terms of subsequent use as well as the need to understand the implications of sharing (which goes more to effective notice), only increase in importance over time. The requirements set forth in the Directive contemplate sharing, but were drafted at a time when sharing would be much more limited due to the fact that most sharing would take place between people in reasonably close geographic proximity as opposed to mediated by technology across large distances among parties with relatively little familiarity or pre-established relationships.

New technologies such as reputation engines and technologies that enable individuals to define personal privacy policies and make them apply across transactions (PDP, PEP, sticky policies), will help assure consistency of application of personal privacy requirements across these more disparate information exchanges. These are also the types of technologies contemplated by the new accountability requirements.

As we look at emerging technologies we must also be mindful of the user benefits that can result from this increased sharing. In the employment field, electronic exchange of information creates better listings of and access to opportunities for career development, education and job placement. There are also improved technologies in job application and recruitment processes; ranging from video resumes to pseudonymized job-to-skills matching engines. In the area of health care the portability and control of health records has the potential of improving visibility of care and expanding the patient's choice of providers. Appropriate use of such records also allows health care system operators to cross-check treatments and prescriptions to reduce the likelihood of errors and optimize care. To the extent that the information can be sufficiently anonymized or generalized it may also be made available to provide better information to address public health planning.

TAS³ aims to enable these benefits in a secure and trusted infrastructure. The focus on security and trust may also enable greater information sharing if data

subjects are more confident that the system collecting information will do so in compliance with law and pursuant to the policies they define.

5.2.1 Technical/organizational considerations

- Are the personal data elements being collected really needed?[41]
- Has a business need for access to or sharing of information been defined?
- Are policies articulated that limit employee access to information based on business need?
- Are employees bound to those policies?
- Are there technical procedures/controls to support those policies?

5.3 Accuracy, access and correction

Accuracy and Access/Correction are separate, but related issues which we discuss together because they present some of the same questions. Properly accommodating Accuracy and Correction requirements may be one of the easiest and most problematic tasks at the same time. Today's online environments facilitate compliance with these requirements because information may be kept up-to-date or corrected by the data subject via self-service applications. Data processing within an ecosystem, however, creates additional issues. For one, data that has been minimized and shared with third parties may only have some identifying characteristics and in many, if not most cases, the downstream recipients of information elements may have no direct relation or even knowledge of the data subject. In order for them to meet an access request or update information they essentially have only two options: One - rely on the data provider to update and correct the information thus creating a centralized resource through the entity that has the direct relationship with the data subject; or Two - collect and maintain information about the data subject sufficient to validate their right to access the profile or stored information[42]. The latter path is clearly not desirable, but may inadvertently result if no other path is provided to create a meaningful path to accuracy, access and correction.

5.3.1 Technical/organizational considerations

- Identify what information is provided by the data subject and can be kept up-to-date through self-service applications
- Once data elements, uses and flows are established, develop an accuracy, access and correction models for the ecosystem. These considerations will raise issues related to how information is stored, separation of duties and other technical topics dealt in greater depth under security.

[41] Recall that this inquiry starts with the initial online collection – the technical handshake, cookies etc. While these elements may or may not be personal at the time of collection they could later be associated with a persons identity and as such need to be considered at the outset.
[42] As TAS[3] develops, the greater level of user control afforded by the systems may limit the scope of this issue.

- Develop practices and policies to oversee appropriate access and correction[43] and legal instruments that bind the participants, as needed.

5.4 Security

Privacy and security are essential elements of user trust. Security is also an, if not *the,* essential privacy requirement from a technical design perspective. Security obligations exist at the technical, logical and physical level and all require that appropriate policies be put in place. Annex 2 lays out a very useful compendium of possible policies sourced from guidance related to HIPAA, the healthcare law in the US. Apart from the useful compendium of security policies, the approach to implementing them is also informative. The policies are broken out into "required" and "addressable'. Addressable policies are those with greater flexibility of specification and grouping to all for more adaptability to existing implementations.

The increased public attention with regards to issues of identity theft has driven calls for improved security. As a result of some very notable public and private sector breaches, for example, the Information Commissioner for the UK has been pushing for required encryption and has promulgated detailed security guidance on his site.[44] In the US, the same concern has spawned breach notification bills 46 of the 50 states[45]; Canada and Australia are also considering breach notification bills[46]; and the EU has recently introduced amendments to the e-Privacy Directive[47] that provide for notification of security breach (cf. supra).

Security is a concept that organizationally permeates the entire information lifecycle. Because it represents the driving force behind TAS[3], it is dealt with across all aspects of the project. In this section, we will look to the concepts that stand behind security in privacy legislation as well as current hot topics. Most privacy legislation and international instruments, including the five that are the basis of this review, do not provide detailed or proscriptive requirements as legal requirements. They do however share broad themes:

1. They relate to technical and organizational measures – technology, policies, practices and processes.
2. They presume that state-of-the-art is being considered, but accept balancing factors that might influence decisions such as nature/sensitivity

[43] There may also be requests to supplement information, blocking and deletion, but those must be appropriate to purposes and circumstances. On this point the Directive has instituted a balancing test. For instance, the data subject does not have a unilateral right to block the processing of an accurate credit report (provided that it is being used in the accepted course of transactions), merely because the report is negative.

[44] Good practice note on security: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/security%20v%201.0_plain_english_website_version1.pdf; see also http://www.ico.gov.uk/Home/about_us/news_and_views/current_topics/Our%20approach%20to%20encryption.aspx for guidance on approach to encryption.

[45] http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

[46] See generally, Maurushat, Alana, Data Breach Notification Law Across the World from California to Australia, Berkeley Electronic press, 2009, http://law.bepress.com/unswwps/flrps09/art11.

[47] Directive 2002/58/EC

of the information, size of the enterprise, potential risk as well as risk mitigation.
3. They are looking at both external and internal threats (unauthorized access from within or outside the data controller's organization)
4. Access to information is the tripwire and wrongful access can include access by an authorized person with no legitimate need[48]
5. Information should not be maintained in an identifiable fashion beyond the time necessary to accomplish the specified purposes[49]
6. While not a specific requirement – former ISO/IEC 17799 (now ISO/IEC 27001/2) is often referenced as an example of a set of comprehensive security practices.

5.4.1 Technical/Organizational considerations

Major topics that MUST be addressed include:

a. Intrusion detection
b. Virus Protection
c. Firewalls
d. Encryption at rest and in motion
e. Authentication/ID Management systems
f. Authorization
g. Access control
h. Audit/logging
i. Data retention/deletion
j. Separation of duties
k. Security policies

See Annex 3 and Annex 4 for a more comprehensive list of topics and related requirements. Annex 3 maps TAS[3] requirements and practices to legal obligations defined in the Directive, while Annex 4 provides a more detailed information to help guide other WPs of TAS[3] on legal requirements. These two documents are common to both D6.1 and D6.2.

5.5 Governance

A number of issues that are closely related to security may more properly be dealt with under the concept of governance. Beyond the complexities of making all of the elements listed above work together, an organization must also have a

[48] This may be an especially prevalent concern in medical systems where people may try to glean information on a celebrity or VIP for non-medical reasons
[49] There is no hard and fast rule as to what the proper period of retention is related to a specific purpose. Interpretations rely on concepts of appropriateness and proportionality. One must also be aware, however, that certain information like communication headers and medical records often have minimum retention periods.

governance model. TAS³ addresses that requirement at the ecosystem level by contractually binding organisations as a prerequisite for participation. Issues of trust do not start and end with just one particular organization. Consequently, mechanisms and procedures must be in place that allow distribution of trust in such a way that the system as a whole – the ecosystem – is trusted, not just the entity in question. Such an approach will allow systems to grow in an efficient and organic fashion, based on dynamic needs and innovation, while at the same time reducing undue burdens. Trusted ecosystems have the ability to migrate trust across entities because individuals feel that they can rely on the governance framework, which justifies their trust.

A governance framework must address: The legitimate operational needs of the organizations; the legal rights of the end-users; and the risks of the environment in which they operate. The framework can be developed in primarily two ways. It may be either organization- or user-centric. In the case of the former, the needs of organizations are tempered by the needs of the users; in the case of the latter the desires of the users help shape and inform the needs of the organizations. Ideally, systems will be developed over time in which a win-win scenario can be created; whereby the desires of the users and needs of the organization are optimized. TAS³ is an attempt at such an optimization, in which appropriate user control becomes a functionality valued by the organizations, as it reduces their burden in achieving compliance.

A governance framework thus requires a risk analysis, a needs analysis for both users and organizations, a mapping of data flows and an identification of requirements. The operational elements of the governance framework include the policies and practices of the organizations, the legal instruments that bind the employees/agents to the organizations, the organizations to each other and the users to the system. These policy and legal aspects of the system work in conjunction with the technical elements of the system.

By way of example, one could consider the legal framework used by credit card companies. There are agreements and policies that control relations between banks, processors, merchants and cardholders. There are likewise policies and agreements that bind what employees can do with card-member/institutional information. All parties are bound to an ecosystem that does not require any prior contact or relationship between transacting parties. This is why a tourist from the US is able to purchase a watch in the EU from a merchant he has never met by using a credit card. The governance framework, that also controls onward transfers and other uses of the information, is one of the key factors in enabling the user to trust the system with sensitive personal information. This provides a good example of broad sharing of appropriate information with required controls to assure trust and security. Need-to-share and need-to-know can be appropriately optimized and effectively overseen under this approach.

In the EU healthcare arena there is a similar desire to enable records access needed to treat an increasingly mobile population. Consequently, governance frameworks for e-health records are starting to emerge. The healthcare system is of course much more complex than that of credit cards; due to the sensitivity of health-related information and the nature and organization of entities providing services. While credit card information may provide information on some of your

habits and person traits, it's greatest benefit (for legitimate exploitation) would consist in using the aggregate information as input to a profile for marketing or customization purposes. Thus broad categories, risk-based metrics and implications of failure of compliance are more easily identified and quantified. Different procedures are in place to guard against criminal use of information, including ID theft.

Health information, on the other hand, is personally identifiable at the level of each item and may have significant implications to create harm or embarrassment for misuse at the item level. Unlawful uses may include wrongful access to pharmaceuticals or health services through fraudulent credentials. Solutions to these problems are being addressed at the organizational level, but need to be addressed at the ecosystem level as well. The way in which service providers in the health care sector are organized is another fundamental area of difference. While governments play a central role in payment of services, there is a much broader set of players with a less straightforward method of coordinating operations. Unlike the credit card industry, which has coordinated the PCI Security standard there is no similar unifying standard for healthcare across the various actors. There is likewise no similar unifying contract infrastructure across all of the aspects of treatment, payment or operations, not to mention the necessities of medical research and public health administration. One must also consider the implications of system failure in health care information systems, which go beyond economic consequences to include matters of health, including those of life and death. Thus the integrity and availability of health information can be critical beyond measure.

TAS³ is an ecosystem-based solution that coordinates many of these disparate elements. In most cases these concepts are backed into over time. In the case of TAS³, these elements are a prime consideration during the design process. This level of coordination takes the concept of privacy by design to a higher level. TAS³ is undertaking the integration of the technology, policy and legal elements at the design stage through collaborative processes. Since this will remain an interactive and collaborative process beyond the design stage, it will require continuous refinement and optimization. A significant benefit from designing security and privacy obligations into technology, policy, and legal requirements at the outset is that it enables an optimization of resources to assure that all three project aspects are complementary and mutually supportive. In some cases, technology enables an organization to demonstrate compliance with policies; in other cases, policies underpin concepts difficult to code and lastly, contracts may be required to bind organizations and users to both policy and technical requirements.

After appropriate needs and risk analyses, policies are the next logical step, which helps define the obligations and rules of behaviour that will be supported by the technology and contractual framework. A broad variety of policies may be required or considered that relate to security, privacy, compliance and operations. While not relevant to specific EU obligations, Annex 2 provides an example of policies that were either considered required or addressable under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the US. While the policies are not surprising and approximate requirements of ISO/IEC

27002, they do specify agreements/contracts as required elements of the security matrix.

Among the most notable policies that need to be considered from a privacy/trust perspective:

1. Privacy policy
    a. Data subject
    b. Employees /third parties
    c. Personal information of other customers transferred for processing
2. Employment/HR Policies
    a. Policies related to employee screening
    b. Workplace monitoring (includes systems)[50]
3. Security Policies
    a. Security policy
    b. Internet Access and Use
    c. Incident Response Policies
    d. Encryption
4. Business continuity/disaster recovery

As these and other required policies are being considered, recall that they must be considered at both the enterprise and ecosystem level so that assurances of trust can be provided with regards to the system as a whole.

5.5.1 Technical/Ecosystem Considerations

- Is it possible to identify minimum technical requirements/capabilities required for participation?
    - Are they ecosystem-wide or do they vary by type of participant, nature of information flow etc.?
- Are there minimum security requirements for all participants[51]?
    - Are they ecosystem-wide or do they vary by type of participant, nature of information flow etc.
- What privacy promises were made or legal obligations are owed to data subjects that need to be respected across the Ecosystem?

Once these factors are identified the contractual framework can support them.

5.6 Compliance and oversight

While we have discussed many of the inputs to developing a governance framework, we have not yet focused on the important operational factors of compliance and oversight. Again, under normal circumstances, these issues are more complex at the ecosystem level, but the fact that these considerations are being taken into account at the legal, policy and technical level of project

[50] Guidance from the UK Information Commissioner http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html

development, lessens the compliance overhead related to these obligations. In the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, the principle of "each according to their role" was highlighted and reminds us that all participants to a system, even users, have some security obligation that should be proportional to their role.[52]

From a privacy perspective, two main points need to be stressed. All privacy laws require that there be an effective mechanism for complaint. Thus an essential element of a proper governance framework is an easily accessible and user-friendly complaint process. Good practice often favours the inclusion of a dispute resolution or mediation processes. Another critical component is a compliance/oversight process. It is hoped that appropriate compliance and oversight processes can help resolve issues before they result in formal complaints.

Compliance and oversight in TAS[3] will be assisted to a larger degree than usual by the technical infrastructure. Concepts of "sticky policies" and other automated means inherent to the architecture such as the so-called "dashboard" shall be used assure more correct use of, and access to, information. This is an important example of how technology, policy and legal issues considered at the outset can enable greater compliance with lower overhead. Compliance and oversight are multifaceted concepts that must exist in dimensions beyond technology – no matter how good the technology is.

5.6.1 Organizational/Ecosystem Considerations

- Are there specific persons appointed to the various tasks and are there appropriate separations of duties, reporting lines etc?
- Is all the information needed to prove or investigate compliance being logged securely?
    - What are the investigatory policies?
    - What are the retention periods?
    - Can any of the information be retained in an anonymized or otherwise de-identified fashion?
- Have audit procedures been defined that provide backing for compliance?
- Can you audit across transactions and interactions involving multiple parties?
- Where issues do occur[53], is there a complaint mechanism in place that is easily accessible?
- Are there processes to handle, escalate and archive complaints?
- Are there mechanisms that facilitate reporting/registration requirements with data protection authorities?[54]

---

[52] http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html. This approach is further elaborated in D6.2 in sections 5.4-5.5.

[53] The complaint system should be able accessible from across the workflow as issues are not solely generated at the close of a transaction.

[54] These reporting and registration requirements start with the need to register system that collect and process personal information (the detail of these requirements vary by country) and go to consideration of breach notification.

6 Sectoral Issues

6.1 Health Care

Innovative treatments in healthcare are often dependent on new forms of capturing and exchanging medical information. For example team-based treatment of disease, remote consultation, electronic monitoring of patient status and delivery of home care all imply the need for additional information sharing. This increased sharing often causes concerns in relation to privacy, identity theft, insurance fraud and denial of insurance.[55] A recent OECD study on health policy[56] highlighted similar issues:

> *How health care organisations handle their digital information environment affects the uptake of health its. Sharing sensitive patient data in a large and heterogeneous environment through the use of web-based applications raises a series of privacy and security issues. For treatment purposes, an individual's health information will need to be accessed by a variety of health providers: physicians, nurses, radiologists, medical students, or others who are involved in the patient's care. In this process, the main challenge is to create a smooth interface between privacy and confidentiality policy and security requirements for defining access to and use of personal health care information. These requirements must be very obvious to users, and must be high on the list of information that patients are provided with*[57].

TAS[3] seeks to address a number of these issues, specifically by enhancing the trustworthiness of ICT solutions for health care as well as by creating the smooth interface between privacy, confidentially, security and access control. The dashboard functions within TAS[3] also to help make not just the requirements, but the actual controls both more obvious and accessible to users.

Electronic exchange of patient information in the healthcare context is governed not only by data protection law, but also by a number sector-specific regulations. These regulations have not yet been harmonized at European level. It is not

[55] See e.g. J. Anderson, 'Social, ethical and legal barriers to E-health', Journal of Medical Informatics 2007, vol. 76, 480-483, available at http://computer.shahinshahrpnu.ir/manage%5Cimages/uploads/files/5198041sdarticle39.pdf.

[56] OECD Health Policy Studies, 'Improving Health Sector Efficiency. The role of information and communication technologies, OECD, 2010, available at http://www.oecd.org/document/61/0,3746,en_2649_33929_45501565_1_1_1_1,00.html.. Canada was one of the countries participating in the OECD study and the reports drafted Canada Health Infoway confirmed patient concerns related to healthcare information, privacy and security which further demonstrate the need for solutions as the one envisaged by TAS[3].

[57] Id at 66

within the scope of this project to undertake a comparative analysis of the legislation of each Member State which regulates the exchange of medical data. However, we have analyzed the relevant sector-specific legislation of the Netherlands, seeing as the eHealth pilot of TAS³ is scheduled to take place there. This analysis has been incorporated as an annex in this document (annex 5) , which will serve to inform the further development of both TAS³ requirements as well as the TAS³ contractual framework. The Netherlands is also an informative example because of high adoption of EHR, the well-functioning public-private partnership and the well defined health privacy regulatory framework.

7 Conclusion

The legal requirements of data protection in the EU exist across a number of Foundation documents, which have been implemented into national legislation. These documents provide a common set of principles providing individuals with rights related to the processing of their personal data. Applying those high level principles to applications of current and evolving technology is proving to be more challenging every day. Matters become complicated further due to the increased complexity of systems and mobility of people.

In order to be of assistance to stakeholders ranging from end-users to policymakers, this deliverable has provided multiple levels of guidance. First, the summary principles from the Foundation documents on privacy, human rights and data protection were listed. These are the antecedents of the Directive. Secondly, a review was made of ongoing discussions regarding notions accountability and accountable systems, seeing as they illustrate important trends which may supplement the traditional notice and choice approach to privacy contained in the Directive. Third, more specific challenges posed in applying existing definitions in the Directive to today's technology and business models were discussed. Finally, we reviewed the requirements of the Directive and related them to the operational context in which they are intended to be enforced, and supplemented them with relevant questions, which act as further guidance towards interpretation and implementation of these requirements. The deliverable is further supported by six annexes: a comparative table of the foundation privacy documents, a listing of the security obligations set forth in HIPAA; a summary table of privacy requirements and related TAS^3 requirements and practices and a more detailed set of TAS^3 requirements that are provided as guidance to other WPs (and have been included in D1.4); an overview of the regulatory framework for eHealth in the Netherlands; and two updates describing relevant developments in the field of privacy that took place in 2009 and 2010 respectively.

Throughout this deliverable, we have described how TAS^3 will provide the elements to support the current notice and consent model as well as the evolving accountability model. We have further highlighted the importance of the approach, which underlies TAS^3: the collaborative development of technical, policy, business and legal requirements to provide a more seamless and trusted end-to-end architecture that enables greater compliance with privacy. The greater compliance with privacy is accomplished in mainly two ways: by taking a collaborative ecosystem approach and by providing technical means to help honor user generated policies across the ecosystem. The result is a user-centric architecture that enhances privacy and security through its integrated technical, policy, business and legal requirements. Privacy and security are the essential elements of trust that are needed to support the enhanced information sharing that lies at the basis of so many developing citizen and consumer services, as well as key to supporting future competitiveness and economic growth.

8 Annexes

8.1 Annex 1 – Foundation documents on privacy

OECD	**COE**	**EU**	**UK**	**Netherlands**
Collection limitation principle lawful and fair means with consent where appropriate*	Fair and lawful collection and processing*	Fair and lawful processing*	Fair and Lawful Processing*	Lawful processing in a proper and careful manner*
Purpose specification at time of collection	Stored for specified and legitimate purposes	Collected for specified, explicit and legitimate purposes	Collection only for one or more specified purposes	Collection for specific, explicitly defined legitimate purposes
Relevant to purpose of collection	Relevant and non-excessive	Adequate, relevant and non-excessive in relation to purpose	Adequate, relevant, non-excessive collection in relation to purpose	Adequate, relevant and non-excessive collection to purpose
Accurate and up-to-date as needed	Accurate and where needed, up-to-date	Accurate and where needed, up-to-date	Information kept accurate, up to date	Correct and accurate for the purposes collected/processed
Inherent in relevance…	Preserved in a manner that does not allow identification beyond time needed to accomplish purpose	Kept in a form that identifies data subject no longer than necessary	Personal data not kept longer than needed to accomplish purposes	Processing not kept in form which allows subject to be identified longer than needed
Use/subsequent use not incompatible with collection purpose	Not used in a manner incompatible with purpose of collection	Not used in a manner incompatible with rights of the	Processing in accordance with rights of the data subject	No processing incompatible with purpose of collection

		data subject		
Reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data	Appropriate security measures against unauthorized/accidental destruction, loss, access, alteration, or dissemination	Appropriate technical and organizational measures against unlawful destruction or unauthorized disclosure or access and any other unlawful processing.	Appropriate technical and organizational measures against unauthorized/unlawful processing, or loss, destruction or damage to personal data	Appropriate technical and organizational measures to secure data (take account of state of the art)
Used only for purposes collected, except with consent or authority of law and be accountable for complying with measures that give effect to guidelines	No outright prohibition on transfer, but specific regulations are permitted except where regulations of destination jurisdiction provide equivalent protection	No transfer outside of Member States unless third/destination country provides adequate protection of rights and freedoms in relation to processing personal data	No transfer outside of EEA unless recipient country provides adequate protection of rights and freedoms in relation to processing personal data	Adequate guarantees from third party processors, governed by agreement or legal act, complies with obligations at destination, proof or agreement or act related to data protection and security
Knowledge of collection; consent, where appropriate,		*Unambiguous consent, necessary for contract to which subject not party, controller legal obligation, vital interests of data subject, public interest, necessary	* Consent, necessary for performance, required for non-contract legal obligation, needed to protect vital interests of data subject; for public functions, in order to pursue	*Unambiguous consent, Necessary for the performance of a contract to which subject is party or at request of subject, legal obligation of responsible party, vital interest of data subject, proper performance of public law, legitimate interests of responsible party

		for legitimate interests of controller or third party	legitimate interests of data controllers/third parties.	
Access and correction without undue expense or delay in intelligible form	Access and correction without undue expense or delay	Is data being processed, categories of types of data and processors, Access and correction without undue expense or delay	Comply with written requests for access/correction without undue expense, limited by confidentiality obligations to others	Is data being processed, categories of types of data and processors, Access and correction, supplement, deletion or blocking without undue delay, includes
Duty of confidentiality	Duty of confidentiality	Duty of confidentiality	Duty of confidentiality	Duty of confidentiality
Special requirements for sensitive data	Special requirements for sensitive data	Special requirements for sensitive data	Special requirements for sensitive data	Special requirements for sensitive data

8.2 Annex 2 – Compendium of US HIPAA security requirements

Security Standards: Matrix
Standards Sections Implementation Specifications (R) =Required, (A) =Addressable

Administrative Safeguards
Security Management Process ..... 164.308(a)(1) Risk Analysis (R)
Risk Management (R)
Sanction Policy (R)
Information System Activity Review (R)
Assigned Security Responsibility ..... 164.308(a)(2) (R)
Workforce Security ..... 164.308(a)(3) Authorization and/or Supervision (A)

Workforce Clearance Procedure
Termination Procedures (A)
Information Access Management ..... 164.308(a)(4) Isolating Health care Clearinghouse Function (R)

Access Authorization (A)
Access Establishment and Modification (A)
Security Awareness and Training ..... 164.308(a)(5) Security Reminders (A)
Protection from Malicious Software (A)
Log-in Monitoring (A)
Password Management (A)
Security Incident Procedures ..... 164.308(a)(6) Response and Reporting (R)
Contingency Plan ..... 164.308(a)(7) Data Backup Plan (R)
Disaster Recovery Plan (R)
Emergency Mode Operation Plan (R)
Testing and Revision Procedure (A)
Applications and Data Criticality Analysis (A)
Evaluation ..... 164.308(a)(8) (R)
Business Associate Contracts and Other Arrangement.
164.308(b)(1) Written Contract or Other Arrangement (R)

Physical Safeguards
Facility Access Controls ..... 164.310(a)(1) Contingency Operations (A)
Facility Security Plan (A)
Access Control and Validation Procedures (A)
Maintenance Records (A)
Workstation Use ..... 164.310(b) (R)
Workstation Security ..... 164.310(c) (R)
Device and Media Controls ..... 164.310(d)(1) Disposal (R)
Media Re-use (R)

Accountability (A)
Data Backup and Storage (A)

Technical Safeguards (see § 164.312)
Access Control ..... 164.312(a)(1) Unique User Identification (R)
Emergency Access Procedure (R)
Automatic Logoff (A)
Encryption and Decryption (A)
Audit Controls ..... 164.312(b) (R)
Integrity ..... 164.312(c)(1) Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication ..... 164.312(d) (R)
Transmission Security ..... 164.312(e)(1) Integrity Controls (A)
Encryption (A)

Source:
http://www.cms.hhs.gov/securitystandard/downloads/securityfinalrule.pdf

8.3 Annex 3 – Data protection requirements and implementation overview

The following table maps specific data protection requirements into both TAS³ techical/organizational measures to achieve compliance as well as with TAS³ best practices. This represents the further development of the legal requirements categorized in D6.1. Both the measures listed for compliance as well as the TAS³ best practices are essential to the successful implementation of the data protection requirements set forth in the previous section. The table also cross-references other relevant TAS³ deliverables to which the reader may turn for additional clarification. This table (Figure 5) provides a useful summary overview of the interrelation among the techical, business, legal and policy, components of TAS³.

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

Data Minimization	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. TAS³ participants shall be required to adopt privacy policies which inter alia: -specify the purposes of processing; -provide assurance that only the information which is absolutely needed for a specific purpose is collected; -explicates data life cycle management (incl. intended storage duration); -describes how access and processing capabilities are restricted within the organization so that its members are only able process personal data in accordance to what is strictly needed for the performance of their tasks / their role within organisation 2. Authoritative sources (i.e. sources trusted to provide accurate & up-to-date information) shall be designated and vetted (thereby reducing the need for unnecessary duplication) (cf. infra; data accuracy) 3. Access and processing limitations that support a sufficient level of granularity (access/data release on a 'need-to-share' basis) shall be implemented 4. Mechanisms shall be in place to respond to data requests with only that information that the requesting entity is authorized to receive 5. Policies shall be in place to restrict propagation of more attributes than needed 6. Personal data shall be removed or anonymized once the purpose for which it was collected / further processed has been completed (taking into account need for accountability at later time) 7. All technical and organisational measures relating to data minimization procedures shall be documented and audited on a regular basis	1. User-controlled attribute aggregation through 'linking' service (see deliverables D2.1, D4.2 D7.1) 2. Purpose and storage duration specification (inter alia in 'sticky policies', including obligations relating to removal); (see deliverables D2.1, D4.2 and D7.1) 3. Selective attribute disclosure during authentication: additional measures to avoid unnecessary linkability, pseudonym management) (see deliverables D2.1, D4.2 and D7.1) 4. Additional measures to avoid unauthorized or unnecessary monitoring (inter alia providing user choice where possible as to whether or not persistent ID or transaction ID is used) (see deliverables D2.1, D4.2 and D7.1)

Data Accuracy	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Authoritative sources (i.e. sources trusted to provide accurate & up-to-date information) shall be designated 2. Vetting of sources of attribute information - Procedures shall be established to ensure verification of each attribute with a level of assurance proportionate to the interests at stake 3. Data life cycle management procedures shall be in place, incl. review and update procedures for personal data which is being kept for a prolonged period of time 4. Procedures shall be established specifying how to communicate and deal with suspected inaccuracies 5. Data processed within TAS³ shall be integrity protected where appropriate 6. In the event of indirect collection, data shall be verified with data subject where possible prior to further processing 7. Data modification rights shall be restricted to duly authorized entities 8. Appropriate security policies (e.g. use of cryptography) to ensure authenticity and integrity shall be implemented 9. All technical and organisational measures relating to data accuracy procedures shall be documented and audited on a regular basis	1. TAS³ will enable indication of the "level of confidence" in meta-data where appropriate 2. Sticky policies will restrict unauthorized modification throughout data life cycle (see deliverables D2.1, D4.2 and D7.1)

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

by law or through an exception recognized in law 4. All technical and organisational measures relating to data accuracy procedures shall be documented and audited on a regular basis	

Confidentiality and Security of Processing	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Appropriate identification, authentication and authorisation mechanisms shall be in place 2. Roles and responsibilities shall be defined for at least the following tasks: • performing the required authentications, authorizations and checks for every processing operation • the maintenance of logs for the different processing operations that take place; • trusted (third) party services (e.g. attribute certification, identifier conversion etc); • updating of technical policies in accordance with permissions granted by data subject and legal developments • oversight; including regular verification of compliance, redress and point-of-contact in the event of a security breach 3. Identity life cycles shall be managed in a way which provides an assurance level proportionate to the interests at stake 4. Procedures shall be established for verification of each relevant attribute (e.g. capacity of doctor) of a requesting/asserting entity with a level of assurance proportionate to the interests at stake 5. Access and processing limitations supporting sufficient level of granularity shall be implemented 6. Appropriate security policies to ensure confidentiality, authenticity, integrity shall be implemented 7. Physical access to terminals which enable sensitive processing operations shall be	1. Implementation of advanced security policies to ensure confidentiality, integrity and authenticity (see deliverables D2.1 and D7.1) 2. Use of Authoritative sources in user- and access management (ABAC) in addition to RBAC; credential issuance and validation service (see deliverable D7.1) 3. Use of sticky policies (see deliverables D2.1, D4.2 and D7.1) 4. Additional measures to avoid unnecessary linkability (pseudonym management) (see deliverables D2.1, D4.2 and D7.1) 5. Secure & dynamic delegation service, consent as a default requirement, user call-back mechanism, dynamic policy update and policy evaluation in multiple instances where appropriate (see deliverables D2.1, D4.2 and D7.1) 6. Additional measures to avoid unauthorized or unnecessary monitoring (inter alia providing user choice where possible as to whether or not persistent or transaction ID is used) (see deliverables D2.1, D4.2 and D7.1) 7. Credential aggregation infrastructure (see deliverable D7.1) 8. BTG infrastructure (see deliverable D7.1)

restricted where appropriate 8. Restrictions and obligations shall be associated with individual data processing operation 9. TAS³ participants shall be required to adopt internal privacy policies (documenting security measures, specifying inter alia persons responsible, what to do in the event of a breach, …) and to provide education and awareness training for all persons who come in contact with personal data 10. Confidentiality agreements shall be put in place or exacted where appropriate 11. Security officers shall be designated or designation thereof shall be required where appropriate 12. All technical and organisational measures relating to security shall be documented and audited on a regular basis	

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

where appropriate (e.g. notification to oversight committee in the event of suspicious behaviour) 6. All technical and organisational accountability measures shall be documented and audited on a regular basis	

Transparency and Data Subject Rights (notification, access, rectification, object, deletion)	
Technical and organisational measures used to achieve compliance within TAS³	*Technical and organisational TAS³ best practices*
1. Data controllers and otherwise responsible entities shall be clearly communicated to data subjects 2. It shall be widely communicating to whom and how data subject may direct requests regarding data subject rights and how they are to be exercised 3. Internal procedures shall be adopted and/or exacted to reply to these requests in a timely manner 4. The source of personal data and logic of processing shall be communicated when notifying data subject of decision based on such data where appropriate 5. All technical and organisational measures related to transparency and accommodation of data subject rights shall be documented and audited on a regular basis	1. TAS³ will provide notification to the data subject and/or to the public in the event of security breach 2. Enhanced transparency mechanisms allowing direct data subject access to view the processing operations performed upon his personal data (see D2.1)

This annex is a compendium of the TAS³ legal requirements set forth in both TAS³ D6.1 and D6.2. [58] The Annex includes not only the legal and policy requirements but also identifies several of the technical components needed to enable them. The Annex serves as the iterative working document between WP6 and the other Work Packages.[59]

[58] The tables provided here have been adapted from earlier work performed by one of the contributors in the context of the EU FIDIS project. See J.C. Buitelaar, M. Meints and E. Kindt (eds.), "D16.3: Towards requirements for privacy-friendly identity management in eGovernment", 2009, forthcoming on www.fidis.net.

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

8.4 Annex 4 – WP6 Requirements list

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

The current list is still not exhaustive and will continue to be updated. For readability purposes, we have grouped the requirements below in terms of data protection and more general operational requirements. Several requirements additionally have explanatory 'notes' associated with them to draw attention to certain specificities or additional considerations which need be taken into account during implementation.

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

1. Enrolment and contractual binding

- Req 6.1: Intake Process (Person). The intake process MUST include: documentation provisioning (including notice of privacy policy, disclaimers, and general terms & conditions) and agreement to be bound; validation of identity (proofing) with an appropriate level of assurance; and specification of a technical user interface.

- Req 6.2: Intake Process (Organization). The intake process MUST include: documentation provisioning (terms & conditions, privacy policies, disclaimers) and agreement to be bound; validation of identity with an appropriate level of assurance; verification of policies, contracts, infrastructure and the capacity to comply; and specification of technical interfaces and protocols.

- Req 6.3: Contract management. All participants to the TAS³ network MUST agree to adhere to and execute the relevant TAS³ contractual documents.
    - Req 6.3.1: A versioning and archiving system MUST exist for contract terms.
    - Req 6.3.2: A versioning and archiving system MUST be in place for the informed consents given by data subjects.

- Req 6.3.3: It MUST be easy to ascertain which terms were in force, after the fact, if an issue arises (e.g. pursuant to a complaint or detected anomaly).

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

- Req 6.5 (EDITED): Binding Effect of technical processes & policies. All TAS³ participants and users MUST agree to be bound by the technical processes within the TAS³ network, including the obligations resulting from the transactions they engage in or choices they exercise through the TAS³ architecture.
  - Req 6.5.1 (EDITED): All TAS³ participants and users MUST agree to accept the contents of TAS³ logs as evidence of their actions within the TAS³ network (to the extent the relevant logging mechanisms are working properly and their properties have been appropriately disclosed and consented to).
  - Req: 6.5.1: The content of the instructions contained in (sticky or other) policies and the obligations associated with those instructions MUST be respected across the TAS³ architecture;
  - Req 6.5.2: It MUST be ensured that commitment to communicated policies and privacy preferences cannot be repudiated at a later time;
  - Req 6.5.3: In instances where personal data will be further processed outside the TAS³ network/architecture, the recipients of this data MUST commit to continued adherence to the content of associated sticky policies or other usage directives;
  - Req 6.5.4: Policy information MUST be easily accessible to all relevant parties;
  - Req 6.5.5 Policies MUST be drafted and communicated in a way that is appropriately tailored to and accessible by its intended audience[60], so as to enable all relevant parties to understand their scope of application and which resources (data, services etc.) are governed by which policies[61];

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

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

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

- Req 6.7: The TAS³ policy framework MUST cover all aspects of data processing and the associated legal data protection requirements.

2. Assignment of roles and responsibilities

- Req 6.8: Allocation of roles and responsibilities: Responsible entities and roles SHALL be defined for at least the following tasks:
    - receiving and registering consent;
    - providing notice and transparency;
    - performing the appropriate authentications, authorizations and checks for every processing operation;
    - the maintenance of logs for the different processing operations that take place;
    - trusted (third) party services (e.g. attribute certification, identifier conversion etc);
    - enforcement and updating of technical policies in accordance with permissions granted by data subject and legal developments;
    - front-end accommodation of the rights of data subjects such as the right of access and correction;
    - oversight; including regular verification of compliance, redress and point-of-contact in the event of a security breach.

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

3. Legitimacy of processing

- Req 6.10: Collection, use, and subsequent use, of personal data MUST be with the informed consent of the data subject EXCEPT where mandated by law or through an exception recognized in law.

    - Req 6.10.1: Data subject consent legitimizing the processing MUST be freely given, informed[62], and unambiguous[63].

---

legalistic language and adopting a plain-English, readable approach see http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_information_sharing_framework_draft_1008.pdf

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

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

- Req 6.10.2: Where required by the competent jurisdiction (e.g. in case of processing of health data), or where this is considered desirable for later evidentiairy purposes, the consent of the data subject MUST be in writing (or electronic equivalent thereof).

- Req 6.11: In instances where the data subject cannot provide his consent to the processing in a valid manner (e.g. relationship of command), an alternative legally permitted ('legitimate') basis MUST be present to justify the processing.[64]

- Req 6.13: The TAS³ network SHALL provide the data subject, if so desired, with the ability to express his privacy preferences in a granular fashion (avoid "all or nothing" approach when possible; support individual privacy preferences)

- Req 6.14: The TAS³ network SHOULD consider technical policy enforcement mechanisms which can establish that there is in fact a legal basis for the processing prior to authorizing an action (e.g. by specifying them as policy conditions or through use of sticky policies)

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

4. Finality

- Req 6.16: Purpose specification. The purpose(s) for collection and subsequent processing of personal data MUST be clearly specified.

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

- Req 6.17 (EDITED): Consent Capture for New or Changed Use: If an entity wishes to process personal data in a manner which cannot objectively be considered as compatible with the originally specified purpose(s), a new informed consent MUST obtained from the data subject prior to this new or changed use, unless this processing is explicitly required or permitted by law.[65]

- Req 6.18: Each participant of the TAS³ network MUST have a privacy policy that articulates restrictions and obligations with regards to subsequent use of the personal data it has under its control.

[64] See articles 7-8 of the Data Protection Directive.
[65]

- Req 6.19: When personal data is forwarded from one TAS³ participant to another (or from a participant to a non-participant), it MUST be determined under which policies (in particular: under which restrictions and obligations) this data is being passed on.

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

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

    - Req 6.19.3: The data subject SHALL be provided with additional and explicit information if the if a requestor/future recipient of information is not a part of the TAS³ network.

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

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

  Note: Seeing as such information (the purpose for which a processing can be authorized / has taken place) can be highly-sensitive in and of itself, careful consideration MUST be given to deciding which entity shall be trusted to register and verify the asserted/permitted purposes.

5. Data minimization

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

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

- Req 6.23: Collection Limitation: The TAS³ network and related processes MUST install appropriate limits on personal data collection to what is needed for legitimate, identified and notified business purpose.

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

- Req 6.25: Selective attribute/personal data disclosure during authentication: Authentication protocols MUST be designed in a way which ensures that no more attributes/personal data than needed for the processing are verified or propagated (e.g. avoid unnecessary leaking of identifiers).

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

- Req 6.26: Storage limitation: Procedures MUST be in place to ensure destruction or anonymization of personal data once the purpose for which it was collected and/or further processed has been completed

    - Req 6.26.1: Prior to initiating any processing operation upon personal data, the storage duration of each data element MUST be specified, either individually or by category, for every entity that is involved in the processing. This SHALL be done as part of the service/process definition.

    - Req 6.26.2: Data Management. Data MUST be managed according to a data life cycle which describes its management from collection to deletion, and all processes in between, including which events trigger which processes.

    - Req 6.26.3: The TAS³ network SHALL support technical obligations languages which allow data providers to specify the time-span after which deletion is mandatory.

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

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

6. Data accuracy

- Req 6.28: Designation of authoritative sources: In order to ensure data accuracy to the fullest extent possible, an inventory MUST be maintained that describes which entities are authorized to act as data providers (authoritative source) for which data sets.

- Req 6.29.: Verification procedures MUST be in place to ensure the trustworthiness of each attribute with a level of assurance proportionate to the interests at stake.
    - Req 6.29.1: Where appropriate, review and update procedures MUST be in place for personal data which is being kept for an extended period of time.
- Req 6.30: Procedures MUST be in place on how to report and deal with suspected inaccuracies.
    - Req 6.30.1: Data subjects MUST have the ability to check the accuracy and quality of the data, and to report suspected inaccuracies. (see Reqs 6.58 et seq.);
    - Req 6.30.2 (EDITED): In the event of indirect collection, the accuracy of the data SHOULD be verified with the data subject where this is both possible and appropriate;
    - Req 6.30.3: In case of amendment, notification MUST be provided to relevant entities (e.g. entities to whom data has been forwarded / who have accessed the data and continue to rely on it) (see also Req 6.65)
- Req 6.31: Where further verification or assurance of data quality is still needed, there MUST be a clear indication of the need for further verification when appropriate.
    - Req 6.31.1: Indication of level of confidence: each element of personal data SHOULD have a 'level of confidence' associated with it (e.g. self-asserted, verified with authoritative source by trusted data manager, inaccuracy reported etc) and this level of confidence SHOULD be reflected in its meta-data where appropriate.
- Req 6.32: The integrity of data maintained in authoritative sources MUST be appropriately guaranteed.
    - Req 6.32.1: Modification rights MUST be restricted to authorized entities on a 'need-to-modify' basis.
- Req 6.33: Data to and from authoritative sources MUST be authenticated through use of data origin authentication protocols to ensure authenticity and integrity where appropriate.
- Req 6.34: Relying Parties and other data recipients SHALL commit to only process personal data further if there is sufficient certainty as to its origin and integrity (i.e. upon verification that it emanates from the trusted source and has not been subject to unauthorized manipulation).
    - Req 6.34.1: Policies SHALL be in place which specify how a 'sufficient level of certainty' as to the origin and integrity of personal information is established.

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

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

7. Confidentiality and security of processing

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

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

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

- Req 6.39: Identity and credential life cycle management. Policies and measures to ensure appropriate identification and authentication of entities attempting to perform a particular action MUST be in place.

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

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

    - Req 6.39.3: Adequate policies specifying minimum levels of entity authentication assurance in a manner that is proportionate to the interests at stake MUST be in place;

    - Req 6.39.4: Adequate procedures to ensure proper verification of relevant attributes of requesting/asserting entities (e.g. a pre-requisite professional qualification) MUST be in place (e.g. through use of authoritative sources as an integrated component in user- and access management).

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

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

- Req 6.40: Authorization. Technical policy enforcement mechanisms MUST support a sufficient level of granularity with regards to the access and further processing rights (privileges) of each requesting entity. To this end at least the following measures MUST be taken (see also Req 6.24):

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

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

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

    - Req 6.40.4: For each object that qualifies as personal data a list of valid recipients MUST be defined or definable immediately upon request at any point in time;

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

    - Req 6.40.6: Authorization profiles for resources MUST be defined and enforced; indicating which resource is accessible to which type of entity/application in which capacity, in what situation and for what time period.

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

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

- Req 6.42: Use of cryptography. TAS³ MUST support the use of cryptography to ensure confidentiality, authenticity and integrity of personal data where appropriate.

  Note: this requirement pertains both to transmission (channel security) and storage.

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

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

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

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

- Req 6.47: Each participant MUST adopt internal privacy policies documenting security measures (specifying inter alia the persons responsible within the organization (e.g., security officers), what to do in the event of a security breach etc.).[66]

- Req 6.48: Confidentiality agreements. Natural persons who are employed by (or otherwise perform services for) TAS³ participants MUST be bound by a contractual duty to respect the confidentiality of data when this is required by law.[67] TAS³ SHOULD consider instituting such an obligation towards all TAS³ participants.

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

8. Transparency and notice

- Req 6.49: Whenever personal data shall be processed, the following MUST be specified: the identity of the controller, what data is collected and how, why it is being collected (purpose of the processing), how it will be used, who it might be shared with, and how it will be managed.[68]

8.1 *Direct collection*

[66] Such policies must of course be compatible with the TAS³ governance framework.
[67] E.g. in certain jurisdictions such agreements are required when such employees or contractors are charged with handling of sensitive data such as health data.
[68] The data subject MUST in principle be notified of the elements listed in Req 6.49 prior to initiating any (entirely new or 'incompatible') processing operation involving personal data (or at least have access to this information upon request – see Req 6.53).

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

    - Req 6.50.1: In case of direct collection, the data subject MUST be provided with the following information (except where he already has it):
        - the identity of the controller (and, if applicable, of his representative);
        - the purposes of the processing for which the data are intended;

    - Req 6.50.2: The data subject SHOULD also be informed of:
        - the recipients or categories of recipients of the data;
        - whether replies to questions he is asked are obligatory or voluntary, as well as the possible consequences of failure to reply;
        - the existence of the right of access to and the right to rectify the data concerning her.

    - Req 6.50.3: The data subject MUST be provided with the information listed in Req 6.44.2 when this is necessary to guarantee fair processing in respect of the data subject, when considering the specific circumstances in which the data are collected.

8.2 *Indirect collection*

- Req 6.51: Notice requirements where data is not obtained directly from data subject herself (indirect collection):

    - Req 6.51.1: In case of indirect collection, the data subject MUST**, at the moment of undertaking, or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed, be provided with the following information:
        - the identity of the controller and of his representative, if any;
        - the purposes of the processing;

    - Req 6.51.2: The data subject SHOULD also always be informed of:
        - the categories of data concerned;
        - the recipients or categories of recipients;
        - the existence of the right of access to and the right to rectify the data concerning her

    - Req 6.51.3: The data subject MUST be provided with the information listed in req 6.28.2 when this is necessary to guarantee fair processing towards the data subject (taking into account the specific

circumstances in which the data are collected) or when this is required by the applicable national legislation.

** Note: Requirements 6.51.1-3 MAY in principle be discarded where:

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

8.3 *Implementation*

- Req 6.52: All the information elements listed in Reqs 6.44-6.45 SHALL be made readily available to (both actual and potential) data subjects in the form of a privacy policy (or policies), which is (are) both easily accessible and easy to understand.

- Req 6.53: Layered approach. In order to limit complexity, the fulfilment of Reqs 6.51-6.52 need not necessarily take the form of a single document.[69] TAS³ SHALL adopt a 'layered' approach for notice when appropriate.
  - Req 6.53.1: This approach SHALL NOT contain more than three layers of information (short – condensed – full)
  - Req 6.53.2: The sum total of these layered notices MUST meet the notice requirements imposed by the applicable national legislation.
  - Req 6.53.3: It MUST be easy to ascertain which data processing operations are governed by which policies.

- Req 6.54: Privacy policy for TAS³ portal (full notice). The privacy policy notice provided on the TAS³ portal SHALL not only cover the processing operations performed by the portal provider itself, but SHALL also include a general notice with regard to the operations of entities participating to the TAS³ network as service providers.
  - Req 6.54.1: In addition to the elements in Reqs 6.44-6.45, this notice SHALL also contain a point of contact for questions and information and redress mechanisms

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

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

- Req 6.55: Each entity participating in the TAS³ network as a service provider MUST also provide notice of its own privacy policy (policies), which provides further details specific as to its particular processing operations.
  - Req 6.55.1: In addition to the elements in Reqs 6.44-6.45, this notice SHALL also contain a point of contact for questions and information on redress mechanisms
  - Req 6.55.2: These privacy policies SHOULD also cross-reference the TAS³ infrastructure privacy policy where appropriate.

- Req 6.56: Consent to notices. The consent of the data subject MUST (as a rule[70]) be obtained in relation to privacy policies listed in 6.47-48 prior to any processing of his personal data, by either TAS³ Infrastructure Members or one of the participating TAS³ entities (see Req 6.10).
  - Req 6.56.1: A versioning and archiving system MUST be in place for the informed consents given by data subjects to enable later verification that appropriate notice was given (see also Req 6.3)

- Req 6.57: If any entity within the TAS³ network intends to process personal data for an additional purpose (i.e. a purpose which has not yet been previously specified and communicated to the data subject), a subsequent notice MUST be provided, and the data subject MUST be given the ability to either accept or reject the envisaged processing, EXCEPT where the processing is mandated by a legal obligation (see also Req 6.17).[71]

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

- Req 6.58: Access request process/Accuracy: a process MUST be in place which enables users to request access to (and possibly amend or correct) personal data relating to them which has or is being processed within the TAS³ network.

- Req 6.59: Blocking and erasure: a process MUST be in place which enables blocking or erasure of specific data elements upon request of the data subject, unless the processing is specifically mandated by law.

---

[70] In instances where the data subject cannot provide his consent to the processing in a valid manner (e.g. relationship of command), an alternative legally permitted basis must be in place (see Req 6.11). This situation does not remove to obligation to inform the data subject of such processing (see Reqs 6.49 et seq.)

[71] Req 6.57 does not apply where the processing is based on a legally admissible basis other than consent AND where such notice is impossible or would involve a disproportionate effort. However, such instances of overriding legitimate interest MUST at least be generically outlined in the TAS³ privacy policy notice(s) mentioned in Reqs 6.54-55.

9.1 *Right of access*

- Req 6.60: Upon request, the data subject MUST be provided with confirmation, as to whether or not data relating to her are being processed, and information at least as to:
    - the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are (have been) disclosed;
    - the data undergoing processing and of all available information as to its source;
    - the logic involved in the processing of data particularly where automated decisions are involved.
- Req 6.61: The confirmation and information listed in Req 6.53 MUST be provided without constraint or excessive delays or expense.

9.2 *Rectification, blocking and erasure*

- Req 6.62: Data subject requests to rectify, block or erase data MUST be accommodated at all times EXCEPT where an overriding legitimate interest exists.
    - Req 6.62.1: Such overriding interest SHOULD be specified in the TAS³ privacy policy notice(s).
    - Req 6.62.2: Data subject requests to rectify, block or erase data MUST in any event be accommodated in case the processing infringes upon the applicable national data protection legislation.
    - Req 6.62.3: In case of denial, the reason for denial MUST be communicated to the data subject.
- Req 6.63: The TAS³ privacy policy MUST specify:
    - to which entity in particular data subjects should address their request for access, rectification, blocking or erasure in which instance;
    - which entity shall decide these requests;
    - valid reasons for denying the request;
    - the time-frame in which this request will be processed;
- Req 6.64 (EDITED): A procedure SHOULD be in place to adequately deal with the situation whereby a TAS³ actor receives a data subject request which is not competent to decide itself.

9.3 *Notification to third parties*

- Req 6.65: A process MUST be in place that provides notification to third parties to whom the data have been disclosed in case of corrections, erasure of

blocking of processing of personal data pursuant to a request by the data subject.

9.4 *Implementation*

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

- Req 6.67: Where appropriate, the TAS³ Dashboard SHOULD also provide data subjects with more detailed information as to the processing operations performed upon their personal data (e.g. at what time individual processing operations took place, under which pretext etc.).

- Req 6.68: The TAS³ Dashboard SHOULD provide an interface which enables exercise of the data subject rights listed in Reqs 6.55 (or at least direct the user as to how those rights may be exercised).

- Req 6.69: The TAS³ Dashboard SHOULD support automatic notifications to relevant parties in case of corrections, erasure of blocking of processing of personal data pursuant to a request by the data subject

10. Accountability and compliance verification

10.1 *Logging*[72]

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

- Req 6.71: The level of detail of log files MUST be sufficient as to enable compliance verification and oversight of processing operations with the governing policies

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

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

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

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

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

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

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

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

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

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

    - Req 6.75.2: In case of non-targeted compliance verification (e.g. detection of anomalies through dedicated algorithms), the log data MUST first be de-identified/pseudonymized. Only after an anomaly has been detected may the log information be re-identified.

10.2 *Audit & oversight*

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

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

- Req 6.78: Each participant MUST be bound to provide co-operation to entities in the TAS³ network charged with oversight & audit.

10.3 *Other accountability mechanisms*

- Req 6.79: Both within the TAS³ network and within each participating entity internal responsibility and accountability mechanisms MUST be adopted (e.g. designating 'owners' for both equipment and processing operations where personal data is involved).

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

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

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

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

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

- Req 6.82: Procedures MUST be in place to ensure that when requested it is possible to indicate the source of the personal data that is being processed, as well as what the reason for processing has been.

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

9.4 *Complaint handling*

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

  - Req 6.84.1: The complaint capture system SHOULD include a feedback mechanism which enables users to both
    - provide information to reputation engines or other trust entities that may be evaluating service providers, and to

        - initiate procedures for privilege revocation as a consequence of intentional or uncured breach of terms, and corresponding redress.

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

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

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

11. Notification & prior checking

- Req 6.87: Where required by the applicable law, the TAS³ network and/or its participants MUST ensure prior notification and/or prior checking with national data protection authorities

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

- Use of up-to-date Anti-virus/ Spyware/ Malware detection systems
- Spam filters (may need to define settings to assure that legitimate mail is not suppressed)
- Penetration testing (may only be appropriate for largest players)[i]
- Encryption
    - In transit
    - At rest
- Security policies
    - Physical
    - Logical
    - Administrative
    - Separation of Duties
- Privacy policy
    - W/specific obligation to honour preferences and negotiated obligations of end-users
    - Notice
- Complaint handling policies / mechanism
- Compliance processes/officer
- Contact points

- Internet Access and Use Policies
- Training
- Code of ethics
- HR Policies (related to vetting of employees that have access to personal to the extent permitted by law)
- Service Level Agreements
- Breach Notification
- Disaster recovery / Business continuity plans/exercises
- Audit/oversight
- Exceptions and Emergencies handling policies
- Government/Law Enforcement obligations/request for information policies
- Third party agreements' obligations/requirements clauses

8.5 Annex 5 – Requirements for the TAS³ eHealth pilot

1 Introduction

This annex describes the legal framework to be taken into account for the deployment of the Tas³ health pilot in the Netherlands. It focuses on Dutch law only compiling requirements in the fields of data protection and patients' rights, the two most important legal domains for the health pilot. The comprehensive discussion on data protection and patients' rights is completed with highlights of other regulatory instruments that should be taken into account when developing a trusted architecture for securely shared services in the field of health. Finally the annex furthermore reflects on the recent legal developments in the Netherlands concerning the implementation of ICT in health in general and the Electronic Patient File specifically.

Since this annex is focussed on the legal knowledge necessary to deploy the health pilot in the Netherlands in a legally correct way with respect for the involved patients, it was decided to include it in Work Package 6 – Legal, privacy and ethics. However, dissemination will take place within WP9 – Employability and Healthcare demonstrators as it is to their use that this deliverable was written.

Coloured boxes throughout the text mark policy recommendations and for Tas³ important conclusions to ease the reading.

2 The Regulatory Framework for eHealth in the Netherlands

After a short introduction to the Dutch healthcare system and the current developments concerning eHealth in the Netherlands, this first chapter will provide an overview of the regulatory instruments to be taken into account for the Tas3 health pilot in the Netherlands.

2.1 Introduction to eHealth in the Netherlands

Only recently the Dutch eHealth strategy was carefully studied in the EC SMART study on Legal Framework of Interoperable eHealth in Europe[73]. That report concludes:

"The Dutch government has taken major steps over recent times towards the development of the Electronic Health Record. The introduction of legislation relating to the 'Burger Service Nummer' and the use of this number for the exchange of electronic information has made the actual use of the EPD a possibility. The fear of invasions of privacy due to misuse of the patients' details has delayed the introduction of the EPD over recent years. This still remains a worrying aspect."

2.1.1 The Dutch healthcare system

The Dutch healthcare system has a private character with public limiting conditions. In The Netherlands healthcare is – in principle - provided by private care suppliers both individuals and institutions. The Dutch the government, more specifically the Dutch ministry of Health, Welfare and Sport[74], does not participate in the provision of care, but aims to ensure the wellbeing of the population and to help the populace to lead healthy lives by defining policies limiting the private care suppliers.

Since 2006 a new health insurance system has been in place seeking for a balance between a solid basis and the dynamics of the market and centralizing the patient. The New Health Insurance Act, introducing the new health insurance system, stipulates that a) everyone in the Netherlands is obliged to take out insurance on the threat to be fined, but are free to change insurer every year; b) health insurers can compete for the business of the insured by paying

[73] The full results of the SMART study for The Netherlands can be found in the National Profile of The Netherlands, available at: http://ec.europa.eu/information_society/activities/health/studies/published/index_en.htm. The concluding report can be found at: http://ec.europa.eu/information_society/activities/health/docs/studies/legal-fw-interop/ehealth-legal-fmwk-final-report.pdf.

[74] Ministerie voor Volksgezondheid, welzijn en sport, in short 'VWS'.

more attention to their performances and by providing tailor-made care, but are obliged to accept everyone irrespective of age, gender and state of health; c) the patient / client is given a more central role with more opportunities but also more responsibility because he will need to single out the provider offering the best care conditions and it is up to him to bring about improvements of the quality of care; d) the government remains responsible for the accessibility, affordability and quality of health care, including the provision of compensation to people on low incomes.

In general, three parallel compartments of insurance should guarantee access to health care facilities and services of high quality should be guaranteed for all.

- Insurance for short-term medical care is provided and funded by the state and the insurers.
- The so called 'uninsurable medical risks' and the long-term care are covered by the 'Exceptional Medical Expenses Act' and is largely provided and funded by the state.
- For care which is not included in the first or second compartment (such as dental care and alternative medicine) can be insured on a voluntary basis.

2.1.2 ICT in Dutch healthcare

The aim for an affordable, accessible and high quality healthcare was not only the underlying factor to the reform of the health insurance, but also to the uptake of ICT in healthcare in general. The Ministry of Health, Welfare and Sports works in close collaboration with the National IT Institute for Healthcare[75] and the Central Information Point for Healthcare Professions[76] on this domain.

The most recent realization from the Dutch Ministry - together with the players in the health care sector – is the development of a nationwide system for the safe and reliable electronic exchange of medical data, called 'AORTA'. The infrastructure consists of a) a national registration system for identification and authentication of patient, healthcare providers, insurers and other care agencies and b) a National Switch Point which provides a reference index for routing, identification, authentication, authorization and logging.

Currently the priority of the Dutch government is the deployment of a nationwide electronic patient file ('electronisch patiënten dossier', or in short 'EPD'):

"The EPD is a virtual record, comprising a set of applications which are connected to the national infrastructure, AORTA. Data from different healthcare information systems are linked in the EHR. Authorized care providers can consult these data to obtain a clear picture of a patient's medical history or medication use."

[75] NICTIZ, www.nictiz.nl.
[76] CIBG, www.cibg.nl.

2.1.3 Key regulations for health and ICT

With regards to the use of ICT in health in the Netherlands in general and Electronic Patient Files more specifically, two laws in particular constitute the legal framework:

- the Wet Geneeskundige Behandelingsovereenkomst[77] (law concerning the contract for medical treatment)

- and the Wet Bescherming Persoonsgegevens[78] (law on Data Protection).

Since 2008 discussions are furthermore going on about a proposal of law altering the law on the use of the citizen service number in care in connection to electronically shared health data (de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg). This altering law aims to introduce a national electronic health record[79].

Each of these three key pieces of law will be discussed in the following paragraphs and chapters.

Since the implementation of a new health insurance system in 2006 the Dutch government considers the patient as the driving force for innovation in and evolution of healthcare. Through the obligation for the patient to take out private health insurance, but allow them free choice of insurer, the government hopes to commend consumer driven changes. This does however not mean the government stopped the push for change. After having developed a national infrastructure for safe and reliable exchange of medical data 'AORTA', its current priority is the deployment of a nationwide electronic patient file. Discussion on the regulation of the EPD was ongoing at time of writing.

2.2 Regulatory Framework for Data Protection

As is the case in all the EU Member States, the Dutch Data Protection regulations are characterized by the transposition of Directive 95/46 (hereinafter 'DPD'). In 2000 the Law Protecting Personal Data (Wet van 6 juli 2000 houdende regels inzake de bescherming van persoonsgegevens, hereinafter 'Wbp') was approved and the focus was shifted from registration to the act of processing. Before the introduction of the DPD the Dutch privacy regulations focused a lot on the registration, use and supply of personal data in person registration systems[80]. The introduction of the DPD however required a shift in focus to the act of data processing, subjecting every single data processing act to regulation. Ever since, a distinction is *in se* not made between data processing actions in which data are actually handled and purely technical data processing actions. This causes a more rigid data protection regime, protecting the processing of personal data not

[77] The WGBO consists of artt 7:446-7:468 NBW.
[78] Wet van 6 juli 2000 houdende regels inzake de bescherming van persoonsgegevens (in short 'Wet Bescherming Persoonsgegevens' or 'WBP').
[79] Voorstel van wet tot wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische uitwisseling in de zorg, stuk 31.466.
[80] Old Wet Persoonsregistraties (WPR), 1989.

only when the protection of the privacy is at stake, but at any time[81]. Furthermore, the new data protection regulation is also characterized by a broadened scope, protecting not only personal data *strictu sensu* but also personal images and sounds. Naturally this includes also personal health information.

With regards to personal medical data account should however not only be taken of the Wbp, but also of the Civil Code (Burgerlijk Wetboek, hereinafter 'BW'). Although the Civil Code primarily aims to regulate the patient-carer relationship, it also protects personal data by explicitly protecting the right to privacy of the patient. The privacy related provisions of the Civil Code should be regarded as specifications of the Wbp, causing both laws to be applicable in parallel to the processing of medical data[82].

The regulatory framework for the protection of personal health data in the Netherlands constitutes (primarily) of the Law Protecting Personal Data (Wet van 6 juli 2000 houdende regels inzake de bescherming van persoonsgegevens, in short 'Wbp') and the Dutch Civil Code.

2.3 Regulatory Framework concerning Patients' Rights

In the Netherlands patients' rights are protected in a special section of the Civil Code, also called the 'Wgbo' or Wet Geneeskundige BehandelingsOvereenkomst (in English that makes the Law on Medical Treatment relationship)[83]. The articles 7:446 – 7:468 Civil Code, which constitute the Wgbo, entered into force on the 1st of April, 1995 intending to reinforce the legal status of the patient. Through the enactment of previously recognized but scattered patient rights and the uptake of some new rights, the patients' and practitioners' legal certainty was strengthened[84].

The patient – practitioner relationship is regulated as a service agreement. The first implication thereof is that the practitioner can – in principle – not terminate the contract[85]. Secondly this also implies - as is the case in many European Member States - that mainly patients' rights are regulated. Patients' obligations are – except for the obligation to pay the health care practitioner and to cooperate – not enacted. The fact that the agreement is characterized as a provision of services, does however not prevent the Wgbo from providing some protection to the practitioner too.

---

[81] J. Prins en J. Berkvens (eds), Privacyregulering in theorie en praktijk, in Recht en Praktijk, Kluwer, Deventer, 2002, 1.
[82] J. Nouwt, "*Privacy en medische informatie*" in J. Prins en J. Berkvens (eds), Privacyregulering in theorie en praktijk, in Recht en Praktijk, Kluwer, Deventer, 2002, 255.
[83] Boek 7, Titel 7, afdeling 5 Burgerlijk Wetboek: De overeenkomst inzake geneeskundige behandeling, artt 7:446 – 7:468.
[84] J. Legemaate, De Wgbo: van tekst naar toepassing, Bohn Stafleu Van Loghum, Houten-Diegem, 1998, 1-3.
[85] exceptions are however possible when the practitioner can call upon decisive elements.

As was the case with data protection, patients' rights are also protected trough other regulations than the Wgbo. Some protection can be found in

- the Wbp;
- the Law regulating Mentorship for adults (Wet mentorschap ten behoeve van meerderjarigen)[86];
- the Law BOPZ (Wet BOPZ)[87];
- the Law medical examinations (Wet medische keuringen)[88];
- the Law medical-scientific research with human beings (Wet medisch-wetenschappelijk onderzoek)[89];
- the Law concerning consumer complaints in the healthcare (Wet klachtenrecht cliënten zorgsector)[90];
- the Law concerning organ donation (Wet orgaandonatie)[91].

Because of the specificity of these provisions and given the impression that they are not of particular importance for the Tas3 health pilot, they will be further elaborated on and are only mentioned for the reason of completeness.

In the Netherlands patients' rights are primarily regulated by the articles 7:446 – 7:468 of the Civil Code. This special section is also referred to as the 'Wgbo' or Wet Geneeskundige BehandelingsOvereenkomst, in English: the Law on Medical Treatment Relationship. It has to be noted that specifications to this law are often provided in situation specific regulatory instruments.

2.4 Other relevant regulations

2.4.1 Regulatory framework for patients' summaries

Up until today The Netherlands don't have legal provisions in the area of patients' summaries. However it looks like this will be changing soon as account should be taken of the above mentioned developments concerning the proposal of law altering the law on the use of the citizen service number in care in connection to electronically shared health data (de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg). This law introduces a national electronic health record[92], addressing issues such as

[86] Wet van 29 september 1994, houdende mentorschap over meerderjarigen
[87] Wet van 29 oktober 1992, houdende bijzondere opnemingen in psychiatrische ziekenhuizen
[88] Wet van 5 juli 1995, houdende regels tot versterking van de rechtspositie van hen die een medische keuring ondergaan.
[89] Wet van 26 februari 1998, houdende regelen inzake medisch-wetenschappelijk onderzoek met mensen.
[90] Wet van 29 mei 1995, houdende regels ter zake van de behandeling van klachten van cliënten van zorgaanbieders op het terrein van de maatschappelijke zorg en gezondheidszorg.
[91] Wet van 24 mei 1996, houdende regelen omtrent het ter beschikking stellen van organen.
[92] Voorstel van wet tot wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische uitwisseling in de zorg, stuk 31.466.

security, data quality, authorization, access and standardization and intends to at least regulate:

- the mandatory connection of healthcare practitioners with a National Switch Point
- the electronic availability of patient data via the National Switch Point
- safe and reliable information exchange via the National Switch Point (Landelijk Schakelpunt or 'LSP'), which will become the crucial and indispensable hub for a nationwide EPD.

For a good understanding of the current implementation plans it is of crucial importance to distinct local or regional systems from the foreseen national system. Local or regional health records are already in use in the Netherlands, but they are not regulated by any specific legal provisions. The proposal of law currently under discussion in the Dutch senate intends to introduce a system for a countrywide shared EPD, aimed at data processing within the Netherlands.

This EPD will consist of a set of applications linked to the national infrastructure 'AORTA'. The actual deployment of the EPD will happen gradually, starting with the Electronic Medication Record and a Patient Summary Record.

The "Patient Summary Record for the GP" (WDH – Waarneem Dossier Huisartsen) was developed and approved as proof of concept in 2006. It contains a set of basic information elements based on the professional summary for GPs. That professional summary consists of the complete episode list, the journal list of the five consultations, the drug use, all medical intolerances and contra-indications, recent data transfer from other care providers. Many local or regional posts of general practitioners use the WDH now to exchange data between GP's and GP after hours posts.

Dutch regulation on the implementation of a Electronic Patient File is currently under discussion in the Senate. It concerns more specifically the proposal of law altering the law on the use of the citizen service number in care in connection to electronically shared health data (Voorstel van wet tot wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische uitwisseling in de zorg, stuk 31.466).

2.4.2 Dutch identity management for healthcare

In the Netherlands both care givers and care receivers are registered and identified through the use of a unique number. Healthcare professionals are given a Unique Care Providers Identification number (the UZI-number, uniek zorgverleners identificatienummer) [93]. For the identification and authentication of the patients the Citizen Service Number (the BSN-number, burger service nummer) is used[94]. Both identification numbers will also be used within the AORTA system.

[93] 'Unieke Zorgverleners Identificatie' or in short 'UZI'.
[94] 'Burgerservicenummer' or in short 'BSN'.

a) Citizen Service Number

The use of the Citizen Service Number for healthcare is still quite new. Since the 1st of June 2008 healthcare practitioners are entitled to use the BSN of their patients in their administrative systems. Since June last year the use of the BSN in healthcare is mandatory. The practitioners are obliged to include the BSN of the patient in every file and are obliged to use it when exchanging or sharing data with other healthcare professionals and with healthcare institutions[95]. With the citizen service number the Dutch authorities opted for one number used not only for healthcare but also in every other relationship a citizen has with the government.

In practice the patient will have to be identified himself through a physical document such as an ID-card or drivers license. The practitioner registers the number and the sort of document presented. Naturally this only needs to be done when a patient sees a particular practitioner for the first time. During the further course of the treatment relationship the practitioner only has the duty to ascertain oneself that he is dealing with the same patient. He can do this by recognition, by posing some questions or by again requesting an ID. After having identified the patient, the practitioner needs to request or verify the correct BSN from an authentic source such as the Sectoral Message Service for Care (Sectorale Berichten Voorziening in Zorg or in short 'SBV-Z'). This process needs to be followed in all care situations except for emergencies. When there is no time to request the ID or the BSN, however, it will still have to be completed after the care was given[96].

b) Unique identification for health care practitioners

In contrast with the BSN, the UZI-number is a sector-specific number. The UZI-number is a unique identification for healthcare practitioners in The Netherlands in the form of a UZI-card, a kind of electronic passport.

The UZI-card is used by healthcare practitioners to provide authentication, to guarantee confidential communication or to add an electronic signature. Authentication is particularly important when the healthcare practitioner requires access to, for example, an information system or website. With the help of an UZI-card healthcare practitioners can provide authentication, meaning they can prove their identity. The UZI-card also certifies that the pass holder is a healthcare provider and indicates whether he or she provides treatment on behalf of a healthcare institution. To access healthcare information however, authorization must also take place. The UZI-card does not say who is entitled to what information, but it does contain details on which basis authority can be granted. Next, the UZI-card does allow ensured confidential information exchange. The confidential function of the UZI pass guarantees the sender of the information that it can only be read by the person to whom it is sent, preventing anyone else from reading or changing this information. Finally the UZI-card also

[95] Wet van 10 april 2008, houdende de regels inzake het gebruik van het burgerservicenummer in de zorg.
[96] Factsheet Wbsn-z, available at: http://www.infoepd.nl/ufc/file/informatiepunt_sites/5fe84876325b7af0788d05e1c6ecc045/pu/epd_fs_c1.pdf.

allows the healthcare practitioner to electronically sign for example receipts, references or contracts, equaling a signature on paper.

The UZI-register is the organization that provides the unique identification and the UZI-cards to healthcare practitioners. The UZI-register is part of the Central Agency for Information on Healthcare Professions, an agency of the Dutch Ministry of Health, Welfare and Sports. The UZI-card looks like a bank pass and contains the electronic identity of the healthcare practitioner. It is of course protected against misuse by a unique pin code.

The Dutch authorities opted for the use of a single unique identification number for patients and made the use of the BSN in care obligatory since June 2009. Practitioners are obliged to request the patient to identify himself trough ID-card or drivers' license before they can retrieve and/or use the BSN. This is primarily to avoid mistakes.

For the health professionals, the Dutch government chose the opposite approach and launched a sector specific number, the UZI-number, and a sector specific eID, the UZI-pass.

The Tas[3] health pilot will have take the facilitation to the obligatory use of the BSN in patient files and the obligatory authentication of healthcare practitioners trough their UZI-card, into consideration.

2.4.3 Legal conditions for the practice of healthcare

In the Netherlands anyone – Dutch or non-Dutch – can practice medicine. On this principle the Individual Health Care Act (Wet op de individuele beroepen in de gezondheidszorg)[97], regulating the healthcare profession, is based. Naturally the BIG-law does stipulate conditions and restrictions to the use of a protected professional or academic title. The health professionals who are allowed to use a protected title are registered in the BIG-register. That way the legitimate use of the title can be checked and the compliance with legal educational standards can be assured to clients.

Non-Dutch graduates can be granted the right to use a protected professional or academic title in two ways. The Dutch Ministry can firstly recognize the foreign diploma as equal to the Dutch level of education. As a general rule, holders of such a diploma are entitled register or to use a certain academic title. Secondly, the holder of a foreign degree, who is not subject to the first, general rule or whose nationality is not mentioned in the general rule, may request the Ministry to recognize his diploma. The Ministry then can issue a certificate indicating there is no objection to the registration as far as the applicant's competence is concerned[98].

[97] Also called the 'BIG-wet', 11 November 1993.
[98] SMART Country report for The Netherlands, available at: http://ec.europa.eu/information_society/activities/health/studies/published/index_en.htm

Depending on the professional or academic title acquired, you are allowed to perform different medical acts. Doctors are the only professionals qualified to perform all so called "reserved actions". Dentists and midwifes for example are allowed to perform only certain of the reserved actions[99].

The BIG-register, in which all healthcare professionals who are allowed to use a protected title are registered, can be regarded as an authentic source for the qualifications of healthcare professionals.

2.4.4 Professional liability

Healthcare professionals may be held liable for professional errors under general Dutch civil law, criminal law and disciplinary rules. The Wgbo specifies that the healthcare practitioner must always act in accordance with the current professional standards, meaning he should act like a prudent carer[100]. The Wgbo furthermore introduces the liability of hospitals in case of an error made by a hospital-employed professional[101].

2.4.5 Professional secrecy

The patient has a right to secrecy. The professional secrecy in a medical setting is not restricted to the individual patient – practitioner relationship, but also stands with regards to preventive acts, medical examinations and scientific research. Furthermore the professional secrecy protects more than just medical data. Key rule to the professional secrecy is that the information or data provided by the patient should only be used for the purpose for which they were given. The professional secrecy should allow the individual patient to speak freely with the healthcare professional, both for his own good as to protect the society[102].

In the Netherlands the medical professional secrecy is embedded in civil, in criminal as well as in disciplinary rules. It is enacted in article 7:457 Civil Code, article 272 Criminal Code (Wetboek van Strafrecht) and article 218 Code of Criminal Procedure (Wetboek van Strafvordering). The medical professional secrecy is also incorporated in the Wgbo. Article 7:457 states that "*a medical practitioner does not provide information about the patient to a third party, nor does he grant access to the patient's record, unless on the grounds of a legal regulation. A third party is not the one whose professional cooperation is necessary to fulfill the contract, such as colleagues who have been consulted*". An exception is however made in article 7:458. The healthcare professional is allowed to supply information on the patient or allow access to records to a third party without the patient's consent for statistical or scientific research pruposes in the field of public healthcare.

---

[99] Art 36 BIG-law
[100] Art 7:453
[101] Art 7:462
[102] H. Leenen and J. Gevers (eds), Handboek gezondheidsrecht – Deel I. Rechten van de mensen in de gezondheidszorg, Bohn Stafleu Van Loghun, Houten/Diegem, 2000, 220-221.

Dutch healthcare practitioners are bound by a civilly, criminally and deontologically enforced professional secret. Key rule to the professional secrecy is that the information or data provided by the patient should only be used for the purpose for which they were given.

3 Requirements to Data protection in the Netherlands

As indicated above, the general regime for data processing in the Netherlands, is incorporated in the Law protecting personal data (Wet bescherming persoonsgegevens, hereinafter 'Wbp').

3.1 General Principles

Generally speaking the Dutch Personal Data Protection Act is very similar to the European directive. Both the European Directive and the WBP are based on the following principles[103]:

- **Restriction of purpose**: the processing of personal data is limited to prior specified purposes.
- **Quality**: the processed personal data has to be relevant for the registered purpose.
- **Transparency**: the controller has to provide information to the data subject prior to the processing.
- **Rights for data subjects**: such as getting access to the personal data or to request to delete or replace the data.
- **Security**: reasonable, state of the art, security measures has to be taken to protect the personal data.
- **Responsibility**: there has to be controller who is responsible for the processing of the data.

The Wbp does not put forward any different conditions for electronically processed data than manually processed data. However, many advisory bodies do stress the security aspects for electronically stored data. This was also the case in the recent advice of the Royal Dutch Medical Association (knmg) on how to deal with medical data[104].

Security is regarded an essential precondition for the electronic processing of personal data.

[103] Tekst en CommentaarTelecommunicatierecht, P.C. Knol, G.J. Zwenne, A.H.J. Schmidt, Kluwer, 2005, p. 433 ev.

[104] Knmg, Richtlijn inzake het omgaan met medische gegevens, januari 2010, available online: http://knmg.artsennet.nl/Home.htm.

3.2 The Wbp in schemes

The Dutch Ministry of Justice put a lot of effort into the accessibility of the Wbp-principles for citizens. This resulted – amongst other things - in easy to follow, step-by-step schemes determining the applicability, delineation of the roles and duties to notify and inform. In the following paragraphs translated versions of these schemes are provided, complemented with a short explanation.

Please note that in the schemes the words 'ja' and 'nee' were not replaced. 'Ja' means 'yes', 'nee' means 'no'.

3.2.1 Applicability of the Wbp

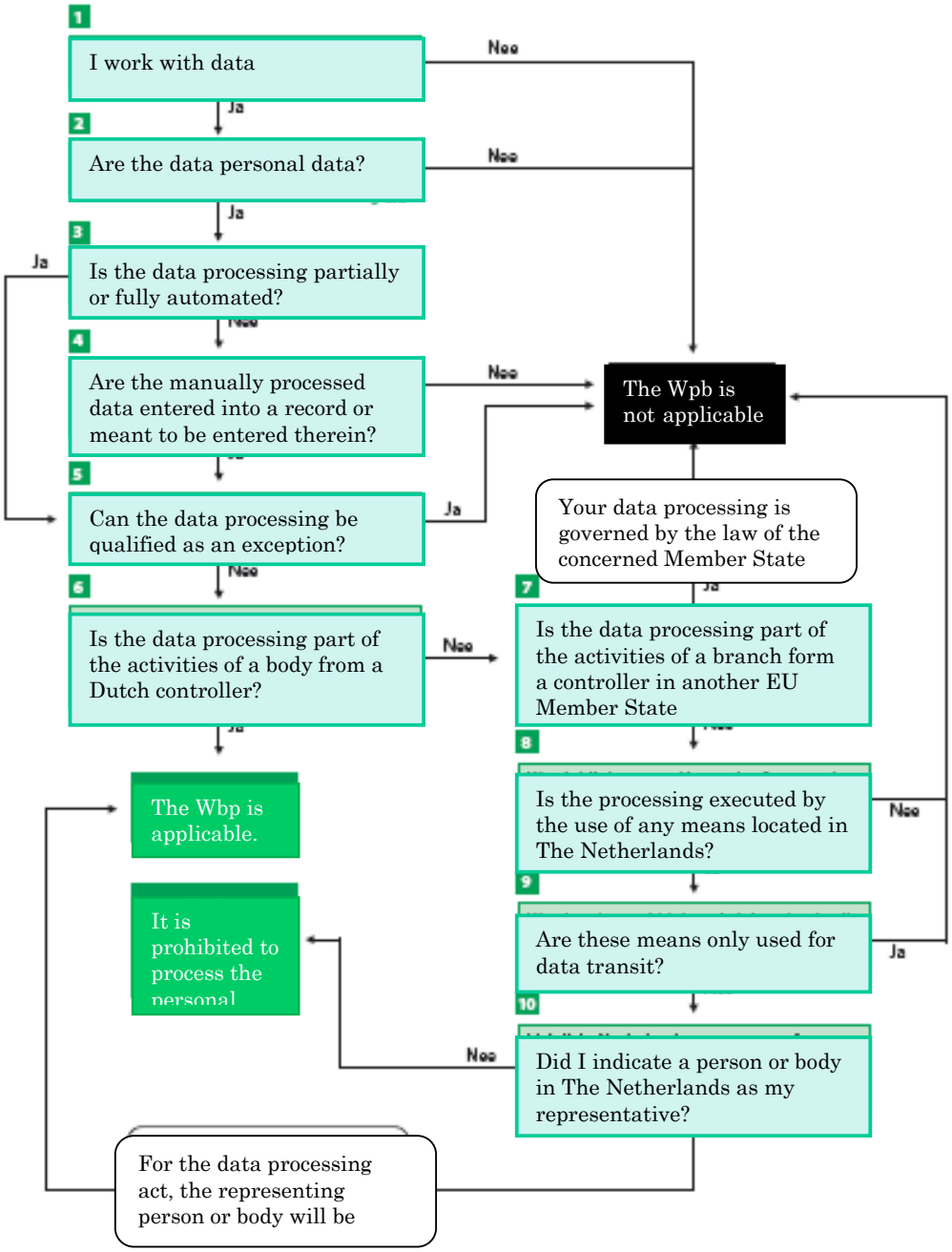
As is generally known, the applicability of the DPD and consequently the Wbp, fully depends on the notions "personal data" and "processing". Data concerning identified or identifiable natural persons are protected when processed wholly or partly by automated means and to the processing otherwise than by automatic means of personal data which form a part of a filing system or are intended to form part of a filing system[105]. Exceptions thereto are the processing of data for purely personal or household activities, the execution of a police assignment or the processing for purposes of journalism, art or literature[106].

Within Tas[3] one can assume that the Wbp is applicable, at least when the individual controller or the controller's establishment (whether simply a branch or a subsidiary with a legal personality) is located on the territory of The Netherlands.

This is because the applicability of the national data protection legislations is determined based on the territorialism principle. The means used for the data processing are thus not determining. When for example Dutch telephone or internet cables are used for transmitting data to a data processor established in Belgium, the Belgian law will be applicable.

[105] Art 1 Wbp
[106] Artt 2-3 Wbp

Scheme on applicability.



3.2.2 Lawful processing

As was already indicated above, three of the most important principles to the lawful processing of personal data are the restriction of the purpose, quality and transparency. Additionally the processing needs to be legitimate and proportional.

a) Restriction of the purpose

Before personal data can be collected or processed any other way, the purpose of the processing needs to be determined and delineated. It needs to be described in a clear and understandable way.

During the process alternations to the purposes are restricted. Article 9 Wbp determines five elements which should be taken into account when evaluating whether or not changes to the purpose are acceptable. Those five elements are:

- the connection between the goal of the data processing and the goal for which the data were gathered;
- the type of data collected;
- the consequences of the change of purpose for the data subject;
- the way in which the data were collected;
- the guarantees offered to the data subject;

Before starting to process personal data, determine and delineate the purpose for which you wish to use the data as clearly as possible. Take into account that within Tas³ it is not unlikely that different sets of data might be processed for different purposes. The purpose needs to be clear for each and one of the processing actions.

b) Legitimate ground

The data processing needs to be based upon a legitimate ground. For medical personal data this implies, the processing actions must fall under one of the exceptions on the general prohibition to process. In the Netherlands these exceptions are quite extensive. The Dutch Ministry opted for two sets of exceptions on the general prohibition to process medical data: on the one hand she determined a set of persons who are allowed to process medical data and on the other hand a set of situations can justify the processing.

Article 21 Wbp states firstly that personal health data can be processed by:

a. *medical professionals, healthcare institutions or facilities or social services, provided that this is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;*

b. insurance companies as referred to in article 1(1)(h) of the Insurance Supervision Act 1993 (Wet toezicht verzekeringsbedrijf 1993), insurance companies as referred to in Article 1(c) of the Funeral Insurance Supervision Act (Wet toezicht natura-uitvaartverzekeringsbedrijf), and intermediaries and sub-agents as referred to in article 1(b) and (c) of the Insurance Mediation Act (Wet assurantiebemiddelingsbedrijf), provided that this is necessary for:
1° assessing the risk to be insured by the insurance company and the data subject has not indicated any objection thereto, or
2° the performance of the insurance agreement;

c. schools, provided that this is necessary with a view to providing special support for pupils or making special arrangements in connection with their state of health;

d. institutions for probation, child protection or guardianship, provided that this is necessary for the performance of their legal duties;

e. Our Minister of Justice, provided that this is necessary in connection with the implementation of prison sentences or detention measures, or

f. administrative bodies, pension funds, employers or institutions working for them, provided that this is necessary for:
1°. the proper implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the state of health of the data subject, or
2°. the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity[107].

All of these exceptions are however under two conditions. Firstly the concerned person or institute should be subject to an obligation of confidentiality by virtue of office, profession or legal provision, or under an agreement. Where responsible parties personally process data and are not already subject to an obligation of confidentiality by virtue of office, profession or legal provision, they are required to treat the data as confidential, except where they are required by law or in connection with their duties to communicate such data to other parties who are authorized to process such data[108]. Secondly the data can only be processed when it is beneficial to good treatment or care of the patient / data subject or to the good management of the medical practice or healthcare institution[109]. With regards to data concerning inherited characteristics, a third condition finally applies: these data may only be processed with respect to the data subject himself, unless a serious medical interest prevails, or the processing is necessary for the purpose of scientific research or statistics.

Secondly article 23 provides that the processing of personal medical data is also allowed in case:

[107] Article 21, §1 Wbp.
[108] Article 21, §2 Wbp.
[109] J. Nouwt, Privacy en medische informatie, in J. Prins en J. Berkvens (eds.), *Privacyregulering in theorie en praktijk*, Kluwer, Deventer, 2002, 260-261.

a. *this is carried out with the express consent of the data subject;*

b. *the data have manifestly been made public by the data subject;*

c. *this is necessary for the establishment, exercise or defense of a right in law;*

d. *this is necessary to comply with an obligation of international public law, or*

e. *this is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy and this is provided for by law or else the Data Protection Commission has granted an exemption. When granting an exemption, the Commission can impose rules and restrictions. This will have to be reported to the European Commission.*

f. *this is necessary for the purpose of scientific research or statistics and under the conditions that:*
   - *the research serves a public interest,*
   - *the processing is necessary for the research or statistics concerned,*
   - *it appears to be impossible or would involve a disproportionate effort to ask for express consent, and*
   - *sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.*

For these – but also the exceptions from article 21 – the general principles as included above should always be taken into account.

The processing of personal health data is in principle forbidden. For the Tas³ health pilot it is advisable to base the processing on the express consent of the data subject/patient. Although a written consent is not explicitly required, it is advisable to obtain it anyway since it will be important in case of conflict and one needs to be able to provide evidence. When looking past the testing scenario and at a roll-out scenario, the legal ground will need to be reconsidered, depending on who might have access to the data and what purpose they will be used for, a consent might or might not be required.

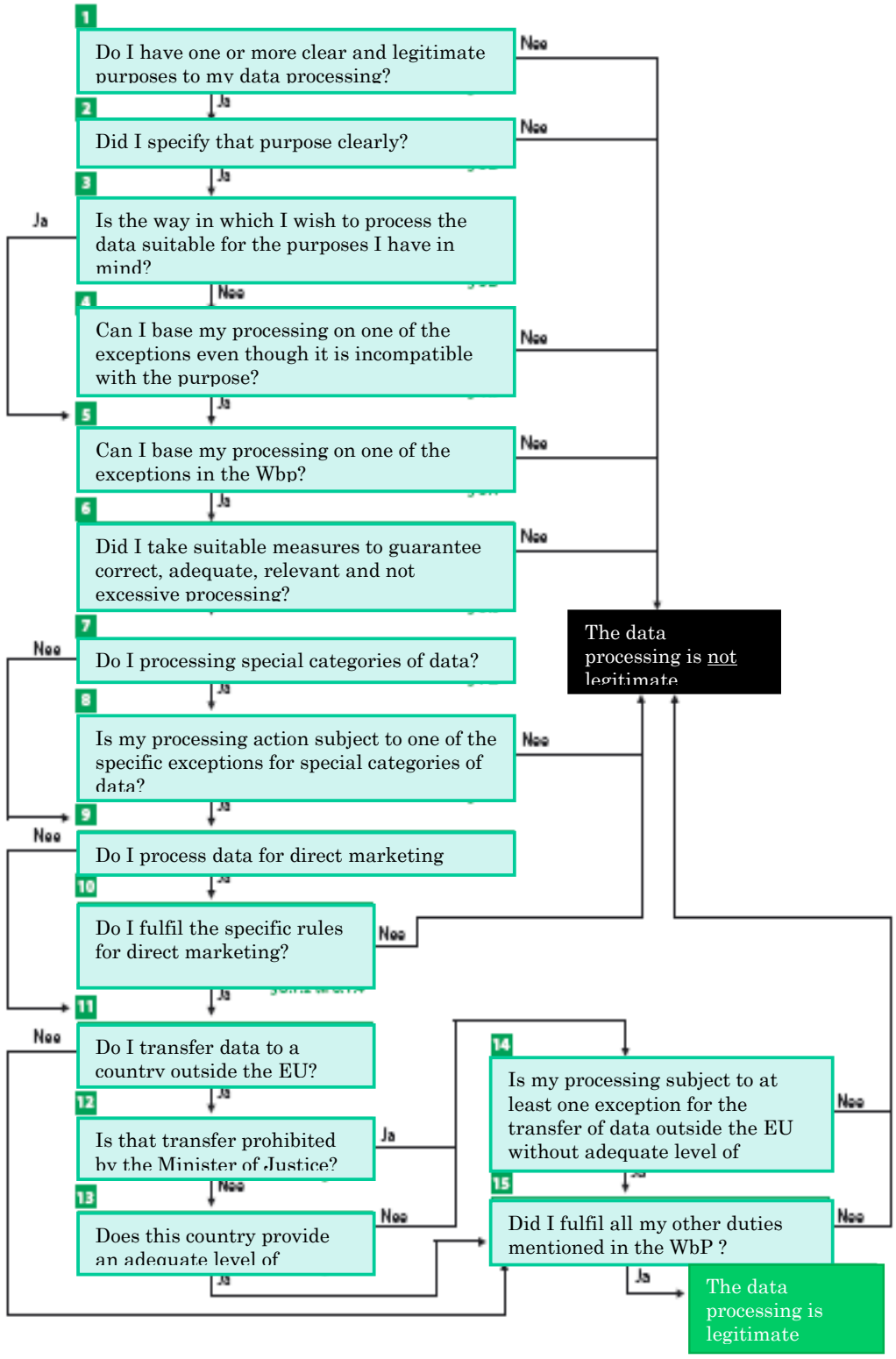
c) Adequate, relevant and not excessive

As is requested by the DPD, the Wbp requests that only adequate and relevant data should be processed. Excessive data should not be processed. This is the well known "need-to-know not nice-to-know" principle.

The Dutch Ministry of Justice clarifies that one should always question whether or not the same goal can be attained in an equally good way through the collection of less data or less personal data. This implies that the application of this criterion can differ on a case-by-case basis.

For each data processing action the Tas³ consortium will need to question whether or not the "need-to-know not nice-to-know" principle is respected.

Scheme on lawful processing.



3.2.3 Delineation of the roles

As has already been discussed in WP6, the DPD distincts the role of the data processor from the data controller. Within this annex we will not further elaborate on the ongoing European discussion on the interpretation of these concepts. However, we will highlight the Dutch view on this as it is very clear. We will furthermore reproduce the scheme on processor / controller from the Dutch government and reflect on the duties of the party / parties qualified as controller. The latter is important because the Wbp addresses primarily the controller. A third point of attention will be the role of the data protection officer ('functionaris voor gegevensbescherming') as this role is not known in all Member States.

a) Scheme on processor / controller

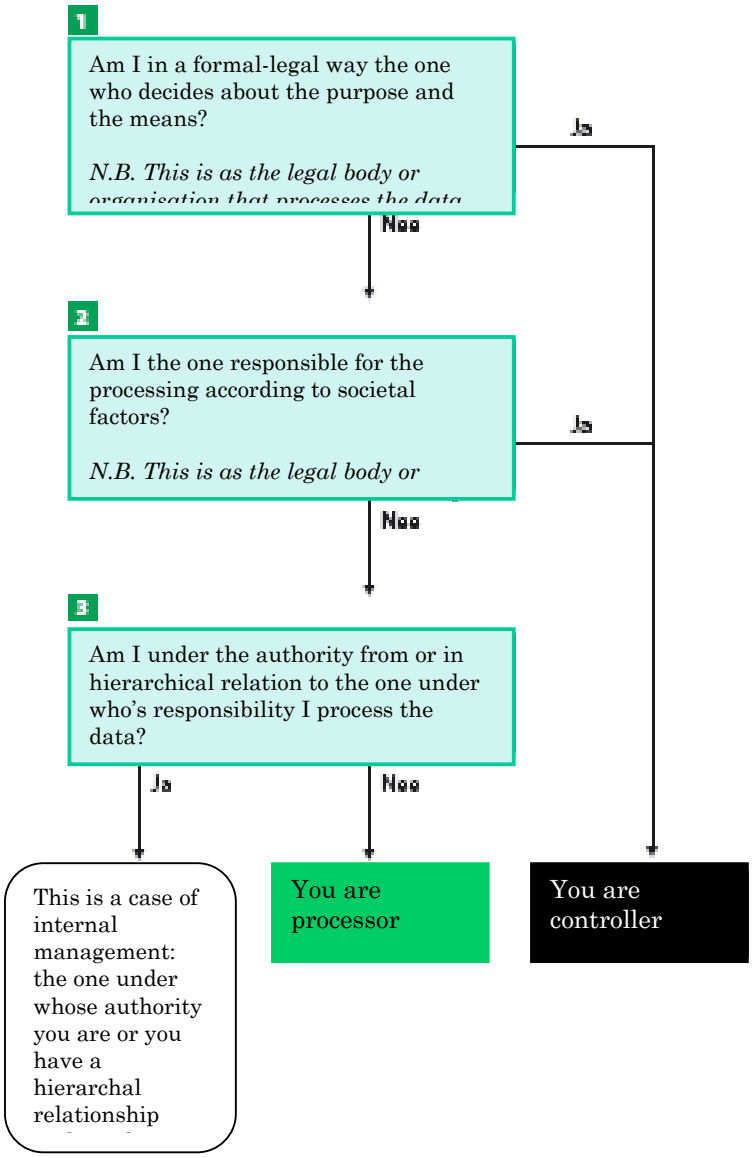
The Dutch explanatory statement accompanying the Wbp found three possible variations on the concept of controller[110]:

- Collective responsibility: there are several controllers, but each of them bares a more or less equal share of the responsibility for the whole data processing. This can for example be the case when several parties decide to develop a marketing database with combined efforts and for collective use.
- Differentiated responsibility: there are several controllers, but each of them has a more or less delineated and not overlapping responsibility for certain data processing actions. An example thereof could be the use of a common database but where the use is geographically separated. Another example could be a coming effort but with different responsible parties for different kinds of processing.
- Shared responsibility: there are several parties who entrust the data processing to a third party. This could be the case for medical information systems in hospitals for example. The hospital will be responsible for the whole, but the different external practitioners who make changes or add information can be regarded as responsible for that.

In this last case, discussion could arise on the question whether this is a controller-controller relationship or whether it is a controller-processor relationship. Within the Wbp fact that the controller has authority over the second party is considered the decisive criterion, as is also shown in the scheme below.

[110] J. Prins en J. Berkvens, 'De wet bescherming persoonsgegevens' in J. Prins en J. Bervens (eds), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, 86.

Scheme on processor / controller.



The Dutch view on the delineation of roles is quite clear and distinct. Three possible scenarios are considered:

Collective responsibility: several controllers with more or less equal share of the responsibility for the whole data processing;
Differentiated responsibility: several controllers with a more or less delineated and not overlapping responsibility for certain data processing actions;
Shared responsibility: several parties entrust the data processing to a third party.

The situation in which the Tas³ consortium finds itself will depend on the concrete approach to the health pilot. Within the setting of a project a collective responsibility seems most likely. In real life a collective responsibility seems – on the contrary - most unlikely given the amount of components for which different parties can be regarded responsible. Ultimately it will however depend on how partners wish to organize themselves.

b) Controllers' duties

In general, the controller needs to:

- Check the lawfulness of the data processing;
- Check if the data processing is lawful and adequate, relevant and non excessive;
- Check if the data processing needs to be notified;
- Secure the data processing;
- Make sure the data are stored no longer than necessary;
- Provide the data subject with information;
- Grant the data subject access when requested;
- Correct the data when requested;
- Terminate the data processing when the data subject objects;

b.1 Duty of confidentiality

In contrast to many other Member States, the Dutch Wbp explicitly states that offences against the duty of confidentiality imposed by the Wbp cannot be sanctioned through the Penal Code[111]. In practice this entails that the procedure will be different, this is civil instead of criminal and that the penalties determined in the Wpb are applicable.

b.2 Duty to implement appropriate technical and organizational measures

The Dutch Ministry chose not to concretize which measures exactly should be taken, but only determined that the technical and organizational measures should guarantee an appropriate level of protection, weighing the risks caused by the data processing and the level of sensitivity of the collected data against the state of the art and the costs of technical and organizational measures. They should moreover also aim to avoid the unnecessary collection or further

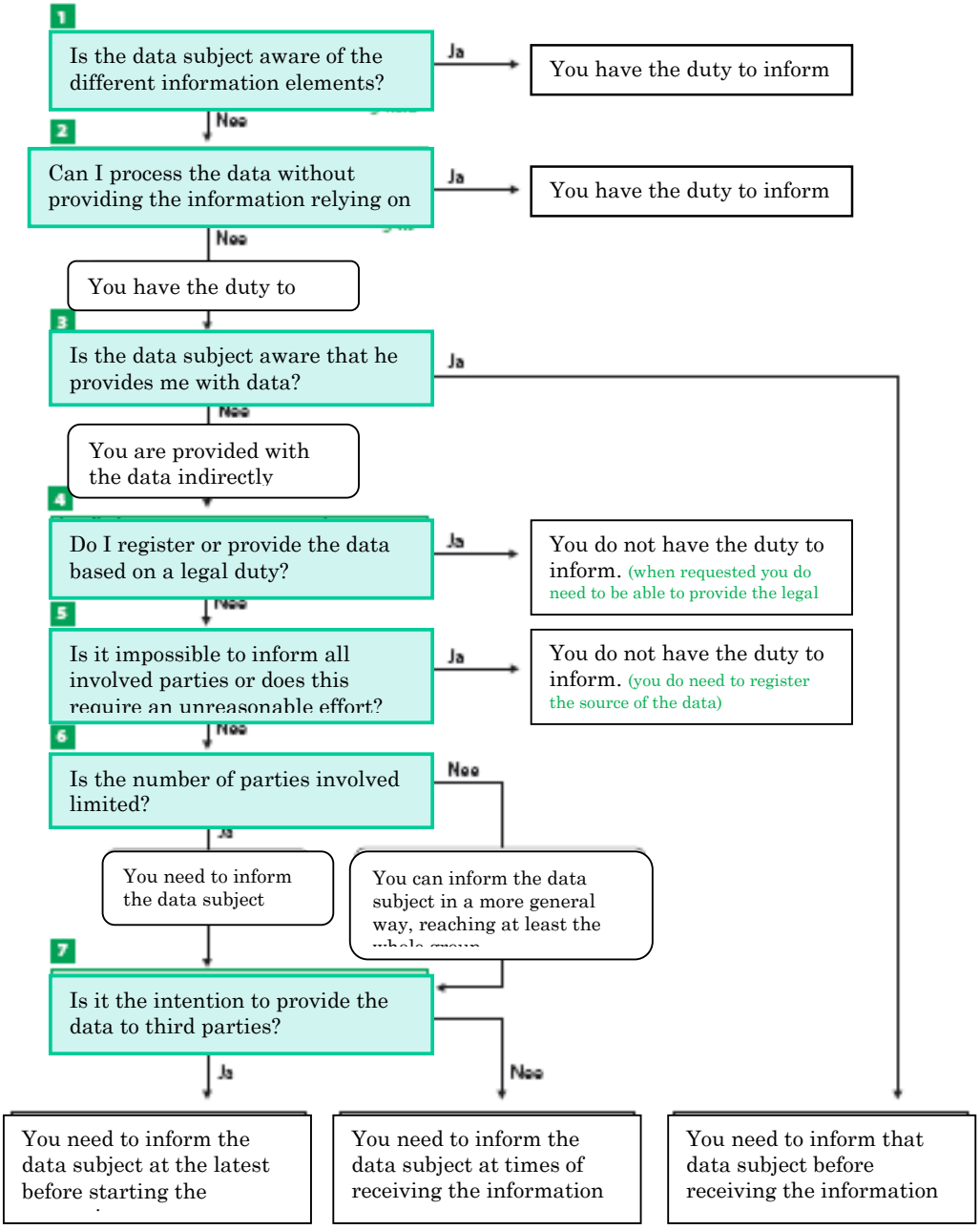
[111] Art 12 Wbp.

processing of personal data[112]. Finally the Ministry of Justice keeps a register of so called branch organizations ('bracheorganisaties') which developed security standards. It is advisable to also take those standards into account when processing data.

b.3 Duty to inform

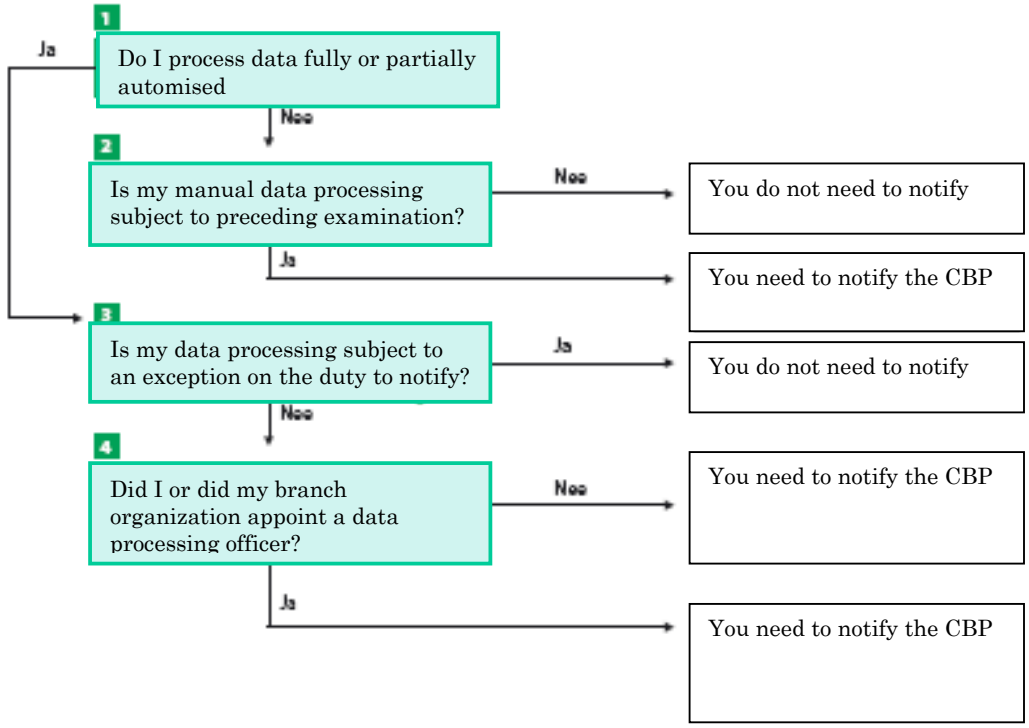
The controller has both an active as well as a passive duty to inform. Actively he needs to inform the data subject about his identity, the purposes of the processing and what the data will be used for. Additionally also all other information needs to be provided when this is necessary to guarantee a proper and careful data processing. The following scheme will help to get a better idea of the concrete duty to inform.

[112] Art 13 Wbp.


1
Is the data subject aware of the different information elements?
Ja
You have the duty to inform
Nee
2
Can I process the data without providing the information relying on
Ja
You have the duty to inform
Nee
You have the duty to
3
Is the data subject aware that he provides me with data?
Ja
Nee
You are provided with the data indirectly
4
Do I register or provide the data based on a legal duty?
Ja
You do not have the duty to inform. (when requested you do need to be able to provide the legal
Nee
5
Is it impossible to inform all involved parties or does this require an unreasonable effort?
Ja
You do not have the duty to inform. (you do need to register the source of the data)
Nee
6
Is the number of parties involved limited?
Nee
Ja
You need to inform the data subject
You can inform the data subject in a more general way, reaching at least the
7
Is it the intention to provide the data to third parties?
Ja
Nee
You need to inform the data subject at the latest before starting the
You need to inform the data subject at times of receiving the information
You need to inform that data subject before receiving the information

b.4 Duty to notify

In principle the Dutch Data Protection Officer – College voor de Bescherming van Persoonsgegevens – needs to be notified about every data processing before this is started. Exceptions can apply, but this will need to be judged on a case-by-case basis as the exemption is provided by order in council ('algemene maatregel van bestuur')[113]. One example of such an exemption is the processing of data by healthcare professionals in healthcare, nursing homes and childcare[114]. Again the following scheme can provide some guidance:



[113] Art 29 Wbp
[114] See Vrijstellingsbesluit.

Before working with real data the following basic elements should be checked thoroughly by all parties. This can be considered a check list.

- lawfulness;
- adequate, relevant and non excessive;
- notification;
- security;
- duration of the storage and timely destruction;
- information duties;
- access rights;
- possibility to correct data when requested;
- possibility to terminate the data processing after objection.

The party/parties that take up the role of controller can be held liable.

c) Data Processing Officer

The data processing officer is an internal supervisor, natural person, who can be appointed by the controller, a branch organization or other organization to which different controllers are connected[115].

c.1 Role of the data protection officer

The data protection officer is assigned different tasks and responsibilities in the Dutch Wbp, replacing to a certain extend the National Data Protection Commission. This way the officer becomes an intermediate between the CBP and the controller for the data processing.

The data protection officer first of all needs to supervise that the controller processes the personal data in accordance with the law. Consequently, data subjects can address themselves directly to the officer with questions or complaints concerning the processing of their data. Furthermore the officer is responsible for notifications and needs to register them. Consequently, when a data protection officer is appointed, it is no longer necessary to send the notification to the CBP.

The data protection officer needs to report to the CBP on a yearly basis.

c.2 Who can be appointed data protection officer and what is the procedure?

The role of the officer can, as was already mentioned, only be taken up by a natural person. He can be appointed by one controller or by an organization representing several controllers. The controller or the organization can freely choose, but they need to make sure the person appointed is properly qualified and reliable. He thus needs to be a privacy regulation expert and he needs to

[115] Artt 62-64 Wbp

have a certain amount of expertise on the data flows within the company, organization or branch. This is particularly important because he needs to be able to operate fully independently.

The data protection officer has to be provided with the same competences as the CBP would have in the case no officer was appointed. The appointment of an officer can be carried out at any moment in time, but it will need to be notified to the CBP.

The data processing officer is an internal supervisor, natural person, who can be appointed by the controller, a branch organization or other organization to which different controllers are connected. He is considered an intermediate between the controller and the CBP and takes over certain tasks from the CBP.

3.3 Data protection and the new EPD

The protection of personal data is marked as an essential precondition for the success of the EPD. The explanatory statement accompanying the current proposal of law, explicitly states that the Data protection legislation as discussed above and the Law on patients' rights as will be discussed below, are applicable to the EPD.

The current proposal of law on the EPD opted to allow the consultation of the EPD based on the consent of the patient, but the registration of patient data will become legally obliged. The consultation of the EPD will in other words be characterized by a right to opt-in, the registration of patient data and thus the creation of the EPD will however depend on the right to opt-out. The right to opt-out can be enforced for the whole EPD or parts of it. The Dutch legislator is convinced that the patient would be stronger empowered by allowing him to restrict the access rights than by allowing him to restrict the registration of data.

According to the latest updates on the proposal of law under discussion the EPD is characterized by a right to opt-out of the creation of the EPD and the duty to opt-in before consultation. It remains however to be seen how the final law will look.

4 Requirements concerning Patients' rights in the Netherlands

As indicated above, patients' rights are protected by the Medical Treatment Agreement Act, the Wgbo. The most important goal of this law is the reinforcement of the patient's position. In the report "From Law to Practice. Implementation of the Wgbo" Dutch healthcare organizations however indicated three topics as crucial pieces to attain this goal: a) information and consent, b) medical files and their storage and c) access to patient data[116]. Since these three topics are also of crucial importance to Tas[3], the elaboration below will follow that structure.

4.1 General Principles

The Dutch legislator chose to strengthen the patients' position through private law. The Wgbo is – as was already indicated above – part of the civil code and is to be seen as a general legal regulation of the rights and obligations of the patients, in addition to which criminal law will have a further role, whereas the standardization that the regulation contains will be important for the application of disciplinary stipulations.

Although the Wgbo is aimed to regulate the relationship of the patient with his carers, the scope of the law extends to the regulation of non-contractual but nevertheless similar relationships[117]. Consequently, the Wgbo will also apply to for example treatments of medical nature in contexts of legal regulations covering working conditions, social security and social facilities.

In the Netherlands the patient has the right to

- Free choice of healthcare practitioner and the right to change that choice;
- Quality of care
- Information
- Give or refuse consent
- A medical record
- Protection of the privacy and intimacy
- Representation in case of incompetence

The patient has the duty to

- Co-operate with the healthcare provider
- Pay the healthcare professional

[116] Samenwerkingsverband Implementatieprogramma Wgbo, J. Witmer en R. de Roode (eds.) "Implementatie van de Wgbo, van Wet naar Praktijk", Rooduijn, Utrecht, 2004.
[117] Art 7:464 Wgbo.

4.2 Information and consent

Article 448 Wgbo states that the healthcare professional must inform the patient in a clear and understandable way on his health condition and the foreseen treatment. The patient needs more specifically to be informed about: the kind and purpose of examinations or treatment, the expected consequences and risks of this for the health of the patient, other methods or treatments that could be considered, the status and prognosis of the patient's health. If requested this information has to be provided in writing. Only after being provided with this information the patient can lawfully be requested for his consent.

4.2.1 Right to information

Patients of the age of 12 and above have the right to be informed, patients of the age of 16 and above have the right to consent. Patients under this age have the right to be represented, in the first place by their parents[118].

The report "From Law to Practice. Implementation of the Wgbo" stresses that on the one hand the healthcare practitioner needs to act with great respect for not only the patient, but also their autonomy when providing the necessary information. This is crucial to gain and maintain the patient's confidence. The healthcare professional on the other hand needs to provided with a clear picture on what exactly he is expected to inform the patient about[119]. The latter can be an obstacle because the duty to inform is not an absolute duty, but regulated according to the principle of reasonable expectations. Dutch jurisprudence shows that the exact interpretation of the duty to inform depends on two elements: on in how far the practitioner's opinion is based on assumptions and on the estimated intellectual capabilities of the patient[120]. It thus seems that the quality of the given information is at least as important as the quantity.

Apart from the right to know, the patient also has the right not to know. This right is captured in article 449: "*when the patient indicates that he prefers not to be informed, the healthcare practitioner needs to respect this as far as the disadvantage to the patient does not overpower his interest*". Furthermore the healthcare practitioner too has the right not to inform the patient when in his professional opinion he is convinced that providing the information would cause serious harm to the patient. This is called the therapeutic exception. The healthcare practitioner should however not withhold information without consulting a colleague of his on the subject and he needs to consider informing another person than the patient[121].

---

[118] Art 450 Wgbo.
[119] Samenwerkingsverband Implementatieprogramma Wgbo, J. Witmer en R. de Roode (eds.) "Implementatie van de Wgbo, van Wet naar Praktijk", Rooduijn, Utrecht, 2004, 23.
[120] J. Legemaate, De Wgbo: van tekst naar toepassing, Bohn Safleu Van Lohgum, Houten, 1998, 29-30.
[121] Art 448, 3. Wgbo.

Finally it has to be noted that not only the patient, but also the healthcare practitioner has the right to be informed. The patient is obliged to inform the healthcare practitioner to its best abilities about all the elements that might be necessary for the proposed treatment. Although this is an active duty for the patient, he does need to be assisted in it by the practitioner. The latter must question the patient in an effective way and keep record of the questions asked. Even though the fact that a patient did not provide the practitioner with the requested information might be regarded an extenuating excuse, this legal provision seems to be rather of a symbolic nature.

4.2.2 Consent

The patient has the right to consent or to not consent. In the Netherlands consent is a prerequisite to treatment or examination. It is required for a) a contract for medical treatment, b) for the medical treatment itself and – even though this falls outside the scope of the Wgbo – c) for data processing[122]. However, an explicit consent is not always required.

As a general principle the Wgbo requires an explicit consent as justification of the doctor's intervention. This is required for all actions taken in the execution of the medical treatment. This implies that a consent is demanded for not only the contract of the treatment and the medical treatment itself, but also each and every medical action. When a medical action itself or its consequences are however not major, the doctor may presume consent has been granted. This can for example be the case for the taking of blood during an operation. Presumed consent can furthermore also be deducted from a person's behavior, but this should not be done too easily. If not, the practitioner risks to be accused of maltreatment[123].

Patients of the age of 12 and above have the right to consent or not consent and the right to know or not to know.

The healthcare professional needs to acquit oneself from his duty to inform in a way respecting the patient and his autonomy. The duty to inform is judged according to the reasonable expectations principle. The patient from his side is obliged to inform the healthcare professional to its best abilities about all the elements necessary for the proposed treatment.

In principle consent needs to be given explicitly for every medical action. Consent may however be presumed for minor interventions.

[122] 0

[123] SMART study for The Netherlands: National Profile of The Netherlands, available online: http://ec.europa.eu/information_society/activities/health/studies/published/index_en.htm, 2008, 29.

4.2.3 Information and consent in the EPD

In the current proposal of law on the EPD the use of the National Switch Point and the national EPD would become obligatory for the all healthcare practitioners. The practitioner will be obliged by law to adapt his information system to the requirements of the NSP and will be required to electronically register health data his patients, excepts when a patient explicitly opts-out from the national EPD.

As indicated above, the entails that every patient will get an EPD unless he expresses his wish to opt-out and that a consent will thus not be required from the patient for the creation of the EPD. The access to the EPD will be based on an opt-in.

It is the Dutch Ministry's intention to allow the patient to express their wish to opt-out or opt-in through the use of a consent server and the eID, but the implementation of eIDs is taking much more time than estimated, causing the service not to be in place yet[124].

4.3 The file and its storage

4.3.1 Obligation to the keep a patient file

In the Netherlands every healthcare practitioner is obliged to keep a patient file when treating a patient[125]. In the file the practitioner needs to include all data which are required for "good care" in the future. Which data are comprised exactly under "good care" can unfortunately not be formulated in a general way and need to be assessed on a case-by-case basis, keeping in mind the goal of the patient file, namely to improve the quality and continuity of care. This of course causes some confusion in practice. Therefore it is recommended to include in any case at least some basic information such as the diagnosis, the plan for treatment or planned examinations, evolution reports, reports about anesthesia and operations, laboratory results, referral and discharge letters and opinions of any consulted specialists. Additionally, all data which the patient requests to be included in the report should be registered by the healthcare practitioner[126]. The data need to be registered in a clear and organized way.

The personal notes of the healthcare professional do not have to be included in the patient file as long as they are intended to create his "own, provisionary line

[124] Voorstel van Wet tot Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg, tweede kamer, 2007-08, 31 466, nr.2; Memorie van toelichting bij het voorstel van wet, tweede kamer, 2007-08, nr.3 and Verslag van de expertenbijeenkomst over het elektronisch patiëntendossier van de vaste commissie voor volksgezondheid, welzijn en sport/jeugd en gezin, eerste kamer, 2009-10, 31 466, E, all available throuhg: http://www.minvws.nl/dossiers/elektronisch-patienten-dossier/kamerstukken/..

[125] Art 454, 1. Wgbo

[126] R. Doppegieter, "Vraagstukken rond het dossier en de uitwisseling van gegevens", in J. Legemaate (ed.) De Wgbo: van tekst naar toepassing, Bohn Stafleu Van Loghum, Houten, 1998, 75-76.

of reasoning". Such personal notes are of a temporary status and are not meant to be public to others. From the moment however the practitioner shares his personal notes with a third party – whether this is done orally or in writing – the notes lose their personal character[127]. Also in time, personal notes either need to be destroyed or need to be included in the patient file.

4.3.2 Storage period

Since a couple of years the data need to be stored – in general - for 15 years, starting from the registration of the data in the file[128]. This used to be 10 years, but that was considered too short, both for reasons of care and with view to scientific research. After 15 years the data need to be destroyed, unless the good care for the patient requires longer storage. Many exceptions to this term do however exist.

The main exception to this term is the case in which the healthcare practitioner considers longer storage necessary for "good care" of the patient. Examples thereof are chronic or recurrent treatments and GP care. In practice however, the criterion "good care" is experienced as very unclear. Additionally, the fact that the criterion is judged on a case-by-case basis, doesn't add to the legal certainty either[129].

Apart from this general exception, several other exceptions are laid down in specific laws. Sometimes requiring shorter terms such as the law on psychiatric care, which requires that patient data are stored for 5 years starting from the end of the stay; and sometimes requiring longer terms such as the law on archives, which requires that certain basic data are stored for 115 years starting from the date of birth of the patient.

4.3.3 On paper, digitalized or digital

In the Netherlands the practitioner can chose to register his files on paper or electronically. After switching to electronic files, he is also allowed to digitalize his paper files. It is furthermore accepted that paper patient files are destroyed after being digitalized as long as the files remain easily accessible and easy to consult. In this regard it is for example important to be aware of the life expectancy of the electronic data carrier. Of course the digitization may also not prevent the patient from enforcing his rights. There is finally one exception to this: when original files are extremely important it is advisable to continue to store the authentic, paper version too. An example thereof is a written living will[130].

---

[127] Knmg, Richtlijnen inzake het omgaan met medische gegevens, Januari 2010, 5; Kamerstukken Wgbo II, 1991-92, nr. 21 561, nr. 10, 22.
[128] Knmg, Richtlijnen inzake het omgaan met medische gegevens, Januari 2010, 7-9.
[129] Samenwerkingsverband Implementatieprogramma Wgbo, J. Witmer en R. de Roode (eds.) "Implementatie van de Wgbo, van Wet naar Praktijk", Rooduijn, Utrecht, 2004, 24.
[130] Knmg, Richtlijnen inzake het omgaan met medische gegevens, Januari 2010, 7.

All healthcare professionals are obliged to keep a patient file and store it for 15 years. The patient file needs to contain all data necessary for the future good care of the patient. This should help to improve the quality and continuity of the provided care. The file can be kept in electronic or paper form. For some formal documents it is however advisable to keep them on paper. 15 years after registration the data should be destroyed unless an exception justifies longer storage.

4.4 Rights with regards to patient data

4.4.1 Right to access

Article 456 Wgbo assigns the patient the right to direct access to and the right to a copy of his medical file, this is without intervention of a third party. Both rights are recognized as fundamental, meaning they can never be denied to a patient. As described above there are two exceptions on the basis of which the access to certain data (but never the whole file) can be denied:

- The healthcare practitioner does not give access to those data which could harm the privacy of another person and this has a paramount character[131];
- The healthcare practitioner can refuse access to certain data referring to his therapeutic exception, in other words when this would harm the patient[132].

4.4.2 Right to remove and destroy patient data

The right to have incorrect or irrelevant information removed is recognized by article 36 of the Wbp. Based on article 455 Wgbo the patient has furthermore the right to have data concerning himself destroyed: "the healthcare practitioner destroys the stored patient data, as explained in 454, within three months after the concerned request of the patient".

Both the removal and destruction of the data are subject to a formal request by the patient. It is recommended to the patient to make this request in writing and it is recommended to the healthcare practitioner to store the written request. The request always needs to be addressed to a particular practitioner and can only affect the data stored by that practitioner.

The request to destroy can concern certain data, but can also concern the complete patient file. In the latter case, the healthcare practitioner can offer the patient to hold on of the file himself, rather than destroying all the data. This is however no obligation for the practitioner.

There are three exceptions to the right to destroy:

- Another law can require a term during which data cannot be destroyed, which is for instance the case in the Law on Psychiatric care;
- Another patient can have a considerable interest in keeping the data, for example data concerning hereditary diseases;

[131] See article 7:457 Civil Code for a more detailed explenation.
[132] Knmg, Richtlijnen inzake het omgaan met medische gegevens, Januari 2010, 11.

- Good care is in manifest contradiction with the destruction of the data, which arises from the liability of the professional for providing care in accordance with the professional standard. This exception does however need to be interpreted in a very strict sense and the application thereof needs to be thoroughly motivated. A procedure before the 'complaints commission' is open to the patient.

The Dutch patient has the right to directly access the health data stored from him and the right to obtain a copy thereof. Both rights are considered fundamental, implying that exceptions will be interpreted restrictively.

4.4.3 Rights with regard to the EPD

a) Right to access

In accordance with article 456 Wgbo, the current proposal of law on the EPD states that the medical practitioner should provide a patient, upon request, as soon as possible with access to the EPD and present him with a printed copy thereof. The patient can – in principle – access the complete file. Just as is the case with regards to other paper of electronic files, exceptions can however be made when the access of the patient to the file would harm the privacy of third people or when the healthcare professional calls upon the therapeutic exception[133].

b) Right to delete and destroy

The rights to delete and destroy data too are adopted in the current proposal of law. It is stated that when a patient expresses the request to destroy certain data from one of his patient's files this should have immediate consequences for the through the EPD available data[134]. The deletion of data is however not yet technically implemented. Additionally discussion is ongoing on the question whether or not a remark should be made in the EPD, such as "incomplete EPD", after such a request has been expressed.

The Dutch patient furthermore has the right to have irrelevant or incorrect information removed and the right to have any data or files concerning himself destroyed. A formal request thereto is required, preferably in writing.

Three exceptions may apply to the right to have data destroyed. This right is outweighed by a legal obligation to store certain data, a considerable interest of a third person and a manifest contradiction with the principles of good care.

The interpretation of these rights will – as is currently accepted – not be any different with regards to the EPD.

[133] Article 13g in the current proposal of law on the EPD.
[134] Article 13e in the current proposal of law on the EPD.

5 Conclusion

When deploying the Tas³ health pilot account has to be taken of a number of legal principles and requirements. The protection of privacy, data protection and the protection of the pa'ients' rights are among the most important. Apart from those chunks of legislation several smaller pieces of regulation can also be of decisive importance, such as regulation of the healthcare professions, identity management in healthcare and regulation implementing new ICT-driven tools such as the EPD.

This annex described the legal framework for a Dutch eHealth pilot. The following recommendations can be deduced from it and should be taken into account at all times.

- The applicability of the Dutch regulatory framework is not always consistent. While the applicability of the Wbp depends on the establishment of the controller, the Wgbo is applicable to all medical treatments provided by a in the Netherlands registered natural person or medical legal body. Furthermore account has to be taken of specific legal regulations applicable to specific healthcare situations such as psychiatric care. The delineation of the field in which the developed application will be deployed is therefore an important exercise to make beforehand.

  Within the currently foreseen Tas³ Health Pilot, it can be assumed that the regulatory framework on data protection and patients' rights is applicable. No specific laws have been found applicable to the specific patient group of VOKS.

- In order to lawfully process data, a good amount of thought should first of all be put in defining and delineating the data processing purposes and what data exactly will need to be processed to attain the purpose. Based on that exercise, the consortium has to decide on what measures can be taken to assure the quality, transparency and security of the data processing.

- A second but similar exercise should be carried out on the delineation of the roles within the Pilot. Three options are possible under Dutch law: collective responsibility, differentiated responsibility and shared responsibility. For the Tas³ Health Pilot a collective responsibility seems most likely, but other options are open and ultimately this will have to be agreed amongst the partners.

- Within the Tas³ pilot, the processing of health data will have to be based in the informed consent of participating patients, but also healthcare professionals. A written consent is not formally required, but nevertheless advisable.

- It will have to be checked whether a data processing officer is appointed within the specific branch of the pilot.

- Patients from the age of 12 and above have the right be informed or to not be informed. Particularly the right not to know will have to be respected, also with regard to electronically share data.

- Furthermore it is of crucial importance to realize that patients also have the right to decide about the access rights to their files. Not only can they request to access the data on them themselves, they can also refuse access to certain healthcare practitioners for the whole file or for certain data. This principle in also acknowledged by the proposal of law on the EPD, as it is foreseen that consultation of the patient file will only be possible after consent of the patient.

- All Dutch healthcare practitioners are obliged to keep a patient file. They are however not yet obliged to share this file. Currently it looks like this will change once the proposal of law on the EPD gets approved.

- Last but not least the patient's will to remove or destroy his data or his file(s) needs to be honoured by the healthcare practitioners, unless one of the three exceptions thereto applies. The right to destroy data is outweighed by a legal obligation to store certain data, a considerable interest of a third person and a manifest contradiction with the principles of good care. If however none of the exception applies, the healthcare practitioner is obliged to comply with a patient's formal request. This will not be any different with regards to electronic files, on the contrary.

8.6 Annex 6 - Privacy update 2009

This addendum provides an update on developments which took place in 2009, in particular in the field of privacy and data protection, which may prove to be relevant to the further development and later deployment of TAS³. In order to fulfil its objective, TAS³ needs to keep abreast of the evolution of legal requirements, emerging regulatory trends and evolving best practices. This addendum is provided to that end. It is provided as a separate addendum to highlight these evolving requirements, trends and practices which shall potentially impact the regulatory framework for TAS³. As the implications of these developments become clearer and we evaluate their specific impacts on the project, content of this addendum will be incorporated into D6.1 and D6.2 and other documents that articulate project requirements, as appropriate.

1. Lisbon Treaty

The competences at the EU level had previously been divided among three pillars. These pillars specified competencies to act based on subject matter, allocating priority of action between Member States and EU institutions. With the Advent of the Lisbon Treaty the Pillars have been merged to develop a "unified personality".

With the Lisbon Treaty the distribution of competences among Member States and the European Union in the various policy areas have been divided as follows:

Exclusive competence	Shared competence	Supporting competence
The Union has exclusive competence to make directives and conclude international agreements when provided for in a Union legislative act.	Member States cannot exercise competence in areas where the Union has done so.	The Union can carry out actions to support, coordinate or supplement Member States' actions.
• the customs union • the establishing of the competition rules necessary for the functioning of the internal market • monetary policy for the Member States whose currency is the euro • the conservation of marine biological	• the internal market • social policy, for the aspects defined in this Treaty • economic, social and territorial cohesion • agriculture and fisheries, excluding the conservation of marine biological resources	• the protection and improvement of human health • industry • culture • tourism • education, youth, sport and vocational training • civil protection (disaster prevention) • administrative

resources under the common fisheries policy • common commercial (trade) policy	• environment • consumer protection • transport • trans-European networks • energy • the area of freedom, security and justice • common safety concerns in public health matters, for the aspects defined in this Treaty	cooperation

[135]

While it is unlikely that the Lisbon Treaty will directly impact the further development of TAS[3] during the next year, it may well impact the revision of the EU Directive (of which the review is currently ongoing). Lisbon in combination with changes in leadership in the various DGs may also impact the development of sectoral requirements in the health and employment areas. Thus, while not creating direct or immediate impacts for TAS3, these developments are worth following.

2. EU Directive 95/46 Consultation and Review

Art. 33 of Directive 95/46 mandates the European Commission to submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society. In May of this year, the Commission organized a conference as part of its open consultation on how the fundamental right to protection of personal data can be further developed and effectively respected, in particular in the area of freedom, justice and security. Since then a formal consultation process has been launched which remains open until the end of the year. The objectives of the consultation are: *'to obtain views on the new challenges for personal data protection in order to maintain an effective and comprehensive legal framework to protect individual's personal data within the EU'*.[136] This initial Consultation exists at a very high level and consists of three questions:

- Please give us your views on the new challenges for personal data protection, in particular in the light of new technologies and globalisation
- In your views, the current legal framework meets these challenges?

[135] http://en.wikipedia.org/wiki/Three_pillars_of_the_European_Union

[136] Consultation on the legal framework for the fundamental right to protection of personal data; http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm.

- What future action would be needed to address the identified challenges?[137]

Replies to the consultation will be posted online. The Consultation represents the beginning of the review of Directive 95/46/EC. There is no specific end-date to this review with many suggesting that the process of review may potentially be a 2-3 year process.

The review of Directive 95/46 coincides with other important reviews. The OECD Privacy Guidelines[138] which predated and influenced the Directive, are also being reviewed pursuant to a mandate from the OECD 2008 Seoul Ministerial.[139] This review will focus on current implementation and applicability to new technologies and business models.

Also under review are the OECD Guidelines for Consumer protection in the Context of Electronic Commerce[140]. These guidelines have relevance to TAS[3] because they review the rights of the consumer in electronic transactions. At a recent conference of the topic hosted by the Federal Trade Commission in the US, significant discussions were had about consumer implications of new technologies and business models, both in general and in relation to specific sectors. Developments in the Guidelines review could inform us of evolving consumer rights as well as effective notice, transparency, and inclusion practices.

3. The 31st International Conference of Data Protection Commissioners

Each year the worlds Data Protection Commissioners meet, discuss the state of data protection, provide direction related to various topics and issue recommendations and declarations. This year, Spain hosted the Conference from November 4-6, during which a number of important issues were highlighted and a number of resolutions/declarations were adopted.

The most relevant development which took place during this Conference was the adoption of a proposal for a global policy standard.[141] The standard is not a technical standard, but rather a reference policy model that blends elements of the OECD Guidelines, the Council of Europe Treaty, the EU Directive and the APEC privacy principles. Relevant sections of the Resolution are quoted below:

> The Conference considers the following:
>
> - The rights to data protection and privacy are fundamental rights of every individual irrespective of his nationality or residence.
> - With the expansion of the information society, the rights to data protection and privacy are essential conditions in a democratic society to safeguard the respect for the rights of individuals, a free flow of information and an open market economy
> - The globalisation of information exchange and personal data processing, the complexity of systems, the potential harms derived from the misuse of more and

[137] Ibid.
[138] OECD Guidelines on the Protection of Privacy and Transborder Data Flows, OECD, 1980; http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[139] Seoul Declaration for the Future of the Internet Economy, available at www.oecd.org/dataoecd/49/28/40839436.pdf
[140] http://www.oecd.org/dataoecd/18/13/34023235.pdf
[141] http://www.privacyconference2009.org/dpas_space/Resolucion/index-iden-idphp.php

more powerful technologies and the increase of security measures require a quick and adequate answer to guarantee the respect for rights and fundamental freedoms, and in particular the right to privacy.

- The persisting data protection and privacy disparities in the world, in particular due to the fact that many states have not yet passed adequate laws, harm the exchange of personal information and the implementation of effective global data protection.
- The development of cross-border rules that guarantee in a uniform way the respect for data protection and privacy has priority.
- The recognition of these rights requires the adoption of a universal legally binding instrument establishing, drawing on and complementing the common data protection and privacy principles laid down in several existing instruments and strengthening the international cooperation between data protection authorities.
- The implementation of the guidelines developed by organisations such as APEC or the OECD, especially regarding the adoption of international frameworks with the aim of improving the respect of the rights for data protection and privacy on the crossborder data flows, is a positive step for reaching this objective.
- The accession to binding instruments of universal value, such as the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data (ETS No 108) and its additional Protocol regarding supervisory authorities and transborder data flows (ETS N° 181), which contain basic principles of data protection, are likely to facilitate the exchange of data between parties as they provide mechanisms and a platform for co-operation between data protection authorities, envisage their establishment exercising their functions in complete independence and promote the implementation of an adequate level of data protection;.
- The 30th International Conference of Data Protection and Privacy Commissioners is an appropriate forum to adopt a strategy specifically aimed at reaching these objectives.

Consequently, **the Conference repeats its appeal** to elaborate a universal legally binding instrument on data protection and privacy, **by adopting the following resolutions:** .

- The Conference supports the efforts that the Council of Europe is making to improve the fundamental rights to data protection and privacy. Therefore the Conference invites the member-states of this organisation which have not yet ratified the Convention for the protection of individuals with regard to automatic processing of personal data and to its additional protocol to do so. The Conference invites nonmember states in a position to do so to consider responding to the Council of Europe's invitation to accede to Convention STE N° 108 and its additional protocol. Taking into account its resolution concerning the Establishment of a Steering Group on Representation at Meetings of International Organisation, the Conference is also willing to contribute to the work of the consultative committee of the Convention ETS N° 108.4
- The Conference supports action taken within APEC, OECD and other regional and international fora to develop effective means to promote better international standards of privacy and data protection.
- **The Conference mandates** the establishment of a working group, co-ordinated by the organising authority of the 31st international conference and composed of the interested data protection authorities, to draft and submit to its closed session a **Joint proposal for setting international standards on privacy and personal data protection** , according to the following criteria.
- To draw on the principles and rights related to the protection of personal data in the different geographic environments of the world, with particular reference to legal and other texts that have attracted a wide degree of consensus in regional and international forums

- To elaborate a set of principles and rights which, while reflecting and complementing existing texts, aim to achieve the maximum degree of international acceptance ensuring a high level of protection..
- To assess the sectors in which these principles and rights are applicable, including alternatives focused on harmonizing their scopes of application.
- To define, taking into account the diverse legal systems, the basic criteria that guarantee their effective application..
- To examine the role to be played by self-regulation.
- To formulate the essential guarantees for better and flexible international transfers of data. [142]

The process of drafting this joint proposal should be carried out by encouraging extensive participation in the working groups, fora or hearings, of public and private organisations and entities, with the purpose of obtaining the broadest institutional and social consensus. Particular attention should be paid to the ongoing work of the International Organization for Standardization (ISO) and of the International Law Commission.

The importance of the Resolution for the purposes of TAS³ is threefold:

- The Resolution was adopted by all of the DPA's and as such it may have impact in the review of the Directive. This could lead to increased prominence for the concept of accountability within the European legal frawork.

.

- The Resolution explicitly references the work of ISO in the field of privacy (which currently includes the development of a privacy framework a privacy capability maturity model as well as a privacy reference architecture). The ISO work as it progresses may impact some of the design criteria for TAS³. A more detailed overview of the work going on with in ISO/IEC JTC 1 SC 27/WG 5 will be provided in the next section.

- Lastly, the Resolution attempts to articulate the broadly and internationally accepted principles of privacy. While we must assure compliance with the laws in force- both at the EU and national level, these principles may form the basis for future compacts related to international transfers. As global data flows become both more prevalent and integrated into business models we must consider the distinct possibility that data flows related to heath or employment portfolios in the EU may include processing or other functions in countries outside of the EU. These transfers must be considered in light of the local legal and policy frameworks. The principles contained in the resolution may form the basis for qualified findings of adequacy or the basis of contractual bindings of accountability. Again more of an issue to watch than a certainty for now.

[142] http://www.privacyconference2009.org/privacyconf2009/dpas_space/index-iden-idweb.html

4. ISO/IEC JTC 1 SC 27/WG 5 standardization efforts in the field of privacy and data protection

ISO/IEC JTC 1 SC 27/WG 5 is currently developing several standards which are closely related to the work being carried out in TAS³. Relevant standards include:

- A framework for identity management (24760);
- Entity authentication assurance (29115 | X.eaa);
- A framework for access management (29146);
- Privacy framework (29100);
- Privacy reference architecture (29101);
- Privacy capability maturity model (29190).

The main objective of the Privacy framework (29100) is to establish a set of common privacy principles, concepts and terminology. This framework is being developed to enable the definition of privacy control requirements in subsequent standards. At the moment of this writing, there are two additional work items which build on 29100, namely the Privacy reference architecture (29101) and the Privacy capability maturity model (29190). 29100 has reached the level of 'Committee Draft', and thus displays a relatively high level of maturity. The two other work items (29101 and 29190) are still in an earlier stage of development ('Working Draft'), but are nevertheless of great interest.

TAS³ obtained the status as a Category C Liaison in September of 2009. Our main purpose is to assist in the progression of work items relating both to privacy as well as those in the areas of identity and information security management.

5. Privacy by Design.

Privacy by design is a concept dating back to at least the 1990's when it was espoused by Ann Cavoukian, the Information Commissioner for Ontario. The day before this year's Data Protection Commissioner's Conference, Commissioner Cavoukian assembled experts in the field of Privacy by Design as part of the "Definitive privacy by design conference". Privacy by Design was also strongly reflected in a number of presentations at the Data Protection Commissioners conference, and in the agendas of parallel meetings created by the International Association of Privacy Professionals and the civil society groups organized by the Electronic Privacy Information Center.

Privacy by design is not a new concept. However, it is currently being reconsidered in a more holistic fashion; to go beyond just design of privacy functionality in technology at the development stage and to include designing privacy into related policies and processes. This evolving approach is very consistent with the approach taken in TAS³ of considering privacy from the outset in technology, policies (both written and technical sticky policies) and legal frameworks.

Commissioner Cavoukian has developed seven 'foundational principles' of privacy by design[143] which serve as useful guideposts for TAS3 development:

[143] A. Cavoukian, 'Privacy by Design – The 7 Foundational Principles', August 2009, available at http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

Privacy by Design now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive information such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.
The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

1. *Proactive* not Reactive; *Preventative* not Remedial
The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. *PbD* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the *Default*
We can all be certain of one thing – the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, *by default.*

3. Privacy *Embedded* into Design
Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum
Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.

5. End-to-End Lifecycle Protection
Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency
Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy
Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

The elements of privacy by design form a useful checklist that helps to validate the TAS³ technical development objectives As we review the principles advanced by the Information Commissioner for Ontario for Privacy by Design, we find that TAS³ has been fairly successful in considering these concepts in the development of the technical architecture. But some concepts of privacy by design such as end-to-end lifecycle protection and visibility/transparency cannot be realized through technology alone. These two elements have significant policy and process components, which must also be reflected in the TAS³ governance model.

6. Galway Project (2009) / Paris Project 2010

The Galway project on accountability concluded the first phase of its work with a paper entitled 'Data Protection Accountability: The Essential Elements'[144]. This paper attempts to outline the essential elements of an "accountable organization". In many ways these essential elements of accountability are in line with TAS3 concepts of the issues that service provider practices need to address. As such they form a good checklist for TAS³ participants to use in reviewing their capacity to be an accountable organization[145]

Essential Elements of Accountability
An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies. The essential elements articulate the conditions that must exist in order that an organisation establish, demonstrate and test its accountability. It is against these elements that an organisation's accountability is measured.

The essential elements are:

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

[144] Data Protection Accountability: The Essential Elements, A Document for Discussion, October 2009 http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf
[145] An extract of these elements is provided in checklist form with commentary on how it is relevant to TAS³ in D6.2 at section 8.2

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

Many global organisations have established policies in accordance with accepted external criteria such as the EU Directive, OECD Guidelines or APEC Principles. These companies demonstrate high-level commitment to those policies and the internal practices that implement them by requiring their review and endorsement by members of the organisation's executive committee or board of directors.

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

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

Organisations in Europe, North America and Asia-Pacific have implemented comprehensive privacy programmes that incorporate personnel training, privacy impact assessments and oversight. In some cases, organisations have automated processes and integrated responsibility for programme obligations into all levels and across all aspects of the enterprise, while responsibility for compliance, policy development and oversight remains in the privacy office.

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

Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. Accountable organisations establish these performance-monitoring systems based on their own business cultures. Performance systems evaluate an organisation's decisions about data across the data life cycle — from its collection, to its use for a particular application, to its transmission across

borders, to its destruction when it is no longer useful — and must be subject to some form of monitoring.

The organisation should establish programmes to ensure that the mechanisms are used appropriately as employees make decisions about the management of information, system security and movement of data throughout the organisation and to outside vendors and independent third parties. The organisation should also periodically engage or be engaged by the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability. Where appropriate, the organisation can enlist the services of its internal audit department to perform this function so long as the auditors report to an entity independent of the organisation being audited. Such verification could also include assessments by privacy enforcement or third-party accountability agents. The results of such assessments and any risks that might be discovered can be reported to the appropriate entity within the organisation that would take responsibility for their resolution. External verification must be both trustworthy and affordable. Privacy officers may work with their audit departments to ensure that internal audits are among the tools available to oversee the organisation's data management. Organisations may also engage firms to conduct formal external audits. Seal programmes in Europe, North America and Asia-Pacific also provide external oversight by making assurance and verification reviews a requirement for participating organisations.

4. Transparency and mechanisms for individual participation.

To facilitate individual participation, the organisation's procedures must be transparent. Articulation of the organisation's information procedures and protections in a posted privacy notice remains key to individual engagement. The accountable organisation develops a strategy for prominently communicating to individuals the most important information. Successful communications provide sufficient transparency such that the individual understands an organisation's data practices as he or she requires. The accountable organisation may promote transparency through privacy notices, icons, videos and other mechanisms.

When appropriate, the information in the privacy notice can form the basis for the consumer's consent or choice. While the accountability approach anticipates situations in which consent and choice may not be possible, it also provides for those instances when it is feasible. In such cases it should be made available to the consumer and should form the basis for the organisation's decisions about data use.

Individuals should have the ability to see the data or types of data that the organisation collects, to stop the collection and use of that data in cases when it may be inappropriate, and to correct it when it is inaccurate. There may be some circumstances, however, in which sound public policy reasons limit that disclosure.

5. Means for remediation and external enforcement.

The organisation should establish a privacy policy that includes a means to address harm to individuals caused by failure of internal policies and practices. When harm occurs due to a failure of an organisation's privacy

> *practices or to a lapse in its compliance with its internal policies, individuals should have access to a recourse mechanism. In the first instance, the organisation should identify an individual to serve as the first point of contact for resolution of disputes and establish a process by which those complaints are reviewed and addressed.*
>
> *The accountable organisation may also wish to engage the services of an outside remediation service to assist in addressing and resolving consumer complaints. Third-party agents, including seal programmes and dispute resolution services, can facilitate the consumer's interaction with the organisation and enhance its reputation for complying with its policies and meeting its obligations to individuals.*
>
> *Accountability practices should be subject to the legal actions of the entity or agency with the appropriate enforcement authority. Ultimate oversight of the accountable organisation should rest with the appropriate local legal authority. The nature of that authority may vary across jurisdictions. However, it is critical that the accountable organisation recognise and respond to the legal authority exercising proper jurisdiction.*

The evolving work on standards, accountability and privacy by design are beginning to coalesce into a new dynamic of compliance requirements and leading privacy practices. There is recognition that information is becoming more ubiquitous and that some information that is in circulation is beyond the current control structures of notice and consent. Use-based models are likely to play an important role in controlling misuse of information given the proliferation and publication of information across various sources. The coalescence of these factors was reflected in comments of both Peter Hustinx, the EU Data protection supervisor and Martin Abrams, the Executive Directive for the Centre for Information Policy Leadership.

> *On Monday, November 2, Peter Hustinx, European Data Protection Supervisor, said accountability would figure prominently in the joint initiative to develop global standards led by the Spanish Data Protection Agency. Hustinx, speaking at the Privacy-By-Design preconference to the 31st International Conference of Data Protection and Privacy Commissioners in Madrid, said that organizations will have to demonstrate they are accountable. Martin Abrams, Senior Policy Advisor and Executive Director, Centre for Information Policy Leadership at Hunton & Williams, commented that an accountable organization is responsible for understanding and mitigating the risks to individuals related the organization's collection and use of information, and is answerable to regulators and individuals for the effectiveness of its processes. Abrams further said that accountable organizations must demonstrate both the willingness and capacity to be accountable, and that privacy-by-design is an excellent road map for creating the mechanisms to demonstrate capacity.*[146]

[146] Hunton and Williams Privacy and Information Security Law Blog; November 5, 2009, http://www.huntonprivacyblog.com/2009/11/articles/european-union-1/centre-releases-galway-accountability-paper-approach-discussed-at-data-protection-commissioners-conference-in-madrid/

The Galway Accountability Project which was overseen by the Irish Data Protection Commissioner in 2009 will continue in 2010 under the auspices of the CNIL (French Data Protection Authority). TAS³ will continue to track these developments to help assure that our project continues to complement leading work in these areas.

7. Development of first EC Privacy Impact Assessment (PIA)

An important tool which assists both appropriate design and implementation of privacy protecting measures is the Privacy Impact Assessment (PIA). PIAs are most commonly referenced in parts of the Anglophone world; they are common in the US, Canada, Australia, New Zealand and are used increasingly in the UK and Ireland. Within the context of the EU there have been companies that are early adopters of PIAs, but fewer governmental entities have used them as such. There are however risk based assessments of privacy that occur as a result of Article 20 of Directive 95/46/EC which provides for the ability of authorities to engage in "Prior Checking" to determine if "… the processing operations [are] likely to present specific risks to the rights and freedoms of data subjects" in advance of the inception of the processing operations.
David Flaherty, former Data Protection Commissioner for British Columbia described the PIA as follows in a speech at the 22nd Data Protection Commissioners Conference in Venice in 2000[147]

> *What I intend to draw to your attention is an additional tool in the arsenal of the data protector in the form of **privacy impact assessments.** The idea is to require the preparation of **privacy impact assessments** for new products, practices, databases, and delivery systems involving personal information. In the last five years, privacy specialists have developed an assessment model for the application of a new technology or the introduction of a new service, which has good potential for raising **privacy alarms** at an early stage in an organization's planning process in either the public or private sectors. Various models exist for privacy impact assessments that can be customized to the needs of any organization. The essential goal is to describe personal data flows as fully as possible so as to understand what impact the innovation or modification may have on the personal privacy of employees or customers and how fair information practices may be complied with. **Ultimately, a privacy impact assessment is a risk assessment tool for decision-makers that can address not only the legal, but the moral and ethical, issues posed by whatever is being proposed.***
>
> *What I am proposing, and it will not be a novel suggestion for those of you from North America and New Zealand in particular, is that privacy regulators require, or at least encourage, those being regulated to prepare a privacy impact assessment for significant personal data systems that are new or enhanced in some significant way, so that their privacy implications can be analyzed and addressed in a coherent manner.*

[147] A presentation to a plenary session on "New Technologies, Security and Freedom," at the 22nd Annual Meeting of Privacy and Data Protection Officials held in Venice, September 27-30, 2000, Revised October 12, 2000. available at http://aspe.hhs.gov/datacncl/flaherty.htm.

A 2007 report[148] found that adoption of PIAs in the EU was still lagging:

> *As such, the development of PIAs in the Member States is at a relatively early stage. While there is interest in the concept of PIAs and the role that they could play within national data protection regimes and in privacy protection more widely, there are currently no completed tools, and there are limited legislative or policy frameworks in place to support their use. In most Member States it appears that the scope of 'prior checking' and similar functions in national legislation would not extend to justifying the broad introduction of PIAs, particularly as a compulsory requirement. As such, it is likely that where Member States' supervisory agencies wish to see PIAs adopted as part of their national data protection regime, this will develop out of persuading public and private sectors to adopt PIAs as an issue of policy rather than via legislation. In the public sector, the desire for accountability, efficient management and effective incorporation of Threat/Risk Assessments into key decision-making processes should aid in uptake. The fact that major European corporations such as Philips, Vodafone and others have adopted such strategies, and that these are seen as potentially conferring competitive advantage, may mean that at least some parts of the private sector will also be open to such developments*

Currently the EC is working on a model PIA for RFID based systems pursuant to its Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification issued in May of this year[149]. This Recommendation stipulates that[150]:

> *5. Member States should ensure that operators, notwithstanding their other obligations pursuant to Directive 95/46/EC:*
>
> *(a) conduct an assessment of the implications of the application implementation for the protection of personal data and privacy, including whether the application could be used to monitor an individual. The level of detail of the assessment should be appropriate to the privacy risks possibly associated with the application;*
> *(b) take appropriate technical and organisational measures to ensure the protection of personal data and privacy;*
> *(c) designate a person or group of persons responsible for reviewing the assessments and the continued appropriateness of the technical and organisational measures to ensure the protection of personal data and privacy;*
> *…*

The EC has created an expert group to develop this Model PIA. The work of this group should be informative as a PIA is one of the tools that TAS3 can use to

---

[148] Andrew Charlesworth, 'Privacy Impact Assessments: International Study of their Application and Effects - Appendix H', Bristol University Law School,. October, 2007, p. 12, available at http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/lbrouni_piastudy_apph_eur_2910071.pdf

[149] Commission of the European Communities, Comission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, SEC(2009) 585, SEC(2009) 586, available at http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf.

[150] *Ibid*, at p. 7-8.

validate that deployment concepts have met all privacy requirements. It should also be noted that PIA topics significantly overlap with those defined above related to privacy by design and accountability.

8.7 Annex 7 – Privacy Update 2010

2010 has been a year initiating the momentous review of three major data protection instruments – EU Directive 95/46/EC, the Council of Europe Treaty 108 and the OECD Transborder Dataflow Guidelines. Within this context of substantial reviews, 2010 has seen significant progress developing the concepts of accountability and privacy-by-design. Furthermore the concept of a right to be forgotten has received additional consideration. In this update, we will set forth the relevant developments of the year and then indicate how they either impact or further support the work and relevance of TAS³.

1. OECD Guidelines

The OECD Guidelines first introduced in 1980 are the subject of a review requested by the OECD Ministers to assure that they remain applicable in today's world of global information flows and more ubiquitous technology. The formal review, which will happen next year, was punctuated by three major conferences[151] that were meant as input to the review:

- the first reviewed the implementation and accomplishments of the Guidelines,
- the second, contemporaneous with the International Data Protection Commissioner's conference focused on the issues that new technologies pose for the application of the OECD principles, and
- The last was focused on the economics of privacy.

2. EU Data Protection Directive 95/46

The European Commission has undertaken a consultation on the revision of the Directive which was organized in two parts. The first part of the consultation was based on a short survey of general questions followed by a more detailed consultation paper.[152] The main areas of concentration in the consultation relative to TAS³ are:

- Breach Notification
- Improved notice
- Transparency of processing
- Data controller obligations
- Enhanced rights of access, rectification and erasure
- The right to be forgotten
- Data portability
- Clarifying consent
- More importance placed on having data protection officers
- Privacy-by-design

[151] www.oecd.org/sti/privacyanniversary

[152] http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm; http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462&format=HTML&aged=0&language=EN

- Exploring self-regulatory initiatives and self-certification schemes
- Promote high policy and technical standards on data protection to third countries and international organizations
- Improved of enforcement,
- Enhanced harmonization across the Union

Responsive comments to the consultation are requested by January 15, 2011 and an initial consultation draft of proposed revisions should be circulated by March or April 2011. The member state and Parliamentary review will likely take up to another two years with iterative drafts.

3 Council of Europe Treaty 108

The Council of Europe adopted Resolution 3 on data protection and privacy in the third millennium[153] at the recent Ministerial meeting in Turkey which formalized the review of its Convention for the Protection of Individuals with regard to Automatic processing of Data . Interestingly, the Resolution noted developments of cloud computing and social networks coupled with growing international data flows as some of the challenges they would address in this review. The Resolution further noted the need for privacy enhancing technologies and privacy-by-design. Lastly, it highlighted recent declarations of the International conference of data protection commissioners for binding global rules on data protection and suggested that Treaty 108, which was founded on the OECD Guidelines and which last year was made available for adoption by non-EU signatories was the logical instrument upon which to base such an international accord.

The COE also engaged in an interesting future-oriented study on the role of Convention 108 entitled Data Protection Vision 2020 – Options for improving European policy and legislation during 2010-2020 (COE Study).[154] While the COE Study focused mostly on how to deal with increased presence of police and investigatory officers in online environments, it provided useful summaries of the evolution of technology over time, the role of new technologies, the need for global instruments.

4. Privacy-by-Design

The concept of privacy-by-design (PbD) – privacy built in from the outset rather than bolted on after the fact, has been a project driven by a number of privacy authorities, companies and advocates, but is generally most associated with Anne Cavoukian, the Information Privacy Commissioner for Ontario who is generally recognized as the founding author of the concept and its principal proponent. Apart from numerous conferences on the topic over the last year, and Commissioner Cavoukian's creation of PbD Ambassadors, PbD has been cited in the revision process of the OECD Guidelines, Directive 95/46/EC and COE

[153] http://www.coe.int/t/dghl/standardsetting/minjust/mju30/MJU-30%20_2010_%20RESOL%203%20E%20final.pdf

[154] http://www.coe.int/t/dghl/standardsetting/dataprotection/J%20A%20Cannataci%20Report%20to%20Council%20of%20Europe%20complete%20with%20Appendices%2031%20Oct%202010.pdf

Convention 108. PbD was further enhanced by a resolution, appropriately introduced by Commissioner Cavoukian, which was adopted at the 32nd International Conference of Data Protection Commissioners in Jerusalem[155].

5. International Privacy Standard

The concept of an International Privacy Standard is also enjoying growing popularity. This concept was dramatically highlighted at the 31st International Conference of Data Protection Commissioners in Madrid where principles of a policy-based international privacy standard were endorsed in the Madrid Resolution[156] led by the Spanish Data Protection Commissioner. At this year's conference, the CNIL (France's Data Protection Authority) introduced a resolution, also adopted, calling for an intergovernmental conference to discuss the adoption of an international convention on privacy in 2011 or 2012[157]. The CNIL recalled the relevance of the Madrid Resolution on this topic and indicated that both houses of parliament in France would adopt resolutions in support of such an international agreement.

Work also continues on international privacy standards of a more technical nature at the International Standards Organization. ISO/IEC JTC 1 SC 27/WG5 has further developed its Privacy framework (29100) which is currently under balloting for Final Committee Draft (FCD). The Privacy reference architecture (29101) is being circulated for approval of its second Committee Draft (CD). Other relevant work items continue to be developed, dealing with topics of identity management (24760), entity authentication assurance (29115), access management (2916) and biometric information protection (24745).

6. Privacy Impact Assessments

As organizations and policy makers continue to understand the importance of privacy in the development and deployment of technologies that concern personal data flows, more emphasis is being placed on the development of tools to assist developers and technologists. Privacy Impact Assessments (PIAs) are privacy risk based evaluations of new technologies which are undertaken prior to deployment. Pursuant to requirements contained in guidance related to RFID, the European Commission empanelled an industry-led drafting group to develop and RFID PIA Framework which would be reviewed by the Article 29 Working Party[158]. Industry proposed the initial draft of PIA Framework in March of 2010[159]. The draft was formally reviewed by both the Article 29 Committee and ENISA and rejected mostly for a failure to elaborate in sufficient detail the risk

[155] http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf
[156] http://www.huntonfiles.com/files/webupload/PrivacyLaw_resolucion_madrid.pdf
[157] http://www.cnil.fr/english/news-and-events/news/article/the-international-conference-calls-on-national-public-authorities-to-adopt-an-international-conventi/
[158] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
[159] http://cordis.europa.eu/fp7/ict/enet/documents/industry-pia-framework-for-rfid-applications.pdf,

analysis process[160]. A revised draft has been submitted in late November and is currently under review by the Article 29 Working Party.

7. Accountability

The principle of accountability has also been included in a number of important instruments, including the European Commission Consultation and a new document from Commissioner Cavoukian addressing the relationship between accountability and privacy-by-design[161]. The Article 29 Working Party has also issued an Opinion on Accountability[162] that highlights the role accountability might play in the context of the review of Directive 95/46/EC. The Article 29 Opinion also highlights the evolving role of the data controller as well as the need to demonstrate that appropriate and effective measures have been taken as needed by the nature and use of information. Along the same lines, the Galway Accountability Project of 2009 which defined the essential elements of accountability was followed up by the Paris Accountability Project hosted by the CNIL, which focused on demonstrating and measuring accountability[163].

8. General Developments

A number of developments of note in 2010 are less directly relevant to TAS^3, but are important elements of trends that speak to the relevance of TAS^3. One of the most controversial issues which gained prominence in 2010 was behavioral advertising, also know as targeted marketing. The concern being that technology could be used to create profiles of individual behavior across sites which might be used for marketing purposes without user consent. Social networks remained topics of great interest for advocates and data protection authorities alike with concerns that such networks created too much visibility into a individual's life and brought up the difficult issue of how one can help individuals to make better choices about what information they make public, or how they should disclose information in general. Lastly the role of technology in obtaining information to tracking behavior from RFID, to Google Street View to cookies all came into question with data protection authorities exploring how to provide users with better information related to what was being collected, how and why as well as how to exert greater control over the information.

9. Relevance to TAS^3

All of the trends and developments highlighted above for 2010 share common threads which are the basis of TAS^3.

---

160 http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia, http://cordis.europa.eu/fp7/ict/enet/documents/opinion-rfid-pia-adopted.pdf

161 http://www.ipc.on.ca/images/Resources/pbd-accountability_HP_CIPL.pdf

162 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

163 http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

TAS³, at its heart, is a standards-based technical architecture supported by policies and contracts that allow individuals to control their information within an ecosystem designed to enhance trust, security and privacy. It should also be noted that a principal driver for TAS³'s development is to enable more accountable use and sharing of information.

The Demonstration projects of TAS³ are, for many functions, among the first test beds for integrated solutions of this type. The complex interplay and coordinated development of technical components, policies and contracts is likewise novel. TAS³ is likewise an engine for the development and eventual testing of practical tools from user-friendly comprehensive dashboards and controls, to privacy intake processes to policy and contract frameworks.

Amendment History

Version	Date	Author	Description/Comments
0.1-3	12-04-2009-24-05-2009	Joseph Alhadeff	Text
0.4	25-05-2009	Brendan Van Alsenoy	Revisions/comments/additions
0.5	26-05-2009	Joseph Alhadeff	Revisions/additions
0.6	26-05-2009	Brendan Van Alsenoy	Revisions/comments/additions
0.7	27-05-2008	Joseph Alhadeff	Minor revisions/final review
0.8	28-05-2008	Brendan Van Alsenoy	Minor revisions/final review
1.0	28-05-2008		Release
1.1	10-12-2009	Brendan Van Alsenoy	Integration in new template
1.1	10-12-2009	Brendan Van Alsenoy	Incorporation update WP6 requirements list
1.2	10-12-2009	Joseph Alhadeff	Incorporation Privacy Update 2009
1.3	17-12-2009	Joseph Alhadeff	Revisions WP6 requirements list
1.4	20-12-2009	Brendan Van Alsenoy	Minor revisions/comments to Privacy Update and Requirements list
1.5	27-12-2009	Joseph Alhadeff	Minor revisions to Privacy Update and Requirements list
1.6	24-3-2010	Griet Verhenneman	Integration of eHealth requirements
1.7	21-06-2010	Brendan Van Alsenoy	Integration of updated WP6 requirements list
1.8	22-12-2010	Joseph Alhadeff	Integration of Privacy Update 2010
1.9	28-12-2010	Joseph Alhadeff	Integration of section on sectoral issues
2.0	31-12-2010		Release