Privacy Management and Accountability in Global Organisations

Siani Pearson

Privacy Management and Accountability in Global Organisations

Siani Pearson

Hewlett-Packard, Security and Cloud Lab, Bristol, UK
Siani.Pearson@hp.com

Abstract. Organisations that operate in a global environment can be subject to potentially diverse and complex regulatory requirements. This paper explains some of the key issues that corporate governance faces related to privacy and some mechanisms for addressing these.

Keywords: Accountability, compliance, data protection, privacy, risk, security

1 Introduction

This paper focuses on 'good willing' organisations that wish to meet, and even exceed, legal privacy and data protection requirements. It considers some of the challenges that they face, best practice today in addressing these challenges and points to examples of cutting edge thinking that may shape future corporate privacy governance.

It is outside the scope of this paper to consider economic incentives for privacy-friendly organisational behaviour and different organisational attitudes towards investment in privacy enhancing mechanisms and privacy-related risk (see for instance [1]), the tension between data minimisation and the value and usage of personal data for organisations (for example, for marketing purposes) and related discussions including issues of market forces leading to erosion of moral standards within an entrepreneurial system (as described for example in [2]) countered to a greater or lesser extent by national regulatory standards, consumer pressure and other mechanisms [3]. Instead, the focus will be on how organisations can satisfy regulatory requirements and provide good data stewardship.

The structure of the paper is as follows: Section 2 considers how privacy requirements are challenging for global organisations, Section 3 describes central aspects and options for privacy governance within organisations, Section 4 shows how accountability forms part of the solutions needed and Section 5 discusses two particular examples of accountability-based privacy management solutions currently being developed or refined by the author. Finally, conclusions are given.

2 How Privacy Requirements can be Challenging

In this section privacy is introduced as a concept and its relationship with security is clarified in order that organisational privacy obligations can be considered and privacy risks and challenges for organisations further elucidated.

2.1 Privacy, Data Protection and Security

At the broadest level (and particularly from a European standpoint), privacy is a fundamental human right, enshrined in the United Nations Universal Declaration of Human Rights (1948) and subsequently in the European Convention on Human Rights and national constitutions and charters of rights. There are various forms of privacy, ranging from 'the right to be let alone' [4], 'control of information about ourselves' [5], 'the rights and obligations of individuals and organisations with respect to the collection, use, disclosure, and retention of personally identifiable information' [6], focus on the harms that arise from privacy violations [7] and contextual integrity [8]. For further discussion about the nature of privacy, see for example [3].

In the commercial, consumer context, privacy entails the protection and appropriate use of the personal information of customers, and the meeting of expectations of customers about its use (which may be reflected as informed consent or within private contracts). What is appropriate will depend on the applicable laws, individuals' expectations about the collection, use and disclosure of their personal information and other contextual information.

Data protection is the management of personal information, and is often used within the European Union (EU) in relation to privacy-related laws and regulations, although in the United States (US) the usage of this term is focussed more on security.

The terms '*personal information*' and '*personal data*' are commonly used within Europe and Asia, whereas in the US the term '*Personally Identifiable Information'* (PII) is normally used, but they are generally used to refer to the same concept. This can be defined as information that can be traced to a particular individual, and include such items as: name, address, phone number, social security or national identity number, credit card number, email address, passwords, date of birth. Some personal data elements are considered more sensitive than others, although the definition of what is considered *sensitive personal information* varies depending upon jurisdiction and even on particular regulations.

Privacy differs from security, in that it relates to handling mechanisms for personal information, although security is one element of that. Security mechanisms, on the other hand, focus on provision of protection mechanisms that include authentication, access controls, availability, confidentiality, integrity, retention, storage, backup, incident response and recovery. Privacy relates to personal information only, whereas security and confidentiality can relate to all information.

2.2 Organisational Privacy Obligations

We have seen that for organisations, privacy entails the application of laws, policies, standards and processes by which personal information is managed. The fair information practices developed in the US in 1970s [11] and later adopted and declared as principles by the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe [12] form the basis for most data protection and privacy laws around the world. These principles are shown in Table 1. This framework can enable sharing of personal information across participating jurisdictions without the need for individual contracts. It imposes requirements on organisations including data collection, subject access rights and data flow restrictions.

Table 1. OECD privacy principles

Principle	**Description**
Collection limitation	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the above except: a) with the consent of the data subject; or b) by the authority of law.
Security safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
Individual participation	Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time;

	ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

The collection and processing of personal information is subject to regulation in many countries across the world. Figure 1 illustrates how many different countries have national data protection legislation in place. The US does not have a comprehensive regime of data protection but instead has a variety of laws targeted at the protection of particularly sensitive types of information that tend to be sector-based or enacted at the state level. This (sometimes inconsistent) matrix of national laws can make it really hard for businesses to ensure full compliance if they are operating in multiple jurisdictions. Hence there is pressure from organisations for greater global interoperability to be achieved via development of a clear and consistent framework of data protection rules that can be applied, in order to reduce unnecessary administrative burdens and risks.

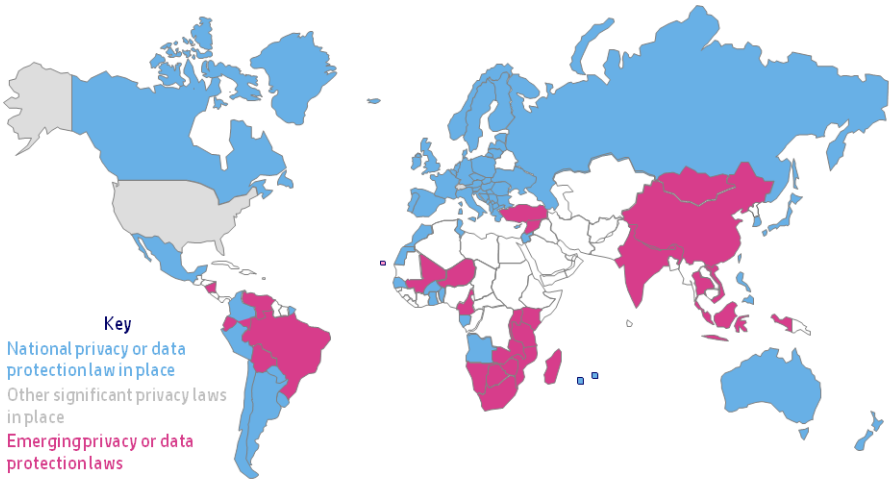

Fig. 1. Global data protection laws

Transborder flow of personal information, including access to this information, is restricted by some of these laws. For example, the European Data Protection Directive 95/46/EC [4] (and its supporting country legislation) is an important piece of

privacy legislation that restricts the movement of data from EU to non-EU countries that do not meet the EU 'adequacy' standard for privacy protection. Legislation similar to the European Data Protection Directive has been, and continues to be, enacted in many other countries, including Australia, New Zealand, Hong Kong, Japan and Asia-Pacific Economic Cooperation (APEC). In practice contractual mechanisms like Binding Corporate Rules or Model Contracts might need to be put in place in order to allow data access. However, these arrangements typically take several months to set up, and hence are not well suited to dynamic environments. Hence the OECD revised guidelines [13] now recommend the practical implementation of privacy protection through an approach grounded in risk management and stress the need for improved global interoperability.

With regard to security, it is a common requirement under data protection law that if a company outsources the handling of personal data to another company, it has some responsibility to make sure the outsourcer uses "reasonable security" to protect those data. This means that any organisation creating, maintaining, using or disseminating records of personal data must ensure that the records have not been tampered with, and must take precautions to prevent misuse of the information.

Of course, in addition, organisations need to take into account the privacy-related expectations of their customers, which may be specified within private contracts, and this is likely to involve a combination of process-based and access control mechanisms. The legal obligations vary according to the regulatory context and indeed there are likely to be some quite significant changes in the near future. Problems with the 1995 EU Data Protection Directive [4] as a harmonisation measure and in relation to new technologies including cloud computing have led the European Commission (EC) in January 2012 to publish a draft of replacement General Data Protection Regulation [5] that is currently being discussed and revised, in which accountability features and privacy by design take greater precedence. Amongst other things, this imposes new obligations and liabilities for data processors, new requirements on data breach notification and stricter rules on international data transfers. It also empowers National Regulatory authorities to impose significantly higher fines. In addition, a European Cloud Computing Strategy [14] has been launched aiming at more clarity and knowledge about the applicable legal framework and making it easier to verify compliance with the legal framework (e.g. through standards and certification). Furthermore, in February 2013 the European Commission published a cybersecurity strategy [15] alongside a draft directive on network and information security [16]. Once implemented, many service providers will be covered by a range of data security obligations including adopting risk management practices and reporting major security incidents.

2.3 Privacy Risks and Challenges

Privacy challenges for businesses include data breaches, risk of litigation due to country-specific laws, the complexity of managing privacy and negative public attention and loss of brand value if exposures occur. Data breaches can be costly – on average 204 US dollars per record, according to a 2010 Ponemon Institute study. When cus-

tomers are concerned for the welfare of their privacy, it can affect a company's ability to do business. This concern may arise for example due to worries about unsolicited marketing, identity theft, surveillance or unwanted inferences about behavior.

Privacy issues depend upon the role of the company. For example, an organisation could be a custodian of employee personal data, could collect end-user personal information, or could just be providing outsourcing services for another organisation. Legally, the requirements are quite different depending upon whether the organisation is a data controller or a data processor in that situation (although it might be both).

A *data controller* is an entity which alone or jointly with others determines the purposes for which and the manner in which any item of personal information is processed. It could be a person, public authority, agency or other body and is legally responsible for ensuring compliance requirements are met. Obligations and risks of the data controller include: regulatory fines, criminal liability, civil liability if data subjects enforce their rights, investment risk, business continuity impact and reputational damage. In environments such as cloud computing, a data controller has a responsibility to ensure that the service providers are meeting regulatory obligations and this can be challenging [17].

A *data processor* is an entity which processes personal information on behalf and upon instructions of the data controller. Contractual agreements may add additional responsibilities or constraints with respect to privacy, although data protection laws stipulate that the organisation that is transferring personal information to a third party for processing remains responsible for the personal information. The data processor may also face issues such as lack of training of key personnel and deliberate targeting of sensitive information by criminals.

When considering privacy risks, context is an important aspect, as different information can have different privacy, security and confidentiality requirements and privacy threats differ according to the type of scenario: for example, they would tend to be higher for services that are dynamically personalised, based on people's location, preferences, calendar and social networks, etc. Privacy need be taken into account only if a service handles personal information, in the sense of collecting, transferring, processing, sharing, accessing or storing it. Even if the same information is involved, there may be different data protection requirements in different contexts, due to factors including location and trust in the entities collecting and processing it. There are special laws concerning treatment of sensitive data, and data leakage and loss of privacy are of particular concern to users when sensitive data is processed. In addition, privacy issues vary across different stages of the information lifecycle, e.g. data collection, processing, storage, archival and destruction. Some companies might choose to ignore the issue and pay the penalties if they are found to be in breach, but at the time of writing, regulations, enforcement activities and sanctions are currently increasing the world over.

Privacy risks and concerns are increasing, not least due to the recent revelations about the extent of government surveillance [18] and to the rapid rise in big data analysis [19]. Correspondingly there is a need to push compliance and reduce risks throughout organisations, including to untrained people that might expose hundreds of files by the click of a button, lose a laptop containing unencrypted confidential infor-

mation or switch sensitive information to the cloud almost instantly using a credit card. However, requirements can be complex to ascertain and a privacy staff is typically small, making effective oversight over hundreds or possibly thousands of projects per year difficult. Hence the role of both process and technology is important. This is considered further in the following section.

3 Corporate Governance for Privacy

In this section it is briefly explained how privacy governance may be achieved within an organisation.

3.1 The Role of Corporate Governance

Companies differ in the resources they have available to deal with privacy. Many larger organisations have a Chief Privacy Officer and privacy staff in order to implement compliance in their organisations. Smaller organisations often do not have the resources for hiring qualified privacy experts and instead the person appointed who is responsible for overseeing the organisation's compliance with applicable privacy legislation could well be the owner or operator. Key elements of privacy management such as defining a corporate privacy policy can often be difficult to achieve in such situations. However, small companies are largely domestically bound, and hence driven by domestic legislation, except in the case for certain small companies in niche areas that might quickly become multinational. For multinational companies, requirements are more diverse and privacy management is more difficult. Nevertheless, data is an asset, so proper privacy management will be valuable for forward-thinking companies, quite apart from being mandatory from a legal point of view.

Privacy management programmes serve as the core operational mechanism through which organisations implement privacy protection. In addition, a related element that needs to be in place within an organisation is data security breach notification, which may require both notice to an authority and notice to an individual affected by a security breach affecting personal data.

Key elements of a successful privacy programme include:

garnering senior management support and establishing a comprehensive organisational privacy policy
establishing clear processes and assign responsibilities to individuals
using proven, existing standard and frameworks for security and IT management
establishing proper monitoring and audit practices, in order to verify and assess what is happening in the organisation against the privacy policies, and take action where required to achieve alignment

More specifically, a privacy management program would ideally include the following measures [20]:

1. establishing reporting mechanisms and reflecting these within the organisation's privacy management program controls
2. putting in place privacy management *program controls*, namely:
   - a *Personal Information Inventory* to allow the organisation to identify the personal information in its custody, its sensitivity and the organisation's authority for its collection, usage and disclosure
   - *policies* relating to: collection, use and disclosure of personal information (including requirements for consent and notification); access to and correction of personal information; retention and disposal of personal information; privacy *requirements for third parties* that handle personal information; security controls and role-based access; handling complaints by individuals about the organisation's personal information handling practices
   - *risk assessment* mechanisms
   - *training and education*
   - *breach and incident management*
   - procedures for *informing individuals* about their privacy rights and the organisation's program controls
3. developing an *oversight and review plan* that describes how the organisation's program controls will be monitored and assessed
4. carrying out *ongoing assessment and revision* of the program controls above

3.2 Privacy by Design

Privacy by Design refers to the philosophy and approach of embedding privacy into design specifications, as first espoused by Ann Cavoukian and others [21, 22]. It applies to products, services and business processes. The main elements are:

1. recognising that privacy concerns must be addressed
2. applying basic principles expressing universal spheres of privacy protection
3. mitigating privacy concerns when developing information technologies and systems, across the entire information life cycle
4. integration of qualified privacy input
5. adopting and integrating privacy-enhancing technologies (PETs) [23]

In essence, companies should build in privacy protections at every stage in developing products, and these should include reasonable security for consumer data, limited collection and retention of that data, as well as reasonable procedures to promote data accuracy. Various companies have produced detailed privacy design guidelines (see for example [24]). In addition to the Canadian regulators, there has been strong emphasis and encouragement from Federal Trade Commission (FTC) and EC amongst others on usage of a privacy by design approach [25, 26].

'Privacy by policy' is the standard current means of protecting privacy rights through laws and organisational privacy policies, which must be enforced. Privacy by policy mechanisms focus on provision of notice, choice, security safeguards, access and accountability (via audits and privacy policy management technology). Often,

mechanisms are required to obtain and record consent. The 'privacy by policy' approach is central to the current legislative approach, although there is another approach to privacy protection, which is 'privacy by architecture' [27], which relies on technology to provide anonymity. Unfortunately, the latter is often viewed as too expensive or restrictive. Although in privacy by policy the elements can more easily be broken down, it is possible (and preferable) to enhance that approach to cover a hybrid approach with privacy by architecture.

In summary, perfection is not reachable in a complex and moving global context, but companies are expected to think upfront about the impact and the risk they create, and privacy by design has a strong role to play in helping organisations balance innovation with the expectations of individuals. In addition, both regulators and individuals expect organisations to act as a responsible steward of the data which is provided to them, and the way in which companies need to do more to live up to their promises and ensure responsible behaviour is considered in the following section. In particular, corporate governance plays a central role in providing accountability within an organisation, by means of the organisation identifying risks, having appropriate policies that mitigate risks, mechanisms for enforcement internally and for monitoring that these are effective within the enterprise, and for internal and external validation of this. In addition, provision of transparency can help enforce privacy obligations along the service provision chain.

4 Accountability

In this section the role of accountability is explained, in the sense of being an essential aspect of privacy governance. Furthermore, a model of accountability is presented and it is explained how organisations can be accountable. Accountability is a broader notion than just data protection and privacy, but the scope of discussion within this section is largely restricted to that domain as this is the area of interest for this paper.

4.1 What is Accountability?

Accountability is a notion of which there is no universally agreed definition, although it is generally agreed that responsibility, transparency and holding to account are key elements. It is a complex notion that is used in a slightly different sense in different domains. For example, in computer science it is often used to refer to formal verification, compliance and privacy and security policy enforcement; in information security, accountability is meant to generate assurance, transparency and responsibility in support of control and trust; from a corporate governance perspective accountability is an organisational privacy management program and from a social, legal and ethical perspective the emphasis is often on holding organisations and actors accountable for their actions.

In data protection regulation, as we have seen in Section 2, accountability is normally about complying with measures that give effect to practices articulated in given guidelines. For example, a data controller is responsible for complying with particular

data protection legislation and, in most cases, is required to establish systems and processes which aim at ensuring such compliance. Indeed, the notion of accountability appears in several international privacy frameworks in addition to the OECD Privacy Guidelines (1980) already considered above, including Canada's PIPEDA (Personal Information Protection and Electronic Documents Act) (2000), APEC Privacy Framework (2005), Article 29 Working Party papers [28] and some elements of the draft European Data Protection Regulation (although in that case not directly associated with the word 'accountability' largely for reasons of translatability) [25]. The usage of this notion by regulators is evolving towards an 'end-to-end' personal data stewardship regime in which the enterprise that collects the data from the data subject is accountable for how the data is shared and used from the time it is collected until when the data is destroyed. This extends to onward transfer to and from third parties.

Building on such analysis, a definition of accountability that is applicable across different domains and that captures a shared multidisciplinary understanding is [29]:

> *Accountability consists of defining governance to comply in a responsible manner with internal and external criteria, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly.*

Internal criteria are not necessarily visible to stakeholders external to that organisation, as they might for example reflect the risk appetite of that organisation or known security vulnerabilities; external criteria could include best practice on security, data protection and breach notification, as well as privacy regulatory and contractual requirements and societal expectations.

Although it is a complex notion, it could be argued that its core, accountability is a very simple idea. It says that not only should an organisation do everything necessary to exercise good stewardship of the data under its control, it should also be able to demonstrate that it is doing so. Good stewardship is achieved by designing systems appropriately, so that they reflect privacy principles and security expectations from partners, regulators and data subjects, as well as by the organisation living up to its promises and ensuring responsible behaviour. The demonstration – via provision of an account – is an essential aspect, but can be challenging to provide. Furthermore, if events do not work out as planned, organisations need to provide a means of remediation as well as needing to try to prevent such an occurrence happening again. These elements are captured in Figure 2, which shows how accountability should complement the usage of appropriate privacy and security controls in order to support democratically determined principles that reflect societal norms, regulations and stakeholder expectations. Governance and oversight of this process is achieved via a combination of Data Protection Authorities, auditors and Data Protection Officers within organisations, potentially supplemented by private Accountability Agents acting on their behalf.

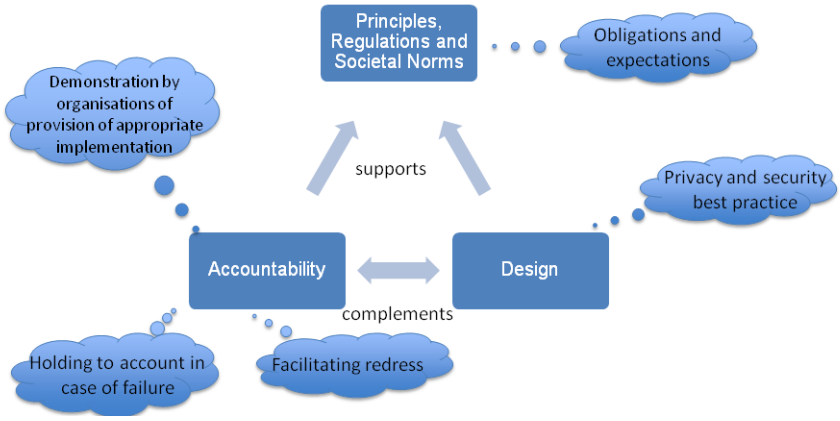

Fig. 2. Accountability context

At its core, in the sense that a data controller should be accountable for complying with measures which give effect to principles that have been set within a democratic context, and that they will be held to account in case of failure, as well as the provision of tools to help organisations to 'do the right thing' (including for better remediation, breach notification, etc.), accountability is obviously a good thing and not very controversial. However, there are a number of different and even conflicting opinions related to additional (or even alternative) potential features of an accountability-based approach. In the main these relate to how accountability can help address the issue of the lack of take up of privacy by design by organisations to date, the role of accountability in moving towards greater regulatory interoperability, the importance of measures that prevent privacy harm and the extent to which punishment for a privacy violation should be lessened by evidence that appropriate privacy and security measures have been taken by an organisation. The former can be done in particular by easing transborder data flow constraints and regulatory complexity in favour of a single set of organisational requirements that need to be adhered to that could apply globally (as is the case with Binding Corporate Rules for instance [30]), allowing differentiation in terms of privacy (so long as legal requirements are met), being less prescriptive in terms of the specification of regulatory requirements, encouraging (or even mandating) usage of privacy impact assessments to guide design and also of course increasing punishment in cases of non-compliance as well as taking into account the controls an organisation has used when determining punishment. Opinions about the relative merits of these approaches differ. In addition, Weitzner views accountability as retrospective (arguing that a shift is needed from hiding information to ensuring that only appropriate uses occur) [31] whereas preventive risk identification and mitigation is viewed as an essential element of accountability by others [32, 20].

It is often regarded as underpinning an accountability-based approach that organisations should be allowed greater control over the practical aspects of compliance with data protection obligations in return for an additional obligation to prove that

they have put privacy principles into effect (see for example [32]). Hence, that whole approach relies on the accuracy of the demonstration itself. If that is weakened into a mere tickbox exercise, weak self certification and/or connivance with an accountability agent that is not properly checking what the organisation is actually doing, then the overall affect could in some cases be very harmful in terms of privacy protection. As Bennett points out [33: p45], due to resource issues regulators will need to rely upon surrogates, including private sector agents, to be agents of accountability, and it is important within this process that they are able to have a strong influence over the acceptability of different third party accountability mechanisms. This can be achieved via independent testing of practices, provision of evidence that is taken into account, including auditing against the ISO 27001 series and associated security standards.

Hence, the way in which accountability is achieved is key, which includes the need for adequate resources in checking and enforcing whether organisations are indeed using appropriate measures, involvement of different stakeholders, including the public (or representatives of the public) in data privacy regulation, provision of suitable accountability tools and help for organisations to form appropriate risk assessment mechanisms and policies. In the next two sections the type of measures are elucidated that are needed as part of such an approach.

4.2 A Model of Accountability

In Figure 3 a model of accountability is presented that shows how accountability can be captured at different layers of abstraction. The top layer of the triangle shown in Figure 3 corresponds to the definition of accountability, as given in the previous subsection. Moving down the model in terms of becoming less abstract, the other layers correspond in turn to the following aspects:

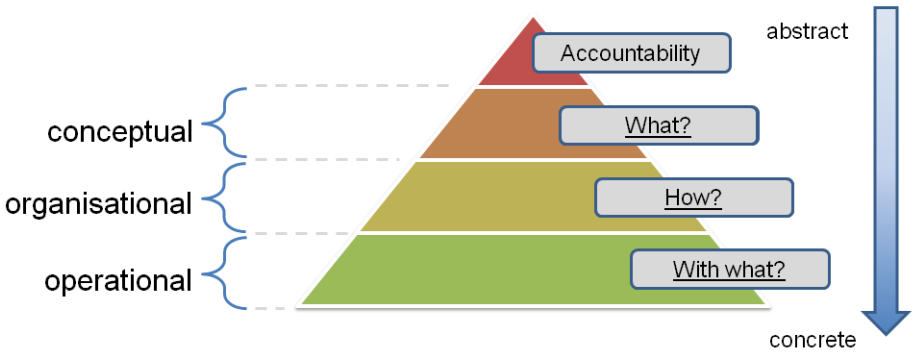

Fig. 3. Conceptual model of accountability

Accountability attributes. These are the central taxonomic components of accountability, namely: observabililty, verifiability, attributability, transparency, responsibility, liability and remediability. Further details are given in [34].

Accountability practices. These define the central behavior of an organisation adopting an accountability-based approach. From the definition given above, it can be seen that these are: defining governance, ensuring implementation of appropriate actions, explaining and justifying those actions and remedying any failure to act properly. These map to the Galway project's 'essential elements' of accountability [32]. Further details are given in the following section.

Accountability mechanisms and tools. These tools and mechanisms offer enhanced accountability; organisations in addition will need to use privacy and security controls appropriate to the context, as described in the previous subsection. The tools may form a toolbox from which organisations can select as appropriate. They can be (extensions of) existing business processes like auditing, risk assessment and the provision of a trustworthy account, or non-technical mechanisms like formation of appropriate organisational policies, remediation procedures in complex environments, contracts, certification procedures, and so on. Or they can be technical tools, which would include tracking and transparency tools, detection of violation of policy obligations, notification of policy violation, increased transparency without compromising privacy, and so on. The tools are targetted at different stakeholders, and some are designed for usage as a preventive measure (for example, to assess and reduce privacy harm before personal data is collected), some as a detective measure (for example, to assess the degree to which privacy obligations are actually being met) and others as a corrective measure (for example, to facilitate redress).

4.3 How can Organisations be Accountable?

This subsection provides more detail about the third layer of the model above, namely how to be accountable. An accountable organisation must commit to responsible stewardship of other people's data, which in brief entails that it must define what should be done, monitor how it is done, remedy any discrepancies between definition and fact, and explain and justify relevant actions. We now consider these aspects further below.

First and foremost, an accountable organisation must demonstrate willingness and capacity to be responsible and answerable for its data practices with regard to personal data. Analogously, the same applies more broadly with regard to confidential data that may or may not be personal data – for example, business secrets, although that takes us out of the remit of privacy concerns and hence we do not say too much more about that in this paper.

In order to achieve this, senior management support for an accountability-based culture within the organization must be obtained and a reporting structure set up with responsibilities allocated to individuals, as discussed already in Section 3.1. In addition, an accountable organisation must address the following four central aspects:

1. *define and deploy policies regarding their data practices* that link to relevant external criteria and are supported by senior management. The policies include specification of the entities involved in the processing of data and their respon-

sibilities; the scope and context of processing data; the purposes and means of processing and data handling and data access policies. The policies need to take account of relevant external legal obligations. In addition, policies need to be defined related to risk monitoring and risk mitigation. Mechanisms are also needed in order to put these policies in place, including risk assessment and means to make uses transparent to individuals and to assure that their rights are respected.

2. *monitor their data practices:* this includes how they process data, evidence that the organisation has acted according to its policies, and a running account that is a record of the monitoring and its results. In particular, periodic internal reviews are needed to provide assurance that the mechanisms are working and improve over time.
3. *correct policy violations:* this includes both the effects of the violation that need to be addressed, as well as causes of the violation that need to be addressed, and the informing of appropriate stakeholders, who include authorities, customers and affected data subjects. The effects of the violation could involve errors that need to be corrected and damages that need to be compensated, financially or otherwise.
4. *demonstrate policy compliance:* policy violations need to be reported and compliance with policies needs to be demonstrated in a timely fashion, reactively and where possible, proactively. The organisation must demonstrate that the controls selected and used within the service provision chain are appropriate for the context and should provide evidence that the operational environment is indeed satisfying the policies. There must be openness to oversigh by enforcement agencies, together with remediation if the goals of data protection have been abused in a harmful fashion.

So far, this analysis corresponds in a general way to that given within the Accountability Project [32] and other opinions influenced by that [20]. But in addition, two other important aspects need to be emphasised.

First, accountable organisations must ensure that accountability extends through across their service supply chains, in other words ensuring that the services and partners they use are accountable too, which involves amonst other things proper allocation of responsibilities and provision of evidence about satisfaction of obligations along the service provision chain.

Second, there are implications in terms of the way that the enforcement and verification mechanisms for accountability will operate, the scope of risk assessment and the ways in which other stakeholders are able to hold an organisation to account.

5 Two Example Solutions

Solutions to the above issues could take a number of forms. As considered above, there is a wealth of different privacy and security controls that an organisation could choose to use.

Risk assessment (a core security process) is particularly important for accountability because it is a central part of the process used to determine and demonstrate that the policies (whether reflected in corporate privacy and security policies or in contractual obligations) that are signed up to and implemented by the organisation (that is taking an accountability-based approach) are appropriate to the context. The type of procedures and mechanisms vary according to the risks represented by the processing and the nature of the data [17].

We now consider further two particular solutions for privacy management and accountability within global organisations, namely HP Privacy Advisor, which is a type of privacy risk assessment system, and a range of solutions being developed within the EU Cloud Accountability project. The latter includes further research to provide risk assessment mechanisms in relation to cloud service provision.

5.1 HP Privacy Advisor

Existing organisational risk assessment processes need to be enhanced to meet the requirements above, or else supplemented with separate privacy-specific risk assessment [35]. Privacy impact assessments are already being rolled out as part of a process to encourage privacy by design [35]: in November 2007 the UK Information Commissioners Office (ICO) (an organisation responsible for regulating and enforcing access to and use of personal information), launched a Privacy Impact Assessment (PIA) [35] process (incorporating privacy by design) to help organisations assess the impact of their operations on personal privacy. This process assesses the privacy requirements of new and existing systems; it is primarily intended for use in public sector risk management, but is increasingly seen to be of value to private sector businesses that process personal data. Similar methodologies exist and can have legal status in Australia, Canada and the US [35]. The methodology aims to combat the slow take-up to design in privacy protections from first principles at the enterprise level. Usage is increasingly being encouraged and even mandated in certain circumstances by regulators [35]. Data impact assessment may also become an obligation for some high risk contexts within the forthcoming EU regulation [cf. Article 33: 25].

As we have considered in Section 4, accountability, as articulated by the Article 29 Working Party [28], begins to shift our thinking from only having an obligation to comply with a principle, to an obligation to prove that you can put those principles into effect. Technology can assist organisations in ensuring proper implementation. New laws and regulations are increasingly having explicit requirements that an organisation not only comply, but that they have programs that put the principles into effect. Hence companies will need to do more to ensure that privacy is indeed considered in their products and services.

HP Privacy Advisor (HP PA) is an intelligent online rule-driven system that assesses activities that handle personal data within HP and provides privacy by design guidance. It is a web-based decision support system used internally within HP to assess risk and degree of compliance for projects that handle personal data and to guide individual employees in their decisions on how to handle different types of data. HP PA elicits privacy-relevant information about a project via a customised sequence of

questions. It uses a dynamic interface to minimise unnecessary questions and maintains a record of activities.

As shown in Figure 4, based on the answers given, HP PA:

- Assesses a project's degree of compliance with corporate privacy policy, ethics and global legislation, and the privacy promises the company makes
- Integrates privacy risk assessment, education, and guidance into the process
- Scores projects for a list of ten privacy compliance indicators including transborder data flows, compliance, business controls, security, transparency, and so forth
- Generates tailored privacy design guidance or a tailored compliance report for each project and, if appropriate, notifies an appropriate member of the corporate privacy team for further guidance/intervention
- Provides checklists, reminders, customised help and warnings to users
- Maintains a record of activities for audit purposes.

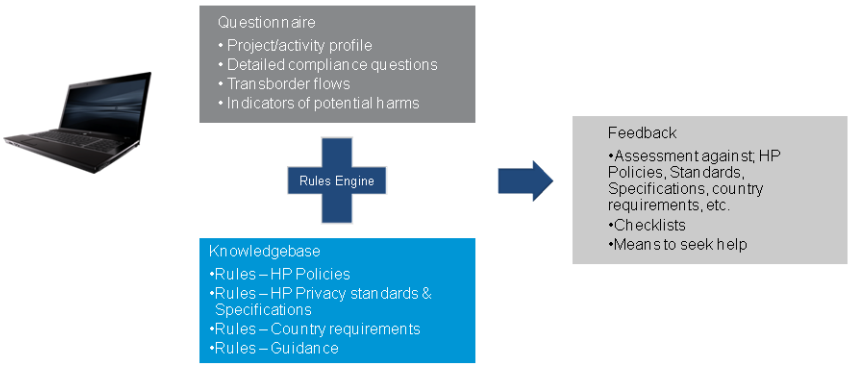

Fig. 4. Functional overview of HP Privacy Advisor

HP PA is a standard three tier web application using Java Enterprise Technology, where the client is a standard web browser, the application tier is a standard Java application server, and the persistence layer is a standard relational database. An accurate representation of organisational privacy policies is provided that encodes HP's 300 plus page privacy policies. HP PA uses JBoss Drools 5, a forward chaining rules engine both for validating the users' responses against a set of privacy rules, and to dynamically tailor the user experience using a questionnaire generated by a set of questionnaire rules. Desirable system properties are ensured such as deterministic behaviour of questionnaire and report generation, tailoring, and completeness of the questionnaire generation. For further information about this system, see [37].

5.2 EU Cloud Accountability Project

As data moves to the cloud, new risks and vulnerabilities arise and in addition there are concerns over data security, integrity and privacy due in particular to reduced

transparency and less control. As a result, organisations are reluctant to let data flow outside the organisations' boundaries into the cloud, and in addition individuals have concerns over privacy and their relative lack of control.

Cloud computing creates new dynamics in that there is an additional role of cloud provider, and indeed there could be several such parties. This not only can cause legal uncertainty in certain cases, but there is more general a need for clarification of distributed privacy and security responsibilities and control. Privacy is a difficult issue to tackle, because of the underlying complexity across multiple dimensions and the interdisciplinary nature of the problem. For example, location matters from a legal point of view and there are restrictions about how information can be sent and accessed across boundaries as briefly discussed in Section 2 above, but in cloud computing data can flow along chains of service providers both horizontally between software-as-a-service providers and vertically, down to infrastructure providers, where the information can be fragmented and duplicated across databases in different jurisdictions. Furthermore, the cloud model can magnify existing issues (such as transborder flow, data deletion, loss of control and transparency) and new vulnerabilities are also possible (such as security attacks exploiting the vulnerabilities of virtualisation mechanisms). The risks, as well as responsibilities, will vary according to the combination of cloud service and deployment models. Correspondingly, security and privacy requirements will vary widely from one use case to the next. Within a cloud ecosystem, issues from one cloud service provider (CSP) may have ramifications further up the chain, for example in terms of loss of governance. Loss of governance may arise in cloud computing for example as the client cedes control to the CSP, but service level agreements may not offer commitment to provide such services on the part of the CSP, thus giving a gap in security. For further discussion of privacy risks in the cloud, see [17].

The overall goal of the EU Cloud Accountability project [38] is to develop and validate techniques for implementing accountable cloud ecosystems. This includes development of techniques that can enable improved trustworthiness of cloud service provision networks, and to prevent breaches of trust by using audited policy enforcement techniques, assessing the potential impact of policy violations, detecting violations, managing incidents and obtaining redress. The outputs of the project include an accountability framework (including recommendations, guidance, models of data governance, accountability metrics and a reference architecture) as well as a range of accountability tools and mechanisms. These are being developed for organisations using cloud services as well as cloud service providers, regulators and data subjects.

The focus of the project is on personal data, but in addition certain types of confidential information that may not involve personal data, such as business secrets, are being considered. The focus is particularly on the accountability of organisations using and providing cloud services to data subjects and regulators. Government surveillance, including government acquisition of data from cloud service providers, is outside the scope of this project, except where it relates specifically to a data protection law accountability mechanism: no accountability controls of the types considered in the project (which are based upon assisting compliance with domestic data protec-

tion legislation and private contracts) are likely to provide effective protection against such activities.

The overall approach is as follows. The legal and contractual context defines obligations, responsibilities and liabilities of actors in a given cloud ecosystem. Businesses need to meet these obligations and mitigate risk and uncertainty in dynamic and global environments. This is a challenging problem especially where service provision chains are complex. Actors within cloud ecosystems may select mechanisms and tools to support accountability practices, and thereby help them to comply with relevant regulatory regimes within specific application domains. Overall, the project aims to move beyond a tick-box culture by providing organisations with the appropriate support to take an accountability-based ethical approach and make that a business advantage.

6 Conclusions

Privacy for companies is about managing privacy requirements end-to-end. Technical point solutions, such as encryption and auditing tools, are vitally important, but often address only a small part of overall privacy concerns. Although a number of different privacy-enhancing technologies are available, privacy requirements for global organisations can still be challenging to properly address.

The way that business environments are changing means that more automation (including much greater adoption of anonymisation techniques and encryption governed by consumers where possible) is needed in order to protect privacy online [39]. The challenge is how to move towards this model, including extension of that beyond the 'good willing' enterprises to others who are not necessarily willing to invest in governance practice that lessens privacy risks. Transparency, responsibility, privacy impact assessment and assurance – key aspects of accountability – are an important part of such a solution.

New technologies and business models can bring a higher risk to data privacy and security. For example, there can be rapid scaling (through subcontracting), remote data storage, and the sharing of services in a dynamic environment. This is a key user concern, especially for sensitive information like financial and health data. In global and dynamic environments especially, the associated lack of consumer trust – whether from individuals or Chief Information Officers in large organisations – can act as a barrier to business, and lack of regulator trust is resulting in increased penalties for non-compliance right across the world at present. The necessary increased trust can come from improved transparency and sound stewardship of information by service providers for which they are held accountable. Ongoing development of complementary solutions in the area of privacy by design and accountability is needed. Some examples of such an approach have been given in this paper.

Acknowledgements. The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no: 317550 (A4Cloud). In particular, acknowledgement is given to Daniel

Pradelles for assistance in creating Figure 1 (which gives a rough indication of the situation in 2012 and should not be regarded as completely accurate for all countries) and input from other members of Work Package C2 within the Cloud Accountability Project in collectively forming the accountability model discussed in Section 4.

References

1. Information Commissioner's Office (ICO), The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection, March http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_DIVIDEND.ashx (2010)
2. Tressell, R.: The Ragged Trousered Philanthropists. Wordsworth Classics (2012)
3. Bennett, C.J., Raab, C.D.: The Governance of Privacy: Policy Instruments in Global Perspective. MIT Press, Cambridge, Massachusetts (2006)
4. Warren, S., Brandeis, L.: The Right to Privacy. 4 Harvard Law Review 193 (1890)
5. Westin, A.: Privacy and Freedom. New York, US, Atheneum (1967)
6. American Institute of Certified Public Accountants (AICPA) and CICA: Generally Accepted Privacy Principles. August (2009)
7. Solove, D.J.: A Taxonomy of Privacy. University of Pennyslavania Law Review, 154(3):477, January (2006)
8. Nissenbaum, H.: Privacy as Contextual Integrity. Washington Law Review, pp. 101-139 (2004)
9. Swire, P., Bermann, S.: Information Privacy. Official Reference for the Certified Information Privacy Professional, CIPP (2007)
10. European Commission (EC): 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. (1995)
11. Privacy Protection Study Commission: Personal Privacy in an Information Society, United Statues Privacy Protection Study Commission Fair Information Practices. (1977)
12. Organisation for Economic Co-operation and Development (OECD): Guidelines for the Protection of Personal Data and Transborder Data Flows. (1980)
13. OECD: Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (2013)
14. European Commission, Unleashing the Potential of Cloud Computing in Europe, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF (2012)
15. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1667 (2013)
16. European Commission, Directive on Network and Information Security, http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (2013)
17. Pearson, S.: Privacy, Security and Trust in Cloud Computing. In: Privacy and Security for Cloud Computing, Computer Communications and Networks, S. Pearson and G. Yee (eds.), Springer, pp. 3-42 (2012)

18. The Guardian: NSA Prism program taps in to user data of Apple, Google and others, 7 June, http://www.guardian,co.uk/world/2013/jun/06/us-tech-giants-nsa-data (2013)
19. Barabási, A.-L.: Scientists must spearhead ethical use of big data. http://www.politico.com/story/2013/09/scientists-must-spearhead-ethical-use-of-big-data-97578.html (2013)
20. Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Colombia: Getting Accountability Right with a Privacy Management Program. April (2012)
21. Cavoukian, A.: Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era. In: Privacy Protection Measures and Technologies in Business Organisations: Aspects and Standards, G. Yee (ed), pp. 170-208, IGI Global (2012)
22. Information Commissioners Office (ICO): Privacy by Design. Report, www.ico.gov.uk (2008)
23. Shen, Y., Pearson, S.: Privacy Enhancing Technologies: A Review. HPL-2011-113, http://www.hpl.hp.com/techreports/2011/HPL-2011-113.html
24. Microsoft Corporation: Privacy Guidelines for Developing Software Products and Services, Version 2.1a (2007)
25. European Commission: Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, January (2012)
26. Federal Trade Commission (FTC): Protecting Consumer Privacy in an Age of Rapid Change: Recommendations for Business and PolicyMakers. FTC Report, March (2012)
27. Spiekermann, S., Cranor, L. F.: Engineering privacy. IEEE Transactions on Software Engineering, pp. 1-42. IEEE (2008)
28. European DG of Justice: Article 29 Working Party. 'Opinion 3/2010 on the principle of accountability (WP 173)', July (2010)
29. Felici and Pearson (eds.), MS:C-2.2, Internal Project Report, A4Cloud project, March 2013.
30. Information Commissioner's Office (ICO): Binding Corporate Rules http://www.ico.gov.uk/for_organisations/data_protection/overseas/binding_corporate_rules.aspx
31. Weitzner, D.J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G.J.: Information accountability. Communications of ACM 51(6), p. 87, June (2008)
32. Center for Information Policy Leadership (CIPL): Data protection accountability: the essential elements. http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf (2009)
33. Bennett, C.J.: The Accountability Approach to Privacy and Data Protection: Assumptions and Caveats. In Managing Privacy through Accountability, ed. D. Guagnin et al., MacMillan, pp. 33-48 (2012)
34. Catteddu, D. et al: Towards a Model of Accountability for Cloud Computing Services. In: Proceedings of the DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC), May (2013)

35. Trilateral Research and Consulting, Privacy Impact Assessment and Risk Management, ICO report, May http://www.ico.org.uk/~/media/documents/library/Corporate/Research_and_reports/pia-and-risk-management-full-report-for-the-ico.pdf (2013)
36. Information Commissioner's Office UK (ICO): Data protection guidance note: Privacy enhancing technologies. (2007)
37. Pearson, S., Sander, T.: A Decision Support System for Privacy Compliance. In: Threats, Countermeasures, and Advances in Applied Information Security, Manish Gupta, John Walp, and Raj Sharman (eds.), Information Science Reference, IGI Global, New York, pp. 158-180 (2012)
38. EU Cloud Accountability project, www.a4cloud.eu
39. Mowbray, M., Pearson, S.: Protecting Personal Information in Cloud Computing. In: On the Move to Meaningful Internet Systems: OTM 2012, R. Meersman, T. Dillon et al. (eds.), LNCS, Springer, pp. 475-491 (2012)