Deloitte.

Being privacy friendly while outsourcing
in light of the forthcoming EU Data Protection Regulation

October 2013

Content

Introduction:
"Is our privacy policy not enough?"

This question is being posed by many boards of directors when confronted with the reality that personal data privacy can pose a problem when outsourcing IT services.

For most organizations the answer is that while having a privacy policy is a good start, it is not sufficient on its own.
Consider:

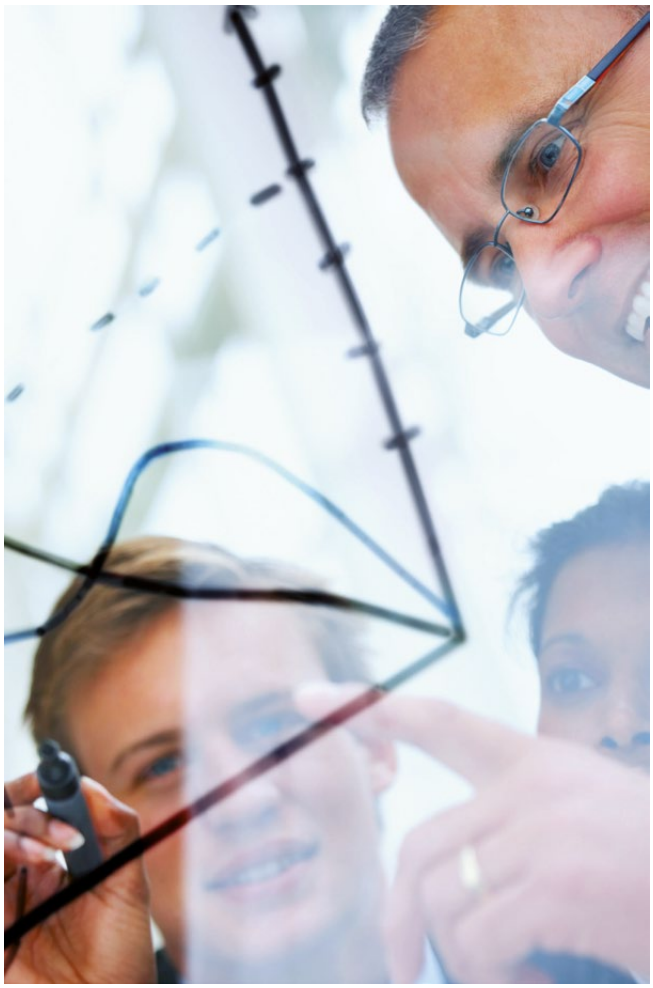
- Five out of the nine top threats, including the top three, for cloud computing in 2013 relate to privacy, according to the Cloud Security Alliance.
- Swedish data protection supervision authority *Datainspektionen* created a precedent in June 2013 by prohibiting Salem municipality from outsourcing personal information to a cloud service due to insufficient data protection procedures.
- Edward Snowden revealed organized personal data breaches conducted by US government agencies. As a result privacy protection officials in the EU recommend end users improve their awareness of privacy and avoid choosing services from non-EU countries.
- Independent studies conducted in 2011 and 2012 indicate that a majority of customers consider their personal information to be "very important". They are concerned about companies handling their personal data. Most importantly many customers object to their personal information being shared with third parties.
- Americans lose around $500 - $1,500 per identity theft case. This amounted to $1.52b in 2011, according to the Federal Trade Commission. The estimates for Europe indicate even higher costs, from €1,500 to €20,000 per case.
- The EU is currently updating their data protection directive to cope with emerging trends on the Internet, clarify existing legislation and strengthening individual rights.

In light of such facts we think it is reasonable to assume that privacy and personal data protection require attention in order to reduce the risks associated with outsourcing services.

While outsourcing remains important for business, we see many companies struggling to determine what, if any, part of their operation they can outsource, and to which suppliers. Protecting personal data is often put forward as a barrier that hinders or delays successful outsourcing. Overcoming this barrier is often beyond companies due to the inherent complexity involved.

Failure to implement privacy and data protection correctly can result in severe legal, economic and reputational penalties. Legal consequences in Europe have ranged from liabilities and fines to a ban on processing personal data, as seen above. We also see that the costs of reactive restoration and mitigation following a privacy incident are significantly higher than proactive privacy investments. Most importantly for companies is that privacy incidents lead to a loss of customer trust, resulting in reduced business or customers opting instead for a competitor's service. In the worst cases we have seen boycotts by customers until privacy omissions were corrected.
So, how is the legal situation changing at the moment? What should an organization do in order to preserve the business case for outsourcing? What should be considered before outsourcing personal data?

This whitepaper provides you with some answers. It will show you Deloitte's framework that can help your organization in succeeding with outsourcing while staying privacy friendly.



Privacy and data protection: "What's the difference?"

Privacy is a fairly subjective concept. It is primarily a human perception of what belongs to one's personal sphere. This perception is highly individual, depending on circumstances and cultural background.

The latter is important to consider for organizations that act internationally or face a broad ethical spectrum in their own country. As an example we can take the apparently similar Baltic Sea Region with notable differences in privacy perception – a low consideration in Sweden, a high consideration in Finland and the historical rooted fear in the Baltic States, based on culture and history.

In addition, we see that privacy perception changes in line with circumstances such as context, control feeling and the passage of time. For example, an individual may be reluctant to provide personal data to a census poll – perceived in a *big brother* context without any control – while happily sharing intimate personal details via Facebook – seen as a private context with the possibility of control. Another example is that customers accept loyalty cards from their local supermarket – an easy-to-grasp context with a perception of control – while they object to online profiling – a virtual environment with an uncertainty of control.

We see that many individuals are surprised that *the Internet never forgets*. People are used to information about them being forgotten over time. If that does not happen and they are, at a later date, confronted with information relating to them (especially about their past behavior) they find this an infringement of their privacy.
When it comes to privacy, it is the individual's perception that counts (even if perceived as counterintuitive by others). This can give the impression to an observer that privacy requirements are inconsistent while, in fact, they follow rules only perceivable for each individual.

Unfortunately, such individuality presents organizations with a level of uncertainty which must be considered when dealing with privacy concerns. Over time it has been established that the privacy perception and the feeling of fair privacy treatment are influenced by the following key aspects:

- how information enters and leaves the individual's sphere;
- how the processing of such information is controlled; and
- how personal data are communicated between third parties.

With that knowledge, the concept of the legal term *data protection* was created, to provide some legal definition to the uncertainty around individual concepts of privacy. Data protection is fairly well defined as the protection of personal data.

However, some uncertainty around this definition remains, especially with regards to *identifiable* data – i.e. data which can be directly connected to an individual. For example, an identifier such as a social security number may not necessarily be considered personal data, but will make any other kind of data it relates to personal.

As a result, the need to protect personal information becomes dependent on the impact data processing has on the individual.

The new EU regulation: "Clarifying the spirit of the law"

Unfortunately, many critics of outsourcing jump to the conclusion that personal data protection poses an insurmountable obstacle to outsourcing, despite the explicit goal of the EU to *guarantee the free flow of personal data*. We consider that the legislation is designed to clarify under which conditions personal data may be processed and outsourced rather than preventing it altogether.

As the title of this whitepaper already indicates, the EU Commission has started to update the Data Protection Directive 1995. Their goals are to modernize the legislation to cope with emerging trends and to clarify legal *grey areas*. Although the legislation is not finalized, we consider that it is already relevant to many organizations, since it clarifies the spirit of the original law and many privacy policies commit an organization to not only follow the letter of the law but also its spirit.

In order to understand the impact of the new proposal let us dig deeper into some of the changes. A summary of resulting requirements for outsourcing can be found in Figure 1.

Lawfullness of processing

An important idea introduced by the Data Protection Directive 1995 is that data processing is permitted if:

- it is performed for a legitimate reason;
- it is bound to a specified purpose;
- it is not excessive;
- it is performed only as long as necessary; and
- it has a clearly assigned responsibility of protection.

Furthermore the original directive states that if the *data subject*, the individual to whom the personal data refer, gives explicit consent, then data processing becomes legal even if the requirements above are not met.

The new draft clarifies this point by specifying how this explicit consent should be acquired and when it can be rightfully assumed that it was given.

Data subject rights

In order to give the individual control, which is an important factor for privacy perception, the law-maker has defined specific rights.

1. It is the duty of the controller, the legal entity that defines the purpose, conditions and means of processing personal data, to give the data subjects access to their data.
2. The data subjects have the right to request correction of any errors.
3. Data subjects have the right to request that their data be forwarded to a new service provider.
4. Data subjects can request to be forgotten, under the condition that the data is no longer required for other purposes. It is explicitly clarified that this is not a mechanism for the data subjects to erase old failings, which should be difficult based on the exceptions given, but rather a mechanism to allow a data subject to remove data traces in the Internet.

Lawfulness of processing

- Personal data list with processing purpose
- Data subject consent acquisition
- Data subject rights
- Mechanisms to retrieve, provide, correct, purge and forward personal information
- Electronic means to communicate with data subjects
- Controller obligations
- Assignment of data protection responsibility
- Internal control and audit procedures for personal data processing
- Personal data risk assessment method
- Documentation infrastructure
- Enhance incident management for privacy breach reporting
- Internationalization aspects
- Control location of outsourcing partner
- International organization plan location of personal data processing

Figure 1: Some legal requirements from new EU regulations

Controller, joint controller and processor

As already mentioned an important entity is the *controller*. Controllers are required to ensure data protection by design and by default. This means that the controller is obliged to follow the provisions of the law, including the following requirements which have been added or updated in the new directive.

An interesting update, especially in relation to outsourcing, is that a controller may now share the responsibility with a joint controller if the other legal entity participates in defining purpose, condition or means. This is meant to clarify a legal *grey area* where a contractor to the controller, especially service providers that handle employee

data, has insisted on being classified as data processors, without any data protection responsibility.

Also interesting for outsourcing is that the controller now has increased obligations to confirm compliance by regularly reviewing control and audit activities of the processor (i.e. outsourcing provider).

Another area that received clarification is security. The emphasis on a risk-based approach has been strengthened. The controller is responsible for performing and maintaining a systematic and extensive risk analysis. The risk is defined by the impact of the processing on the protection of personal data. Subsequently, data protection controls to prevent unauthorized disclosure, reading, copying, modification, erasure or removal, are chosen based on the risk level. This has increased the business focus and introduced proportionality.

Further, the legislation has introduced responsibility to create and maintain documentation for various areas. The controller is required to create documentation describing their compliance with data protection legislation. In the case of using a processor the controller must produce additional documentation describing the purpose, conditions and means with which the processor is employed.
In case of a personal data breach the controller is now obliged to inform the data subject and the relevant supervision authority. In addition a processor is responsible for informing the controller of a breach.

Finally, when it comes to fines for data protection violations by the controller the EU commission felt that the amounts were not sufficiently discouraging. The new regulation therefore will introduce fines ranging between 0.5 % and 2 % of global annual turnover.

International perspective

An area that has received a lot of attention is the interaction with countries outside the EU. The territorial scope of the new legislation has increased by covering not only controllers and processors residing in the EU but also any who provide data processing to data subjects in the EU. If a controller resides outside the EU the controller must have a representative inside the EU that takes responsibility. Furthermore the EU commission has clarified that violations by controllers will also be prosecuted outside the EU jurisdiction, although then according to local legislation.

It has further been clarified that data transfers to third countries shall be only possible in future if adequate legal protection can be assured. National legislation is the preferred criteria. The commission will establish a list of approved countries, where such protection exists, and also a list of countries where the protection is inadequate, which shall result in a prohibition of transfer. Organizations residing in countries which are on neither list must include standard data protection clauses to make transfer permitted.
The EU commission has explicitly stated that when the new legislation is introduced, the Safe-harbor agreement will become void. This agreement previously allowed personal data to be transferred to compliant organizations in the US. In the future, such a transfer will require explicit contract clauses with relevant organizations.

Privacy investments: "Where is the business case?"

A natural question is whether there are good business reasons for privacy investment, or if privacy is just a burden on the outsourcing business case.

In our experience most business case investigations focus only on legal compliance obligations. Privacy protection, or more correctly data protection, is then seen primarily as an unwanted cost and hence a burden. However, many asset valuation schemes indicate that personal data often represent an organization's most important assets – customers and employees. As a consequence it is asset protection that needs to become part of the business case. This implies a more bearable burden – although still a burden – as it relates to a benefit.

In fact, we have found that privacy investments act as a business enabler, or rather that a lack of privacy investment acts as a *business preventer*. This means the level of investment will have a direct impact on the attractiveness of a service to customers. The EU commission goes so far as to suggest that data protection investments can act as differentiator between various suppliers and must hence be considered a competitive factor.

Direct Damage

- Customer loss
- Data corruption or loss
- Restoration damage

Recovery cost

- Investigation cost
- System correction cost

Legal damage

- Court cost
- Fines & Penalties
- Liability

Reputation damage

- Brand value
- Marketing cost

Figure 2: Damage types for privacy assets

Privacy investment for asset protection

As mentioned above, personal data is an important intangible asset for most organizations. Some companies, such as Google or Facebook, rely completely on personal information for their business case. Obviously it varies by industry, but for many companies personal data is such an important asset that they must manage the risks around personal data protection.

The difficulty with assessing and managing personal data risks is twofold. First of all, any damage is primarily suffered by an individual who is usually someone other than the one responsible for assessing the risk, and will have their own interpretation of the valuation of that damage. An organization may be inclined to reduce the risk damage to the loss of the customer, but such a simplification neglects the legal cost, restoration costs and most importantly reputational damage.

Secondly the associated threats, vulnerabilities and their likelihood have the same problem as typical security risks – they are extremely volatile and require substantial experience to be estimated. Applying these elements to outsourcing adds an extra dimension of complexity but is essential, although retaining such competence in-house is often overly expensive.

Privacy investment as a business enabler

It has been promised many times, especially by privacy experts, that privacy would be a good selling point. However, until now we have not seen large financial profits from privacy related services. The willingness to pay for privacy has been low. We have, on the contrary, seen that service consumption has frequently superseded privacy concerns. It seems though that this trend is declining. More and more users choose another service or abstain completely if they consider their privacy is likely to be compromised.

We have also seen customers demanding privacy related improvements to services, such as the massive protests Facebook and Google have faced which forced them to reconsider changes to their privacy policies. These protests directly impacted parts of their business models and generated bad publicity, loss of customers and corrective costs.

However, most importantly, we have seen that services and products have been unable to realize their full market potential or have even become a business failure because of mistreatment of privacy. Notable cases are German Railway's *Bahncard* which was withdrawn after acquiring only about 15% of the projected market potential, or RFID tags in supply chain management of Benetton, a clothing retailer, which had to be disabled. Both business cases were derailed after a lack of focus on privacy expectations.

Recent studies indicate that the concern for privacy is increasing – see Figure 3. Users feel less and less in control of their privacy. We also see increased user numbers in (free) privacy services, especially in the aftermath of the revelations by Edward Snowden. This is a

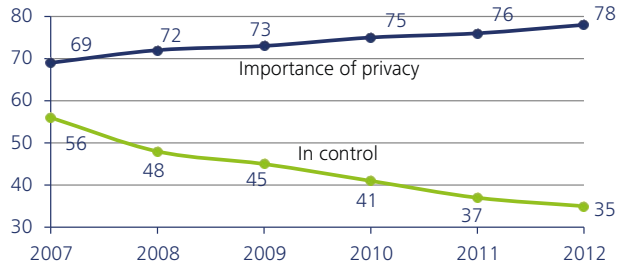


Figure 3: Percentage of data subjects feeling privacy is important and in control. Source: Ponemon Institute, 2013

clear indication that customers are actively changing their behavior. Although it does not necessarily lead to the conclusion that users will be willing to pay for privacy, companies which do not include a focus on privacy will see customers who are even less inclined to share their personal data and will either not become customers at all or will leave for more privacy friendly competitors. This means that privacy investment becomes a business enabler, a hygiene factor, which if it is ignored will inhibit the growth of the business.

Experiments have shown that around on in four in the customer population is privacy conscious, approximately one in two adapt their behavior according to the perceived threat and around one in four is considered insensitive. Combined with the increased privacy concerns voiced by customers this may mean that a privacy-friendly service could positively attract up to 75% of the customer population, providing an opportunity to gain a competitive advantage.
The important conclusion is that an organization should include their position on privacy in their strategic planning and adapt the organization accordingly.

Privacy and the outsourcing business case

We have put forward that considering privacy makes good business sense generally. But how does it influence the business case for outsourcing?

Outsourcing promises cost savings in the long run due to, among others, superior technologies, expert knowledge and economies of scale. It also transforms fixed costs into variable cost. Obviously there are also a number of pitfalls, for example, *the lock-in* challenge where an outsourcing partner cannot be changed resulting in cost increases over time.

On the positive side, an outsourcing partner may already have data protection competence or can at least distribute the associated costs over several customers. When it comes to keeping the control and legal compliance evidence updated an outsourcing provider may find it easier to reduce the costs. On the legal side an advantage can be that responsibility for data protection is shared or delegated to the outsourcing provider. And finally one important advantage we have seen is that a reliable outsourcing provider is likely to build up trust in the public which in turn increases the trust for the own organization.

On the other hand, the effect of privacy requirements is that additional costs in the long run may emerge due to additional privacy/data protection related requirements, the need for producing data protection documentation and performing regular internal audit activities. Most importantly, though, is that privacy requirements may reduce the amount of viable outsourcing partners, leading to an increased danger of *lock-in*.

It is frequently acknowledged that in the short term additional investments and costs have to be taken. We have seen for example that internal processes have to be adapted, existing internal control infrastructure must be changed and a migration activity has to be performed. In particular the execution of the latter can have significant cost implications.

In our experience this means that privacy increases the delicacy of the outsourcing endeavor. The break-even point may be achieved slightly later as additional investments are necessary. However, there are a number of benefits, especially sharing the costs for privacy controls, the competence advantage and trust benefits, that can be realized. The challenge for an organization is to get it right from the beginning. Simply relying on outsourcing providers, even if they are recognized for their privacy competence, is in our experience not enough. The risk for biased recommendations is not inconsiderable and the internal adaptations require attention from competent and experienced people in order to succeed.

Increase of costs

- Additional requirements
- Reduced number of viable outsourcing
- partners
- Maintaining documentation
- Internal control infrastructure
- Legal and contractual challenges

Decrease of costs

- Data protection competence outsourced
- Costs for technical and security controls
- can be spread out
- Obligations and liability delegated
- Reliable partners increase customer trust
- Maintenace of legal compliance

Figure 4: Cost drivers and advantages of privacy for the outsourcing business case

Outsourcing personal data: "How to prepare for it"

Undoubtedly, the business case for outsourcing is changed by privacy and data protection considerations. So, what are the key challenges in preparing for outsourcing?

In our experience nine common challenges have to be investigated. As a comment we would like to add that these processes are in order but should be understood as iterative rather than sequential.

1. Identifying (personal) data, processes and services to be outsourced
2. Reviewing legal, regulatory and contractual restrictions on outsourcing personal data
3. Assessing data protection risks
4. Defining privacy, security and compliance requirements
5. Defining technical and organizational controls satisfying the requirements
6. Assessing potential outsourcing partners for competence, capabilities and means to comply with the requirements
7. Assigning responsibilities for control implementation
8. Modifying privacy and security policies
9. Aligning internal control capabilities to assess and monitor the service provider

We have found that despite the claims of outsourcing providers, preparing and defining privacy risks and requirements is an activity best addressed internally. Our view is that only after defining the requirements is it reasonable to start a request for information (RFI). This should not mean that the supplier cannot provide input, but the mindset should be that the requirements can and will change based on supplier feedback.

The next activities, defining safeguards and agreeing with the supplier about implementation and responsibility, are naturally solved together with the service provider. Again, some service providers prefer to take control here but our view is that the organization is best served to stay in control. The factor that typically discourages an organization from leading this activity is a perceived lack of competence. Our recommendation is to get help from an independent third party rather than relying too heavily on the supplier, to avoid a conflict of interest between the best solution for the client and the self-interest of the supplier.

Finally, performing the policy modification and internal control adaptation are the last activities before outsourcing, since these are extensive changes that should not been done too frequently.

Contractual considerations

A second area for consideration in preparation for outsourcing is the contract. Obviously partnership with the supplier is the desired outcome, but there are legal obligations and considerations that require attention in a contract. Without doubt each case is different and will depend on the local legal framework, however, the aspects in Figure 5 are those which are typically found to be important when drafting an outsourcing contract.

- List of personal data transferred with an enumeration of the processing purpose
- List of controller(s), processors and sub-contractors
- Ownership of the personal data during and after processing
- Data retention obligations and rights
- Reference to requirements
- Audit rights during the contract and data retention time
- Standard data protection clause from legislation
- Delegation of the documentation obligations

Figure 5: Data protection content in the contract

The list of personal data with there processing purpose and the list of controller(s), processors and sub-contractors will be unique for each contract. The remaining items are generic in our expierence and can be reused for all outsourcing endavours.

Deloitte's Framework: "Outsourcing with privacy in mind"

Dealing with privacy can hardly be guided by financial parameters alone. We believe that in order to succeed the motivation for privacy must be rooted in the strategy, culture and structures of an organization. A privacy policy must not only address the legal issues but should also describe an organization's attitude towards privacy and personal data protection. Naturally, responsibility for privacy does not stop at the highest level but needs implementation throughout the tactical and operational plain.

Given the non-trivial nature of many privacy questions we have found that a structured and repeatable approach addressing various dimensions is needed. Based on our experience we have developed a framework suitable to address the challenges we have outlined – and some more – in what we consider the most efficient and effective way. Figure 6 shows an outline of this framework.

The framework integrates the challenges of privacy perception with the business and economic questions an organization needs to answer and the legal and regulatory compliance demanded. A core feature of our framework is that it addresses those challenge areas and their interdependencies on operational, tactical and strategic levels. Especially on the operational level we find the integration of technological controls an important feature.

Based on our practical experience we have ensured that the framework integrates easily with existing organizational structures. This feature is critical for long term success and the capability to maintain privacy friendliness. We think that nobody is served by a one-time endeavor. An important feature is therefore that both the initial establishment and the long term maintenance templates and methods support iterative working.

Naturally we have aligned with common industrial best practices and the applicable parts of standards like the Common Criteria or ISO 27000 series.

With our framework we think that many outsourcing activities, which frequently concern personal data, can be conducted faster, more predictably and ultimately more efficiently. We are also convinced that the likelihood to reach the breakeven point earlier is increased. Naturally the framework is only part of the story as some data protection experience and knowledge is a good prerequisite.

If you would want to know more or need our help, please use the contact information overleaf.

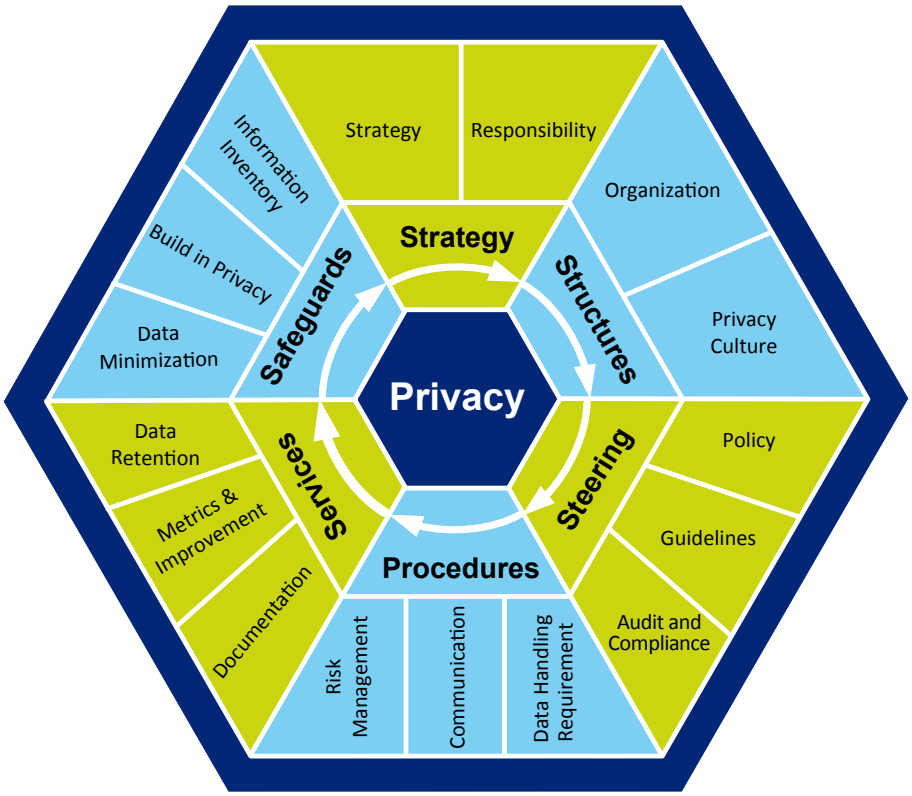


Figure 6 privacy framework

Contact

Marcus Sörlander
Partner
Enterprise Risk Services
msoerlander@deloitte.se

Albin Zuccato
Manager
Enterprise Risk Services
azuccato@deloitte.se