Privacy as a business enabler
From risks to opportunities
Contents

Privacy as a business enabler 5
Executive summary 6
Introduction 8
Use of personal data 9
Privacy legislation 11
Knowledge and awareness 13
Results Privacy Benchmark 14
Contact details 20
Privacy as a business enabler From risks to opportunities

Our Privacy team
Privacy is an important aspect of everyday life. Among consumers, there is a growing awareness that organizations use their personal data, and that this affects them. Therefore, organizations need to keep in mind that handling personal data responsibly is a necessity.

The largest common denominator of our clients is that they want to use personal data in an effective way. With every new product or service being launched, more information is coming in. Collecting personal data is vital for organizations to develop products and services, or to improve what they already offer.

However, the ethical aspect of gathering these data cannot be overlooked. If organizations are able to take privacy and security into account from the beginning of their processes and at every step of the way, this data can prove to be amongst the most important assets for organizations. Given the need for using personal data, there are many differences between organizations in the way they deal with privacy.

Because we are interested in our clients’ views on this, we have started a survey that we plan to perform annually. By gathering information from our clients and performing our analysis, we hope to add to both your and our knowledge on privacy. By doing this, we can make sure that privacy is a business enabler for every organization.

Enjoy reading our analysis, and I trust the results help you in gaining valuable insights!

Annika Sponselee
Head of Deloitte Privacy team
Privacy can only be captured in figures to a limited extent. To delve deeper into the underlying themes requires analysis and insight. In order to create this background for our results, we have spoken to a number of our client’s privacy professionals. We also conducted a survey on privacy, focusing on roles and responsibilities, capabilities and preparedness.

In many organizations, people need to be more aware of the necessity to use personal data responsibly. Recognizing risks is as important as seeing opportunities. We think it is essential to have a clear vision and strategy in order to balance the risks and opportunities. Almost 75% of the respondents in our review state that they are more focused on compliance than on enabling the creation of value using personal data, or that they are equally focused on these two topics. We believe that over the next few years a shift will take place, in which the value-creation becomes a primary concern for organizations as a whole.

Since using personal data gets more important for organizations, the need for senior management involvement grows with it. This goes beyond merely being supportive. Organizations that are successful in this field have management as a driving force to use personal data responsibly and ethically. The large majority of the respondents allocates responsibility at the legal department. Several organizations place privacy responsibility at the compliance department or at the business level.

As the benefits become more obvious, companies will become better at connecting and structuring their privacy organization: they have no choice. Privacy, of course, remains partly tied in with compliance. Although processes to maintain control within organizations mature, well-designed tooling to achieve privacy compliance is still lagging. Personal data is used throughout companies. This causes a need for tools that serve privacy, compliance and legal employees as well as the business.

We think that the introduction of new legislation creates a huge driver for organizations to revise the way they deal with personal data. We see in the market that the introduction of large fines in the Dutch legislation has drawn the attention of CFOs. Similar fines in the European Regulation will have the same effect across Europe. We welcome this attention, and at the same time warn for a perceived ‘chilling effect’ on innovation. We are still convinced that using personal data responsibly is possible – and necessary – after the European Regulation takes effect.
Data breach detection is a major issue. Processes to deal with breaches can be set up within a reasonable amount of time, but learning to notice when and where a breach takes place is tough. We see an increase in monitoring solutions and Data Loss Prevention measures to improve this. 57% of the respondents state that they have adequate security measures in place. Although this is one of the highest scoring responses, it still means that 43% are not confident that this is the case. An important conclusion that can be drawn from our interviews is that detection is a large issue: knowing when and where a breach has taken place may only become clear after the breach has become public. We believe that a combination of technical detection measures and employee awareness of what constitutes a breach will be vital to be able to respond adequately. There doesn’t seem to be a direct link between organization size (measured by annual turnover) and preparedness across the answers: the top two consists of the very large (>EUR 1 billion) and the smallest (<EUR 50M) categories. It is possible that large organizations have the funds to organize privacy well, and small organizations have the benefit of reduced complexity.

Finding professionals to deal with complex privacy topics is difficult. We have the same experience when hiring new people for our own fast-growing team. Because the topic covers an entire organization, you need communicative privacy specialists that can understand the perspectives of others in the organization. But not only privacy specialists need to be aware of these other perspectives. It is very important to also have IT, risk, security, compliance and business people see to it that personal data are used responsibly. This is important from top management through to operations. Strategies need to be designed and carried out. A hopeful thought is that this problem will solve itself over the coming years. The success of some very young entrepreneurs shows that they can be much more effective in getting value from personal data. We are looking forward to developments in the field, and we strive to play an important role as well.
Introduction

An important long-term objective of our survey is to create a workable standard to measure the state of privacy across the industry. This first year, we have started with short and simple questions about general topics. In the following years, we want to work closely with privacy professionals in the industry to design a tool that can be used to measure how everyone is performing and developing.

We are very much aware that privacy — like most topics — can only be captured in figures to a limited extent. To delve deeper into the underlying themes requires analysis and insight. In order to create this background for our results, we have spoken to a number of our client’s privacy professionals.

Using our Deloitte privacy strategy model, we came up with a number of general topics on which we asked our clients to give their opinions. We have combined their answers with our own insights to look at the main themes that come up: challenges, wins and contemplations.
Use of personal data

Innovative use of personal data takes flight
We promote optimizing the use of personal data. It can bring you closer to your clients and enables new products and services. As everyone now sees the value of personal data, they start to be used in ever growing quantities.

There are still risks though. Unchecked innovation can lead to incidents. Enthusiastic communication about the newest service that entails analyzing minute personal details is often not received in the same enthusiastic way.

Awareness of the need to use personal data responsibly should be increased in many organizations. Recognizing risks is as important as seeing opportunities. One of our clients states that, due to privacy’s subjective nature, this message can be difficult to convey consistently. We think it is important to have a clear vision and strategy in order to balance the risks and opportunities.

Almost 75% of the respondents state that they are more focused on compliance than on enabling the creation of value using personal data, or that they are equally focused on these two topics. We think that over the next few years a shift will take place, in which value creation becomes a primary concern for organizations as a whole. However, it is still possible that many privacy professionals will keep focusing strictly on adhering to the rules. We think that an effective privacy department should focus on enabling value creation, although this is only feasible in an organization with a high base level of awareness.

Only 34% of the respondents state that they apply Privacy by Design in their organizations. Paying more attention to Privacy by Design would help to reach this high base level of awareness, while leaving time for privacy professionals to help create value from personal data.

Using personal data responsibly is becoming a strategic topic
We have been saying for a long time that using personal data is a boardroom topic. Especially when it is at the center of innovation in your company. Many digital enterprises recognize this, particularly when their business revolves around their clients’ data. More ‘traditional’ organizations are exploring how to enrich their existing business models and how to get to know their customers better.

As using personal data gets more important for the organization, the need for senior management involvement grows with it. This goes beyond merely being supportive. Organizations that are successful in this field have management as a driving force to use personal data responsibly and ethically.
The maturity level still differs between organizations. As one of our clients states: a single individual at the highest level can have lots of influence on the importance given to privacy. Personal experiences may have a large effect. We think that these individuals are leading a wave of initiatives that will increase the need for strategic thinking about the position and direction of the organization. Other organizations will follow.

**Personal data use covers the entire organization: privacy departments need to connect**

Personal data is used in primary and supportive processes. IT enables its use through technology. Legal and compliance departments will advise on ways to stay within the bounds of privacy legislation. Security protects personal data. Everyone has a role to play, in addition to his or her other duties.

The way the topic is spread out is a risk. When everyone is looking from their own perspective, structure is needed to make sure there are no mistakes or missed opportunities. Dedicated privacy departments can play an important role in bringing everyone together. Short communication lines are important, especially when dealing with incidents and crises.

Several of our clients have stated that long lines and drawn-out organizations are detrimental to understanding privacy issues. A certain level of centralization of specialized privacy professionals is necessary, and everyone needs to communicate. An organization that heavily relies on strict chains of command faces the danger that an individual in the chain who does not see the value of privacy may cause a break.

Responsibility should still be allocated at the business end. Data users are responsible for their own actions, as they also reap the benefits. We think that as these benefits become more obvious, companies will become better at connecting and structuring their privacy organization: they have no choice.

**Simple tools are needed to control privacy**

Privacy is partly tied in with compliance. Although processes to maintain control within organizations mature, well-designed tooling is still lagging. Personal data are used throughout companies. This causes a need for tools that serve privacy, compliance and legal employees, as well as the business.

Because the business is ultimately responsible and provides a lot of information, several of our clients indicate that there should be simple tools for inexperienced users as well. Standard compliance applications may suit their intended audience well, but neither they nor we have encountered tools that take these multiple perspectives into account.

One of our financial clients states that these tools are indispensable in a mature organization. We agree, and we welcome initiatives to build and improve these tools. The focus for these tools should not be completeness, but facilitation and ease-of-use for all relevant roles in the organization. As one of our largest clients observes, this requires a substantial amount of privacy knowledge, in addition to the capability to build a well-functioning IT system.
**European legislation will have a large impact, and may provide clarity and consistency**

The European Regulation is in its final negotiation stages. Commissioner Jourová stated in Amsterdam that she wants to finish before the end of 2015. It will have the biggest legal impact we have seen in the field so far: stronger supervision, large fines, and larger allocation of accountability at companies.

At the same time, the Regulation can provide a clear and consistent approach across Europe. One of our clients in the telecom sector states that she would prefer a single European supervisor, instead of a connected system of local ones. She thinks that authorities will still use their own measures, which is especially difficult for multinational organizations. This would be a very worrying outcome, as one of the main reasons for introducing the new Regulation is to create a more level playing field than the current Directive provides.

We think that the introduction of new legislation creates a huge driver for organizations to revise the way they deal with personal data. We see in the market that the introduction of large fines in the Dutch legislation has drawn the attention of CFOs. Similar fines in the Regulation will have the same effect across Europe. We welcome this attention, and at the same time warn for a perceived ‘chilling effect’ on innovation. We are still convinced that using personal data responsibly is possible – and necessary – after the Regulation takes effect.

59% of respondents state that they are at least somewhat prepared for the coming General Data Protection Regulation. Although you could say that this is not yet possible due to the fact that the text is not yet clear, we think the response should be a bit more active. By building a solid framework right now, you are better prepared for changes in the future. The principles behind the legislation are clear and can be used to work towards the new legislation. A plurality (37%) states that they are fully aware of the expectations of their clients concerning the use of personal data. If you add that to the 35% that is somewhat aware, you get a large majority of 72% that is at least somewhat aware of their clients’ expectations. Because we only see a limited amount of extensive programs where clients are asked what their expectations are, we are not completely sure if the assumption that you know what your client thinks is right.

**Data breach notification is a challenge to implement in time**

The well-known Dutch amendment to the data protection legislation takes effect on the first of January 2016. The implications of this amendment are huge. Its main consequences are that organizations may need to notify the authorities and/or data subjects when a data breach takes place. What’s more, we can expect large fines by the Data Protection Authority of up to € 810,000, or even 10% of the annual turnover in extreme cases.

In several industries an obligation to notify data breaches already exists, notably in the financial and telecommunications sectors. We see high levels of maturity in these sectors. A telecommunications client did remark that the requirements for these sectors are not in
line with those for other organizations. The notification threshold is lower, which is difficult to defend when the same type of personal data is at stake.

In other industries there is still much to do. The short period between the publishing of the notification guidelines and the commencement of the data breach amendment, in addition to the hectic year-end closing for many organizations, are a risk to finish implementation in time. Some leeway from the Data Protection Authority would be appreciated. Organizations that are learning to deal with this new requirement should not be punished immediately.

Data breach detection is still a major issue. Processes to deal with breaches can be set up within a reasonable amount of time, but learning to notice when and where a breach takes place is tough. We see an increase in monitoring solutions and Data Loss Prevention measures to improve this.

57% of the respondents state that they have adequate security measures in place. Although this is one of the highest scoring responses, it still means that 43% are not confident that this is the case. Just like privacy, security is a fast-growing field. We are caught in an arms race with attackers, and we foresee that the topic will become even more important over the next couple of years. 52% state that they are able to detect personal data breaches. An important conclusion that can be drawn from our interviews is that detection is a large issue: knowing when and where a breach has taken place may only become clear after the breach has become public. We think that a combination of technical detection measures and employee awareness of what constitutes a breach will be vital to be able to respond adequately.

43% of the respondents is not confident that they have adequate security measures in place.
Privacy knowledge and awareness is hard to find
Finding professionals to deal with complex privacy topics is difficult. We encounter this problem when hiring for our own team as well. Because the topic covers an entire organization, you need communicative privacy specialists that can understand the perspectives of others in the organization.

But not only does a privacy specialist need awareness of these other perspectives. It is very important to also have IT, risk, security, compliance and business people see to it that personal data are used responsibly. This is important from top management through to operations. Strategies need to be designed and carried out.

One of our clients mentions that this awareness is progressing slowly. A possible explanation he gives lies in a generational difference. A large portion of the workforce, including top management, has seen the use of personal data increase only at the end of their professional careers. Familiarity with the associated risk and reward has not yet been ingrained in their functioning.

Privacy professionals state that increasing privacy awareness takes up most of their time.

A hopeful thought is that this problem will solve itself over the coming years. The success of some very young entrepreneurs shows that they can be much more effective in getting value from personal data. We are looking forward to developments in the field, and we strive to have an important role as well.
Results Privacy Benchmark

General information about the survey and its respondents
We have 75 respondents, all of whom we registered at the Privacy with a View event. There is an even spread across the industries (Consumer Business; Financial Services; Public Sector incl. Healthcare; Technology, Media and Telecommunications). Manufacturing, Energy and Resources is slightly underrepresented, with less than 10% of respondents. We had no responses from the Real Estate industry.

The respondents are almost equally from B2B as from B2C organizations. On average there are about 25,000 employees at the respondents’ organizations. There is a spread from 1 to 250,000. The majority of respondents are from large organizations (see Figure 1). The majority of respondents (approximately 50%) is from large organizations with revenues of over EUR 1B/yr (see Figure 2).
Roles and responsibilities

The large majority allocates responsibility at the legal department (see Figure 3). Several organizations place privacy responsibility at the compliance department, which we didn’t include in the standard answers. Several organizations also place responsibility at the business. In the interviews we held with our clients this was also mentioned: responsibility lies with the business, the privacy-related functions can have an advisory role. It may be worrying that 10% (7 respondents) have not allocated the responsibility for privacy at all. These are mostly smaller organizations, but also contain two organizations with a turnover of more than EUR 500M. Legal, security and IT are the departments where privacy is usually handled, as expected. To a lesser extent, also marketing & communication, a separate privacy department or other departments are involved.

The median number of employees working on privacy in the respondents’ organizations that answered this question is 4FTE. The spread is very large: in one case over 100FTE are working on the subject. The figures indicate that large organizations have significantly more employees working on the subject (about 10 for organizations with a revenue larger that 500M). We do not have sufficient numbers to get a solid statistic. The question addressed the number of FTE in the departments specifically tasked with privacy: it is possible that responsibilities in the business were not included in the count. Most privacy professionals are working on increasing awareness in their organization (53%). At the same time, many spend their time on creating new policies and procedures and increasing their own knowledge. This can be explained by the facts that the field is still developing, the context is changing fast and these tasks take up a lot of time.
Figure 4. I am confident that my organization...

- Has sufficient insight in which personal data are being processed for which purpose.
- Applies Privacy by Design principles to new initiatives (e.g. through Privacy Impact Assessments).
- Has notified the DPA of our relevant data processings.
- Is able to detect data breaches.
- Is able to deal with data breaches in accordance with the Dutch Data Breach Notification requirement, including timely notification of the DPA and data subjects.
- Is able to provide information on the personal data processed to data subjects.
- Is able to deal with objections to processing personal data.
- Informs data subjects effectively about the processing of personal data.
- Has adequate security measures in place.
- Controls the processing of personal data by third-party processors.
- Controls international data transfers.
- Is able to retain and destroy personal data in accordance with the applicable data retention periods.


**Privacy capabilities**

Almost 75% of the respondents state that they are more focused on compliance than on enabling the creation of value using personal data, or that they are equally focused on these two topics. We think that over the next few years a shift will take place in which value creation becomes a primary concern for organizations as a whole. It is still possible that privacy professionals will focus on adhering to the rules though. We think that an effective privacy department should focus on enabling value creation, although this is only feasible in an organization with a high base level of awareness. Only 34% of the respondents state that they apply Privacy by Design in their organizations (see Figure 4). This is an interesting result, as 59% of the organizations state that they are (somewhat) prepared for the General Data Protection Regulation, which will probably take effect somewhere in the next couple of years. Privacy by Design is an important part of the principles behind the Regulation: these organizations will need to work on this before this legislation takes effect.

57% state that they have adequate security measures in place (see Figure 4). Although this is one of the highest scoring responses, it still means that 43% are not confident that this is the case. It’s a good sign that 52% state that they are able to detect personal data breaches (see Figure 4). Security, just like privacy, is a fast-growing field. We are caught in an arms race with attackers, and we expect the topic to become even more important over the next couple of years.

An important conclusion that can be drawn from our interviews is that detection is an issue: knowing when and where a breach has taken place may only become clear after the breach has become public. We think that a combination of technical detection measures and employee awareness of what constitutes a breach will be vital to be able to respond adequately. Lowest scoring is the data retention and destruction capability. In the public sector, which includes healthcare in the survey, none of the 16 respondents were confident that they were ready to retain and destroy data in accordance with the applicable retention periods. ‘In the field’ we also see that this is an enormous issue. Many systems were not built with data destruction in mind. We see a development where retention is being built into underlying architecture models, but legacy systems will still be in use over the coming years.

We encourage everyone to keep on working on the basis to try to solve this issue in the years to come. In addition, destroying the highest-risk data should be a priority. Outside of the data retention issue, there are no major differences in the assessment of privacy capabilities on the specific topics, i.e. a lower score in general means a lower score on the individual topics. If we look at the total scores for the different sectors, the Financial Services industry gives itself the highest score on privacy capabilities. We see that this sector is generally mature on compliance topics. Manufacturing, Energy and Resources gives itself the lowest score. This is also typically the sector that has limited processing of personal data, which may be an explanation.
Privacy preparedness
59% of respondents state that they are at least somewhat prepared for the coming General Data Protection Regulation. Although you could say that this is not yet possible due to the fact that the text is not yet clear, we do think now is the time to make preparations. By building a solid framework right now, you are better prepared for changes in the future. The principles behind the legislation are clear and can be used to work towards the new legislation. The fact that no less than 41% of respondents is unsure, or hasn’t yet prepared at all, merely stresses the need to start taking measures as quickly as possible. We recommend that they act now, to prevent surprises when it’s too late.

A plurality (37%) states that they are fully aware of the expectations of their clients on the use of personal data. If you add that to the 35% that is somewhat aware, you get a large majority of 72% that is at least somewhat aware of their clients’ expectations. Because we only see a limited amount of extensive programs where clients are asked what their expectations are, we are not completely sure if the assumption that you know what your client thinks is right. We recommend organizations to assess this thoroughly and base their strategic decisions on the outcome of that assessment.

There doesn’t seem to be a direct link between organization size (measured by annual turnover) and preparedness across the answers: the top two consists of the very large (>EUR 1 billion) and the smallest (<EUR 50M) categories. It is possible that large organizations have the funds to organize privacy well, and small organizations have the benefit of reduced complexity. It would be very interesting to compare funding for privacy departments with effectiveness. We haven’t asked questions about funding for privacy though, as we feel this is very difficult to estimate across an organization in a simple survey. Almost a third of respondents state that they are not confident that they control international data transfers. Given the recent developments, e.g. the decision that Safe Harbor certification is not adequate anymore for transfers to the US, this does not come as a surprise. The same goes for outsourcing to third parties. The developments in this field warrant attention. Over the next months, we hope a (semi) permanent solution will come in sight.
A typical midsized and larger organization has 4 FTE tasked specifically with privacy.

Of privacy professionals does not think their organization is ready for the European Data Protection Regulation.

Of privacy professionals is not confident in their organization’s data protection measures.
Contact details

If you would like to have more information on this survey or privacy in general, please contact one of us. We are more than happy to help.

**Annika Sponselee**
Head of Deloitte Privacy Team
Deloitte Risk Services
Gustav Mahlerlaan 2970,
1081 LA Amsterdam, The Netherlands
+31610999302
ASponselee@deloitte.nl

**Bart Witteman**
Manager Privacy
Deloitte Risk Services
Gustav Mahlerlaan 2970,
1081 LA Amsterdam, The Netherlands
+31683330029
Bwitteman@deloitte.nl
Privacy as a business enabler
From risks to opportunities
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.nl/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 210,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2015 Deloitte The Netherlands