The Return to the Customer: Three Strategic Choices of Privacy Management

Esmee van Caspel MSc and Marjolijn Honcoop MSc

With the recent changes in rules and regulations, and academics stating that privacy is confusing, it is not a surprise that implementing effective privacy management is not an easy activity in practice. For organizations, there is no one-size-fits-all or best practice approach. This is shown by the many frameworks available and many questions posed by organizations. Organizations have given us insights into their privacy management, and revealed an interesting trend: privacy becomes about the individual again.

E.J. van Caspel MSc
is a senior consultant at KPMG IT Risk Consulting.
vancaspel.esmee@kpmg.nl

M. Honcoop MSc
is a senior consultant at KPMG Cyber.
honcoop.marjolijn@kpmg.nl

Introduction

Ever wondered what the fuzz surrounding privacy is all about? It is all a result of rapid technological developments and changing privacy regulations. Rapid technological developments have provided us the opportunity to collect, store and distribute information via all sorts of digital technologies. As a result, a lot of personal information has been made digitally available: your taxes, your medical history and your expenses, to name but a few (see Figure 1). You can store your data in the cloud and access it via your phone, regardless of your geographic location. Organizations have embraced this development to offer new services such as cloud storage, block chains and virtual reality. Not only to the end user, but also to their own employees, in terms of an online environment to consult their paycheck and change the information of their place of residence, for example.

But these opportunities come with the risk of violating the fundamental rights of the individual when systems are breached and personal information falls into the wrong hands. Governments try to protect these fundamental rights of the individual by tightening the privacy rules and regulations. With the frequent changes of the last years, it is not a surprise that implementing effective privacy management is not an easy activity in practice. It is becoming more and more of a struggle for organizations to comply with the changing privacy rules and regulations. Some of the struggles organizations may be faced with are setting up an incident response procedure, the reporting of breaches or the design and implementation of a clear and transparent communication process.

The privacy of the individual is subject to many rules and regulations of which the upcoming General Data Protection Regulation (GDPR) might be the most important one. Research conducted by the International Association of Privacy Professionals (IAPP) and TRUSTe reveals that 60% of the organizations participating in their study are very concerned about the upcoming GDPR (see Figure 2). To understand why these organizations are concerned, we need to understand what risks organizations face when their privacy management is not sound.

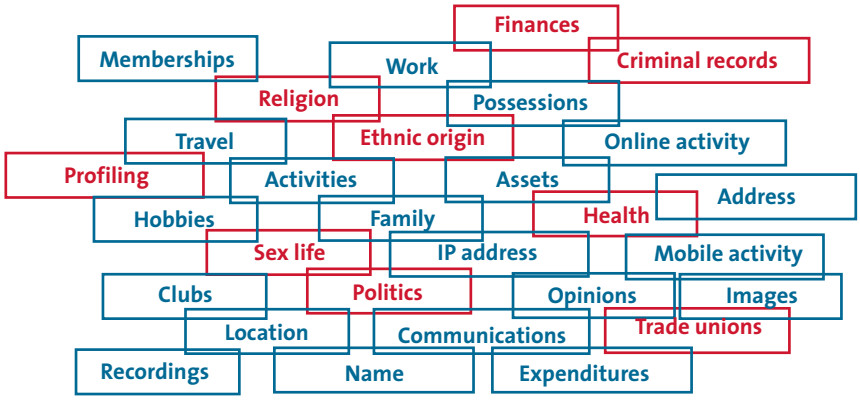

Figure 1. **EU Regulation (2016/679): examples of personal information (red indicates sensitive personal information).**

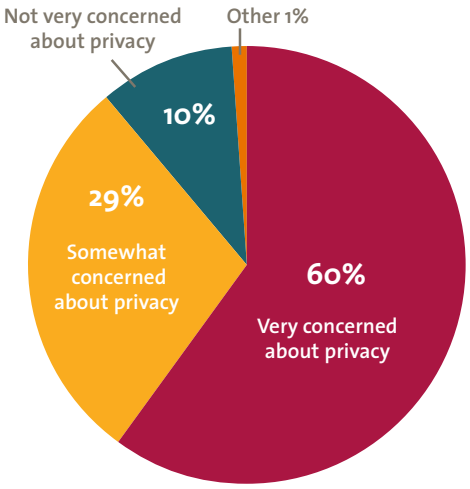

Figure 2. **Concerns of organizations regarding the GDPR (www.iapp.org).**

What Are the Organization's Risks?

To answer this question, a study was conducted in the Online Services sector – a sector which exists solely because of the online market and is characterized by a high online presence. The focus of this study is the personal information of customers. Many of the online organizations easily collect more personal data of their customers than required and have to step up their privacy game in order to remain compliant. Even more important, as the privacy awareness of customers grows and competition is fierce, these organizations have to manage privacy effectively in order to gain the customer's trust and leverage privacy as a unique selling point.

When privacy is not effectively managed, it can have various consequences. Perhaps most obvious, a data breach can occur where the organization loses personal data to a hacker, a disgruntled employee or a script kiddy. Additionally, in many countries the authoritative bodies are competent to conduct research into organizations if they have a reasoned assumption of misconduct. Both events can most importantly result in legislative penalties, erosion of brand and reputation, and increased surveillance of an authoritative body.

Legislative Penalties

The risk of legislative penalties is easy to understand: when an organization does not comply with the privacy rules and regulations of the country, an authoritative body may decide to fine the organization. In 2016, the new General Data Protection Regulation has been ratified which will come into effect in May 2018. If by that time organizations do not have their privacy management sorted out, the authoritative body may fine the organization with a fine of up to 20,000,000 EUR, or in the case of a global enterprise, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. This makes the consequences of not having a sound privacy management directly quantifiable.

Erosion of Brand Reputation

The erosion of brand reputation is less quantifiable than a legislative fine. Many studies have been conducted to research the market reaction to a privacy breach. Privacy breaches have a negative impact on the market value of an organization: organizations lose out on business opportunities, their value on the stock market decreases, and individuals alter their buying patterns as they lose trust. Additionally, organizations are less attractive for employee candidates when the organization has been subject to a privacy breach.

Individuals, both customers and employees, have expressed concerns when it comes to collecting personal data (see Box 1). Individuals feel that an excessive amount of personal data is being collected and stored nowadays. They fear that data is being used for another purpose than originally collected for and that third parties are given access to this data. Because of these concerns and the vulnerable state an individual ends up in when providing privacy data to an organization, organizations are punished with lowered purchases and less job applications from employee candidates when they violate the individu-

al's trust. Though researchers question the sustainability of this change, the immediate result, at least in the short-term, is the erosion of brand and reputation.

Increased Surveillance

A third result is increased surveillance. Organizations that have been subject to research conducted by the authoritative body, or organizations that have been the subject of a data breach, pose a higher risk when it comes to the protection of personal data. As a result, the authoritative body of the country might decide to monitor the organization more thoroughly.

An example of increased surveillance by the data protection authority is the punishment that the Federal Trade Commission (FTC) imposed on Google and Facebook. From 2012 until 2032, Google and Facebook have to conduct ten privacy audits each per year to ensure their processes are according to standards of the FTC. This is a result of a research the FTC conducted after they received complaints about unfair processing and deceiving statements. Not only do these privacy audits cost a lot of money, it also harmed the reputation of both companies.

Why Are These Risks Becoming More Relevant?

Recent developments have caused the likelihood and the impact of these risks to be higher than before. Technological developments allow organizations to collect, store, and use more personal data. Compared to a decade ago, there is more information available, and even other types of information are available. For instance, not only your name and address can be found online, but your bank account is also stored digitally, as well as your mortgage contract and potentially even your medical history. Additionally, the speed of exchanging data increases rapidly, and the costs to store data decreases significantly. Hence, collecting and storing more personal data online thereby increases both the likelihood of a privacy breach, as well as the impact.

Another development that increases the impact of a privacy breach, are changing rules and regulations as a result of the upcoming GDPR. The new GDPR will come into effect on May 2018, but the organizations subject to this study have all expressed concerns when it comes to meeting this deadline. The most important changes of the new GDPR are bigger fines, an obligation to report data breaches, and a set of new requirements, including privacy-by-design and mandatory privacy impact assessments (see Table 1). The changes require organizations to assess their current data flows, and perhaps change their privacy related processes in order to remain compliant.

Individuals have expressed concerns when it comes to collecting personal data and it reflects an increase of privacy awareness. The market is reacting to these concerns. More and more solutions are becoming available that enable individuals to take matters into their own hands, and provide individuals with opportunities to protect their online privacy. From applications that generate complex passwords and that store these passwords in a digital vault (for instance: OnePassword or KeePass), and solutions that let users mask their personal information, such as e-mail addresses, phone numbers and credit card numbers when buying from an online retailer (for instance: Abine Blur) to solutions that let users use the Internet anonymously (for instance: Tor or Tor Browser). On top of this, more and more encryption solutions are becoming available for people to encrypt, for example e-mails and files, without having to understand cryptography procedures or techniques (for instance: Telegram).

Box 1. **Market reaction to concerns of the individual.**

GDPR Changes	
Change	**Description**
Higher fines	The GDPR introduces fines of up to 20 million EUR or 4% of global annual turnoaver, whichever is higher. In every country, a Data Protection Authority (DPA) is present to monitor and enforce.
Right to be forgotten	A change that has frequently been in the news, is the right to be forgotten. This is the right a subject has to have his data removed, so that information that is available from his past, cannot have a negative influence on the present, e.g. job applications.
Privacy-by-design	The GDPR requires organizations to already review their privacy during the design stage of a project. This decreases the chances that a system, process, or data flow is not sufficiently protected.
Mandatory Privacy Impact Assessment (PIA)	The GDPR requires organizations to carry out a Privacy Impact Assessment for systems, processes or data flows that are of high privacy risk. If the result of the PIA illustrates a high inherent risk, the data protection supervisory authority need be consulted prior to processing.
Mandatory DPO	The bigger organizations need to appoint a Data Privacy Officer (DPO). This DPO is employed by the organization itself, but should be independent enough to question the activities of the organization. The DPO role may be carried out by a service organization.
Data breach notification obligation	A data breach notification obligation has already been incorporated in Dutch law, but is now also included in the GDPR. This means that organizations must report data breaches to the DPA within a reasonable period of time.

Table 1. **Most important changes of the new GDPR for organizations.**

The Strategic Choices of Privacy Management

Organizations in the Online Services industry have cooperated in this study and demonstrated a scattered focus on their privacy practices. In general, the organizations focused on the process of collecting data, on the processing and retention of data, and on the disclosure to third parties. When going into details though, it became apparent that when it comes to customer's privacy, organizations adopt one of the three perspectives. Adopting one of the three perspectives is a strategic choice which has a significant influence on the course of an organization's privacy management. The first two strategic choices of privacy management appeared at an early stage and are widely known. However, over the course of the study, a fascinating third strategic choice emerged. Though this strategic choice is not widely known, it can be the unique selling point an organization is looking for in order to survive.

First Strategic Choice: Compliance Based Privacy Management

Compliance based privacy management strives to adhere to the rules and regulations. The organization finds ways to organize their privacy related processes in such a way that they will be compliant. Changes to privacy management are performed in an ad hoc fashion and only when changes in rules and regulations are being enforced by the authorities. An example of compliance based privacy management is informing individuals about their data which is being collected and for what purpose. Organizations are only allowed to collect an individual's data once the individual has been notified about these two aspects. In addition to this, a lot of organizations use one or more third parties to manage their data. In case this "outsourced" data encompasses privacy data, the organization is legally required to draft a processing agreement between themselves and the third party. This agreement has to adhere to certain requirements, one of which is the notification of a data breach. Once the third party has suffered a data breach, it is important that the first organization is notified about this breach, so they can make an estimation as to whether this breach is of such a nature that they have to adhere to the data breach regulation. Each organization is required to notify the Data Protection Authority once privacy sensitive data has been compromised.

The privacy rules and regulations are quite extensive. Making sure the organization is compliant to the numerous privacy related rules and regulations therefore encompasses a variety of tasks: informing individuals about the data collection and its purpose, drafting processing agreements, handling possible data breaches, appointing a Data Protection Officer and the disposal of data in a timely manner. This list is not exhaustive: the privacy regulation encompasses a lot more. It is believed that striving for a compliant based privacy management practice is not an easy task and the research conducted by IAPP and TRUSTe shows that 44% percent of the organizations are still struggling with this. However, striving for even more than just adhering to the rules and regulation, might render interesting results for the organization.

Second Strategic Choice: Risk Based Privacy Management

The second strategic choice of privacy management is establishing a stabilized and continuous process, which is well-documented and covers all aspects of privacy management. This strategic choice can be adopted after the organization has accomplished compliance with the privacy rules and regulations of its country and thereby has the opportunity to mature its privacy processes. With this approach, organizations will shape their privacy management based on the risks they have identified. This risk based approach will help organizations to determine priorities and allocate sufficient budgets for the program.

Risk based privacy management is characterized by certain traits and processes. In contrast to the ad hoc nature of compliance based management where privacy management is only altered when rules and regulations demand it, is risk based privacy management a state where the organization is in control of its processes and applies continuous improvements. Changes are not just a result of changes in rules and regulations, but mainly a result of a pro-active approach of the organization to manage personal data in an ethical manner. Self-assessments, privacy impact assessments and periodic reviews help the organization to maintain a pro-active approach. Additionally, getting certified for a privacy audit (e.g. Privacy Audit Proof) may help the organization to maintain this status and pro-actively identify points of improvement.

Another important trait of the strategic choice of risk based privacy management is communicating the sense and urgency of privacy throughout the whole organization. Organizations will set up a privacy awareness program to explain privacy to its employees and provide them with guidance how to act. Additionally, the organization

will have a whistle blowing hotline where employees can report malpractices anonymously. The organization can communicate its privacy policy throughout the organization as well by incorporating privacy policies in the HR processes. New joiners are informed about the privacy policies, and need to be made aware of the contents of the confidentiality agreement.

The organization has reached the strategic choice of risk based privacy management if their processes are mature, and the sense and urgency of privacy is well communicated throughout the entire organization. Improvements are not done based on changing rules and regulations, but based on a pro-active approach. It decreases the chance of identifying and implementing a change too late and thereby decreases the risk of a data breach or legislative penalty.

Third Strategic Choice: Customer Oriented Privacy Management

The first two strategic choices have been widely studied by various researchers. Though the second strategic choice is not easy to achieve, many organizations will establish a stabilized and continuous process and will thereby reach the state of risk based privacy management. For many organizations, risk based privacy management is then the end goal of their journey after which they maintain the quality of the processes, but do not improve further.

The first two strategic choices can be seen as "hygiene factors". Even though these choices may result in an effective privacy management with a minimum chance of risks, they are not easily visible to the individual. Organizations that want to make a difference and want to leverage privacy as a business enabler, need to meet or even excel the expectations of the individual, since this is what privacy is all about. When organizations have reached compliance and processes are effectively managed, they need to begin to strive for something more: a customer oriented privacy practice. This way of managing the privacy practice excels as it focuses on the concerns of the individual.

Research performed in 2016 by TRUSTe, a leading global privacy management organization, reveals that there are two ways to decrease the concerns of an individual when it comes to privacy: individuals having more easy tools to protect personal data and organizations being more transparent about how they collect data, and what they will use it for (see Figure 3). A customer-oriented approach is therefore characterized by the organization taking steps to increase transparency about the process of the processing of personal data and thereby meeting the expectations of the individual. The view of the organization switches direction from inside to outside. The organization focuses more on communication towards the customer: they simplify the text of the privacy notice and make it visually attractive. They do not tuck it away in some far corner of the website, but give it a prominent place on the website, or shape it in a comic right at the intro of an app. Additionally, the notice which is presented to the customer gets tweaked in a more customer friendly way. Organizations explain the purpose of the data collection not in text, but for instance in pictures or video, to improve the understanding of the customer (see Box 2). When choosing the second strategic perspective, organizations can use privacy certifications to identify points of improvement for their privacy management. When adopting the third strategic choice, privacy certifications are another way to be transparent to the individual and show the organization processes their data with due care.

Figure 3. **Two top ways to decrease concerns of the individual (www.TRUSTe.com).**

A customer-oriented approach is characterized by aiming at the understanding of the individual, supported by simplified texts and attractive visuals. Examples are not yet bountiful, but some great examples can already be found on the internet.

Windows

Windows has updated their privacy statement during 2016. Instead of a long plain text page, they have opted for a more visually attractive overview of their statement. The statement is divided into different topics, which are all displayed in a clear cube. Notable about the statement is that the text is formed around the individual. The individual is personally addressed ("how we use your personal information") and the statement is divided into questions which the individual might have.

The Guardian

The Guardian is one of the great examples. In clear and concise wording, they explain the highlights of their complex privacy policy, including essential principles as the purpose of the collection, proportionality, third party access and security. Their privacy policy is hard to understand for the individual, but their video explains it in simple wording. Together with the attractive visualization, the privacy policy is explained in an easy to understand manner. Everyone navigating to the website can view this video.

LinkedIn

LinkedIn goes a step further and supports its video with a webpage. It summarizes its privacy policy in three topics. These three topics are not only visualized in their video, but are also listed on the top of their privacy webpage. The video supports the webpage and the webpage supports the video. The video and the webpage refer to each other, together giving a complete overview to the individual. This makes LinkedIn another great example of the individual oriented approach.

Figure 4. **Privacy statement on Microsoft.com.**

Figure 5. **The Guardian's privacy policy explained in a video.**

Figure 6. **LinkedIn's privacy policy explained in a video.**

Box 2. **Examples of a customer centric approach.**

Organizations need to return to where it all began: the individual

For the third strategic choice, the customer orientation the organization adopts is key, focusing on explaining their privacy policy to customers as easily and conveniently as possible. The result is that customers value the transparency of the organization, their concerns decrease, and the reputation of the organization increases. Along with an improved trust relationship and possibly an enhanced reputation, there is a direct positive effect on sales as well. When the privacy policy is explained to the customer in an easy fashion, customers do not need to spend a lot of time reading. Spending a lot of time reading the privacy policy, which often contains many difficult sentences and jargon, can make the customer decide not to proceed viewing the website and the organization's offering. Simplifying the privacy policy thereby will have a direct positive effect on the sales of the organization.

Forrester acknowledges and specifies privacy as one of the ten critical success factors for organizations in 2016 (www.forrester.com). The customer-oriented approach is not required for a risk based privacy management, and is also not demanded by any law, though it gives the organization the opportunity to make a difference, decrease the concerns of the individual, and use privacy as a competitive differentiator.

Conclusion

Privacy can be become the leverage that Online Service organizations need to survive in the highly competitive world. Individuals are increasingly becoming aware of the risks associated with revealing personal data to organizations and it can be quite a struggle for organizations to protect this data and comply with changing privacy rules and regulations.

In order for organizations to protect and manage personal data with due care, they need to make a strategic choice. Three strategic choices in privacy management have been identified: they are not mutually exclusive and can be adopted simultaneously (see Box 3). However, for many organizations, the first choice in privacy management, is becoming compliant. As privacy laws are rather complex, this is not a step that should be underestimated and organizations should reserve sufficient time and resources to support this strategic choice. When compliancy has been achieved, risk based privacy management might be the next choice for the organization. This strategic choice is characterized by continuous and stabilized processes and priorities are based on risk assessments. The organization recognizes that rather than just avoiding fines, risk based privacy management adds value to the organization by maintaining the data at a high quality (which can have beneficial effects on marketing activities) and being in control of the processes to reduce risks. Third is the fascinating identification of a step towards the individual which many organizations are not yet aware of. As the individual is increasingly becoming aware of their privacy, changes are required in the privacy management of organizations to explain the privacy policy to the individual and build a trustworthy relationship. Organizations are then leveraging privacy as a unique selling point.

Organizations must realize that neither of the strategic choices is easy to achieve and many organizations are still struggling with adopting the first strategic choice. However, in highly competitive times and with individuals being more aware of their rights of privacy, privacy management can become the differentiator the organization needs to be successful. Only when the organization adopts a customer-oriented approach and is transparent about their privacy processes, can a trustworthy relationship with the individual be established and can privacy become

The sequentiality of the choices as presented is based on the observations in the Online Services sector. Many organizations might choose to steer their privacy management according to this sequence, as a compliance based approach provides a solid basis to build further privacy practices on. However, some organizations might decide to adopt them differently: an organization may choose for a customer centric approach in order to be transparent and aim for increased sales, while at the same time, the organization is still working on being compliant with the law. Non-compliancy is then combined with a customer centric approach. This results in the organization taking account of all measures that keep the individual well-informed, while behind the scenes, privacy management is not (yet) in order. This is a non-desirable state, as the solid basis resulting from being compliant is then missing. A customer-centric approach can therefore best be adopted simultaneously with, or following a risk-based approach.

Box 3. **Where to start**

the unique identifier the organization needs. Therefore, organizations need to return to where it all began: the individual.

This article focuses on privacy management: the risks an organization faces and the strategic choices an organization might consider when it comes to privacy. Privacy is also concerned with the use of IT and therefore (technical) security. If you want to read more about the relation between privacy and security, an interesting read could be Privacy By Design: From privacy policy to privacy-enhancing technologies in Compact 2011/0 ([Koor11]).

Box 4.

References

[Forr16] Forrester, *The 2016 Top 10 Critical Success Factors To Determine Who Wins And Who Fails In The Age Of The Customer*, 2015.

[Guar14] The Guardian, *Our privacy policy – a quick look* (video), 2014, https://www.theguardian.com/info/video/2014/sep/08/guardian-privacy-policy

[Koor11] R.F. Koorn and J. ter Hart, *Privacy by Design: From privacy policy to privacy-enhancing technologies*, Compact 2011/0.

[Link16] LinkedIn, Privacy policy, 2016, https://www.linkedin.com/legal/privacy-policy

[Micr16] Microsoft, Privacy statement, 2016, https://privacy.microsoft.com/

[Stew02] K.A. Stewart and A.H. Segars, *An empirical examination of the concern for information privacy instrument*, Information Systems Research, 13(1), 2002, pp. 36-49.

[TRUS15] TRUSTe, *Preparing for the EU General Data Protection Regulation*, 2015, https://iapp.org/media/pdf/resource_center/TRUSTe_GDPR_Report_FINAL.pdf

[TRUS16] TRUSTe, *2016 TRUSTe/NCSA Consumer Privacy Infographic US Edition*, 2016, https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/

About the Authors

E.J. van Caspel MSc is a senior consultant at KPMG Risk Consulting – IT Advisory with an interest in the human side of IT and the consequences it can have on everyday life. She believes people will become more and more privacy aware, which will cause customer-oriented companies to have to follow suit.

M. Honcoop MSc is a senior consultant at KPMG Cyber and focuses on questions organizations have when it comes to privacy. She is convinced privacy should not be a concern, but an enabler for organizations to build thrust among employees and clients. Trust provides organizations with new opportunities for services and business intelligence.