Building a privacy compliance programme is about successfully putting together pieces of a complex puzzle: privacy, data security, compliance, vendor management, outsourcing, process improvement, change management, and the company's culture, values, and priorities.

Does the following apply to your organization?

- We have identified our most critical personal data processing operations, we have assessed our legal obligations and meet our legal responsibilities;
- We have been able to identify compliance failures and privacy violations and to adequately address these;
- We are able to identify (in time) issues which could develop into compliance failures and privacy violations if not adequately addressed;
- Staff involved in processing personal data know their (legal) responsibilities and work accordingly;
- We are working in accordance with what we communicate through fair processing notices and privacy statements.

If one or more of the above mentioned questions is answered in the negative, then we seriously advise you to consider these topics.

PricewaterhouseCoopers

At PricewaterhouseCoopers Nederland, over 4,400 professionals work together from 19 offices covering various disciplines: Assurance, Tax and Human Resource Services, and Advisory. On the basis of our corporate philosophy, Connected Thinking, we provide sector-specific services and seek novel solutions. Not only for large national and international companies, but also for medium-sized and smaller businesses as well as for government entities and non-profit organizations.

As an independent part of a worldwide network comprising 130,000 colleagues in 148 countries, we can rely on extensive knowledge and experience which we share with each other, with our clients and with their stakeholders. We seek unexpected angles, make surprising connections, feel involved and work together from our strengths.

Contact details

If you wish to receive more information, discuss privacy issues or our services or if you have any questions, please do not hesitate to contact Daniëlla Goudswaard, +31 620 959 964 or Otto Vermeulen, +31 653 361 787.

©2006 PricewaterhouseCoopers. All Rights Reserved. 2005.11.01.01.199.

Your worlds Our people*

www.pwc.nl

Assurance •Tax •Advisory

*connectedthinking™

PRICEWATERHOUSECOOPERS

Privacy and Personal Data Protection.*

*connectedthinking™

PRICEWATERHOUSECOOPERS

Attention for privacy and the protection of personal data: necessities and opportunities. Attention is critical; not only because this is required by law, but also from a commercial perspective. Organizations depend on trust. Losing that trust may result in losing customers.

Inappropriate or unauthorised processing of personal data may damage relationships between customers and their suppliers, employees and their employers and citizens and government institutions.

Are you in control of the use of personal data?

Your clients and employees entrust their personal data to you. They rely on the fact that their data is handled in accordance with their expectations and with applicable laws and regulations. Your organization has taken various measures to protect personal data. But are you really in control of the use of personal data?

Ask yourself for example:

- Do we have knowledge of privacy violations and are we addressing these in an effective manner?
- Are we able to identify (in time) issues which could develop into privacy violations if not adequately addressed? Do we have insight into actual and potential weaknesses in our current data handling practices?
- Is everyone involved in processing personal data aware of their (legal) responsibilities?
- Are we meeting the expectations of those from whom we collect and process personal data? And do we know these expectations?

And:

- Are we aware of privacy related opportunities (e.g. web seal or privacy certificate)?

Do we use these efficiently to strengthen the relationships with those from whom we collect and process personal data?

Is your organization privacy sensitive?

All organizations process personal data. Although all should comply with legal requirements, organizations that can identify with one or more of the following points should review the quality of their privacy compliance program:

- Profit, revenue or success strongly depends on trust of stakeholders;
- A compliance failure or a violation of trust will have negative financial or reputational consequences;
- Financial personal data (such as loans, debts) and/ or sensitive personal data (such as medical data) is collected and processed;
- Personal data is collected on line or processed using complex and interrelated information and communication technologies;
- Data processing operations are (partly or completely) outsourced to third parties;
- Personal data is shared with other organizations (either third party organizations or companies that are part of the same group) outside of the EU.

Audit tool for EU based multinationals

EU based multinationals that would like to use a uniform, coherent audit framework, allowing for an efficient approach and enable audit results comparison between different country organizations, can use the “Personal Data Protection Audit Framework”.

The framework provides for a baseline personal data protection audit to help organisations (regardless of their type of business and size) active in the EU to establish whether their processing of personal data is in accordance with the principles of the EU data protection directive.

Besides guidance on the audit process, two sets of requirements are presented in this framework, namely a set of compliance requirements (is personal data processed in accordance with the principles of personal data protection) and governance requirements (‘governance’ is about the internal controls concerning organisation, process and technology which the organisation has implemented to ensure that personal data protection is addressed in a transparent, efficient and effective manner).

This framework has been developed by PricewaterhouseCoopers, under the supervision of CEN, in cooperation with several organizations (such as multinationals, supervisory authorities and law firms). The framework can be downloaded from www.cenorm.be/isss/cwa-dpp. If you have questions about the framework or if you are interested in an audit, please do not hesitate to contact us (see contact details).

Good privacy practices are critical to comply with legal requirements, and to build trust and maintain corporate reputation.

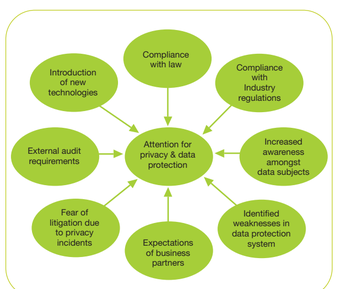

Fig. Drivers for privacy and personal data protection

Need for attention

Attention for privacy and personal data protection is important. Failure to protect personal data may lead to the following risks, among others:

- Legal sanctions (e.g. fines and penalties) instituted by government agencies;
- Harm to a data subject whose personal data is disclosed inappropriately;
- Damage to the organization's reputation and brand image due to e.g. adverse publicity (as a result of non-compliance or unauthorized disclosure of personal data).

The benefits of good privacy practices are for example improved data quality and increased trust, reduction in lost revenues arising from compliance failures or privacy violations and competitive advantage.

Most companies have long been aware of the importance of protecting (confidential) product and market data, but may have been less concerned about protecting customer and employee data. Privacy and data protection laws (such as the Dutch Data Protection Act, the Telecommunications Act) have changed that. Not surprisingly, the introduction of privacy and data protection legislation reflected an increased focus on data privacy, protection and security. The emphasis has shifted from merely protecting data against unauthorised use and loss of data to considering to what extent personal data may be collected and subsequently used.

A heightened awareness for privacy and personal data protection has recently arisen and is reflected in:

- Increased media attention: Over the last year an increasing number of privacy violations have been reported in various news media. Also, there have been several discussions regarding the question of what one can and cannot do with personal data.
- The introduction of new products: For example, CEN (the European standardization organization) published a personal data protection audit framework. See Audit tool for EU based multinationals.
- The introduction of the privacy certificate. See possibility for Dutch organizations to obtain a privacy certificate.

Globalization, identity theft, and a number of high profile data breaches, including a number involving vendors to whom personal information had been entrusted, have materially heightened the risks inherent in data ownership and management for organizations.

Helping our clients

Rapidly changing legislative, regulatory, legal, business, and technological environments in which organizations operate have led to new compliance risks and challenges for our clients. Control over these risks and continuously monitoring these challenges is crucial to maintaining a competitive edge in today’s global economy. PwC has helped clients worldwide in various sectors to meet these privacy and data protection challenges.

Assignments are e.g.:

- Privacy and data protection audits;
- Privacy certification;
- Privacy training for privacy / data protection / security / compliance officers;
- Privacy awareness programs;
- Design and implementation of privacy and data protection compliance and governance programs.

PwC approach

Where privacy and personal data protection are concerned, it is our experience that organizations tend to either push too far (resulting in formalistic approaches that no one wants and which are costly) or focus on the wrong areas. Neither of these approaches is desirable and should be avoided.

Regardless of the motives of our client (ensure regulatory compliance, enhance trust and loyalty or obtain a more positive organizational image and a significant edge over the competition) and the type of assignment, our approach is characterized by a focus on opportunities and threats, whilst striving for (sustained) compliance.

Possibility for Dutch organizations to obtain a privacy certificate

It is possible for Dutch organizations to obtain a privacy certificate for one or more of their personal data processing operations.

Advantages of such a certificate are:

- Certification helps to maintain the quality of data and processes, and contributes to continuous awareness. This, in turn, contributes to a continuous improvement and professionalism of the internal organization.
- The certificate is a means for an organization to show that personal data is handled with care, that the personal data is properly secured and that personal data is handled in acccordance with applicable laws and regulations. This strengthens the trust of clients, the supervisory authority (het College Bescherming Persoonsgegevens) and possible other stakeholders. An important advantage of the certificate is therefore the positive impact it has on corporate image and brand.
- For auditors the certificate can be a reason to (partly) renounce certain guarantees or control activities. This prevents the organization from having to provide complete openness and clear out time in each audit. This saves money and reduces the burden on the organization.

More information about privacy certification can be found on www.cbpweb.nl or www.norea.nl. If you are interested in certification or if you have any questions relating to the certificate, please do not hesitate to contact us.