Deloitte.

10 practical steps to data protection.

Leading business advisers

Privacy and data protection concerns present a growing challenge. Over the past 12 months there have been more high profile data protections incidents in Ireland and across Europe. These have related to both paper and electronic data breaches.

Concerns and losses of personal information and sensitive data can lead to regulatory fines and significant risk to an organisation's reputation. By implementing good practices and conforming to the associated requirements organisations can prevent unforeseen interruptions to their operations. The privacy and data protection balancing act is complicated by a host of factors.

There is the large amount of data held by organisations, the number of people who need to access this as part of their job and the number of forms, reports, systems and databases where data is held. Also with globalisation, organisations operate in countries outside their own jurisdiction. Transferring data across jurisdictions requires understanding of international requirements in addition to significant controls and management of data in transit.

What are the regulatory data protection requirements here in Ireland?

The Data Protection Commissioner has summarised the legislation into eight rules.

Data protection rules	
1	Obtain and process the information fairly
2	Keep it only for one or more specified and lawful purposes
3	Process it only in ways compatible with the purposes for which it was given to you initially
4	Keep it safe and secure
5	Keep it accurate and up to date
6	Ensure that it is adequate, relevant and not excessive
7	Retain it no longer than is necessary for the specified purpose or purposes
8	Give a copy of his/her personal data to any individual on request

10 steps to achieving compliance

In order to comply with the eight rules we have identified ten key steps that we can help you work through to reduce your exposure to critical risks and potential damage to your brand.

1. Strategy

Identification of executive sponsorship is the first step. Without senior executive buy-in it is hard for any individual data protection officer to create a culture of compliance. Together with the data protection officer, the executive sponsor should agree an overall data protection strategy including a clear vision and set of objectives.

2. Data inventory

Understand where your data is, both manual and electronic files. Data flow diagrams should be prepared to detail where the data is collected, how it is stored, how it is used, with whom it is shared, how it is maintained and how it is disposed of.

3. Requirements definition

This will include identification of the requirements of all jurisdictions within which the organisation operates. Despite similarities that exist amongst various privacy models, there are fundamental regional differences that exist.

Examples of global differences

- United States - Data protection can be considered weaker than requirements in many European countries. The prevailing concept in the United States is that once an individual provides personal data to an organisation, the organisation becomes the data owner and can then determine the use of that data.
- Europe - The prevailing concept is that the data subject retains the rights to his/her personal data and that the organisation has the responsibility of a custodian for protecting that data and using it only in accordance with the permission conveyed by the individual.

With the increased trend to outsource processing, significant consideration must be given to the legal and regulatory requirements in relation to transfer of personal data outside the EU.

Additionally, transferring data to a third party or outsourcing partner does not remove your responsibilities. Consideration should be given to EU passporting, US Safe Harbour or other international arrangements when operating in a global environment.

4. Risk analysis

Key risks facing your business should be identified in order to develop an appropriate policy and set of detailed procedures. Data protection requirements have an impact throughout business. The requirements will impact on technology solutions in relation to processing and security of personal data.

5. Data protection policy

The organisation's desire to maintain a compliant culture should be documented in the Data Protection Policy. This should include detail of the roles and responsibilities in relation to data protection within the organisation, e.g., name the data protection officer. It will also include policy on other activities within the organisation such as direct marketing, information security, clear desk policy, training etc.

6. Data protection procedures

Finding the balance between business needs and data protection requirements may be difficult due to opposing forces, e.g., data for direct marketing is a useful tool to increase business but there are strict requirements in relation to cold calling customers and use of existing personal details. Detailed procedures are required to ensure compliance with the requirements and may include marketing procedures, data retention and destruction procedures, data access request procedures, breach and reporting processes.

7. Data management controls

In order to ensure compliance with operational procedures, controls should be implemented. To assess the control requirements, the following steps should be completed:

- Analyse business processes
- Identify controls necessary
- Identify and design common controls and templates

Many business processes will suit similar controls, e.g., data input and access controls. This analysis should include security aspects both from an internal and external perspective to safe guard personal data through the lifecycle within the organisation.

8. Technology enabled tools

With large volumes of data processed within an organisation's IT environment, there is a large volume of possible outlets to inappropriately transfer confidential personal data which may result in a breach of legislation. All organisations should not only ensure adequate access controls but should consider the use of technology enabled tools such as a data monitoring tool. This will monitor the movement of data throughout the organisation, e.g., data printed and screen scrapes.

9. Training

There is no point in having all the documentation if nobody knows about it! It is absolutely vital that all staff are aware of the requirements in relation to working with personal data. Training must be appropriate to the end user, accessible and within budget.

10. Monitoring

To ensure ongoing compliance with policy and procedures, data protection should be included in the annual risk based monitoring plan. This should include the assessment of security of personal data, staff awareness of data protection requirements, review of the breaches register and review of data access requests.

Conclusion

There are few organisations which do not hold personal data, for example, HR files alone constitute personal data. Even if you are exempt from registration requirements, you must comply with data protection legislation. Primarily the business driver must be about protecting data and protecting your business.

Contacts

For more details please contact:

Colm McDonnell
Partner
Deloitte Ireland
T: +353 1 417 2348
E: cmdonnell@deloitte.ie

Gerard Lyons
Partner
Deloitte Ireland
T: +353 61 43 5501
E: cmdonnell@deloitte.ie

Sinead Ovenden
Director
Deloitte Ireland
T: +353 1 417 2545
E: sovenden@deloitte.ie

Sean Smith
Senior Manager
Deloitte Ireland
T: + 353 1 417 2306
E: seansmith1@deloitte.ie

Lisa Knox
Manager
Deloitte Ireland
T: + 353 1 417 2833
E: lknox@deloitte.ie

Guido Vandervorst
Partner
Deloitte Belgium
T: + 32 2 800 20 27
E: gvandervorst@deloitte.com

Philippe Delcourt
Partner
Deloitte Belgium
T: + 32 2 800 22 45
E: pdelcourt@deloitte.com

Tom Van Cauwenberge
Partner
Deloitte Belgium
T: + 32 2 800 22 79
E: tvancauwenberge@deloitte.com

Dublin
Deloitte & Touche
Deloitte & Touche House
Earlsfort Terrace
Dublin 2
T: +353 1 417 2200
F: +353 1 417 2300

Cork
Deloitte & Touche
No.6 Lapp's Quay
Cork
T: +353 21 490 7000
F: +353 21 490 7001

Limerick
Deloitte & Touche
Deloitte & Touche House
Charlotte Quay
Limerick
T: +353 61 435500
F: +353 61 418310

www.deloitte.com/ie