White Paper

August 2014

How to Protect Your Data

Practical ideas to help organizations comply with data protection legislation

NEOPOST

Send.Receive.Connect.

Editorial

Enno Ebels, Executive VP,
Customer Information Management, Neopost

"Making sure customer data is accurate and providing a trace of who changes what and when help organizations make customer communications more cost effective."

"Data protection is becoming a priority for organizations as we move into a digital environment where people care more about what happens to their personal information. The Snowden leaks (related to the National Security Agency in the US and its surveillance activities) and the level of public debate that followed highlight just how important data privacy has become for citizens and enterprises around the globe.

A large amount of information is now being collected on people, so rules need to be put in place in order to control all of the metadata being pulled together from various sources. This sets the stage for companies to re-think their business model and decide how to use data to improve products and services.

I believe that data is an asset and, although there are no clear rules on how to value it from an accounting perspective, I think it should go on the balance sheet at some point. The new data protection legislation planned for Europe will offer opportunities for enterprises that treat data as an asset, and by this I mean an asset with a value. The planned regulations will put more emphasis on data ownership and the need for governance in order to ensure data is handled correctly and stays current.

In the area of data quality and master data management the initial stage involves data capture. Then enterprises do something with the data, for example send a letter, deliver a parcel or post a comment on a social network. However this data needs to be kept alive as people move, products change and all kinds of additional information becomes available. This means that enterprises need to make sure they have a real process in place to manage data in the same way they manage other assets.

Making sure customer data is accurate and providing a trace of who changes what and when help organizations make customer communications more cost effective and enable enterprises to comply with different industry sector rules and regulations. Cleaner and enriched databases offer enterprises an opportunity to create a "single customer view" containing business-critical information. This includes an accurate name and address, purchasing preferences and multichannel delivery and contact points.

I am convinced that data will become a very valuable tool in the future and enterprises will be able to do a lot more for their customers if they learn how to leverage the data they collect while ensuring the protection expected by these customers."

Know Your Customer

Data protection is all about respecting an individual's right to privacy and the new data protection regulations, currently going through final review by the European parliament, will provide organizations with the momentum they need to manage their data more effectively. But what do you need to do in order to ensure your organization complies with data protection legislation while increasing customer satisfaction?

Responsible customer relations

Successful customer relations involves taking into account a consumer's right to be "left alone" and communicating with willing recipients using the customer's preferred channel – either postal mail, digital mail or multichannel delivery. If you wish to use personal data for postal marketing, you must tell your customers, or prospects that you intend to use their data for this purpose and give them the opportunity to refuse such use. Where you yourself have collected the data this should be done at the time of collection by providing, for example, a tick box on a form. If the data has been obtained from a third party the opportunity to refuse direct marketing materials must be provided before any materials are sent out.

Contact details can only be used for electronic marketing purposes (text messages, voice messages, sound messages, image messages, multimedia messages and emails) when:

- The product or service you are marketing is similar to that which you sold to the customer at the time you obtained their contact details
- You gave the customer the chance to object to you using their details easily and free of charge
- Each time you send a marketing message you give the consumer the right to object to receiving more messages in the future
- The sale of the product or service concerned took place not more than 12 months prior to the sending of the customer communication
- This means that organizations need to carefully manage all of the personal data they hold, improve data quality and take steps to comply with data protection legislation.

What is the Data Protection Legislation?

In Europe

The aim of the Data Protection Act (passed in the UK in 1998) is to provide individuals with a way to control information about themselves. The legislation in its current form gives people a right of access to personal data. This includes information held by a company that relates to an individual. A lot of data is considered to be sensitive and if it were to fall into the wrong hands this would be regarded as a breach of civil liberties.

The aim of the 1998 legislation was to align UK law with the 1995 European Union (EU) Data Protection Directive, requiring member states to protect individuals' rights and freedoms - in particular people's right to privacy when it comes to the processing of personal data.

Other European Union countries have passed similar laws as often information is held in more than one country.

The European Commission is currently planning to bring together all data protection within the EU with a single law, the General Data Protection Regulation (GDPR). One of the really significant aspects of the proposed regulation is that it will extend EU laws to non-EU companies selling into the EU. The timeline for this has still not been confirmed.
The European parliament wants to get it through by 2015. There are arguments being put forward in order to delay the legislation, to ensure that it is fully talked through but the aim is to have the regulation implemented by 2017/2018 in Europe.

In the US

The following Data Protection laws exist in the US:

HIPAA
The Federal Health Insurance Portability and Accountability Act (1996)
This legislation offers protection for people's health-related information. It specifies who can have access to an individual's health data. This covers medical providers' records, health insurers' computer records, billing information and conversations that doctors have had with other health professionals about a person's care and treatment.

FACTA
The Fair and Accurate Credit Transaction Act (2003)
This legislation aims to protect consumers' credit information from the risks associated with data theft. It makes it illegal for credit and debit card receipts to contain any more than the last five digits of a consumer's card number, however the regulation is not applicable to handwritten receipts. The most recent uproar in the US concerned the "do not track" movement which is specifically related to tracking online activity in order to create consumer profiles. A "do not track' bill was introduced in early 2013 as some people believe that legislation is the only way to give individuals control over their data. If such legislation is passed it will allow consumers to opt out of online tracking.

There is growing consensus on some of the common principles between EU and US data protection law and the EU is seen as a benchmark framework. Furthermore there is a move in the US to strengthen privacy laws at State level and a push at Federal level to clarify the laws there. The draft EU regulation will have an effect on the US as American companies that are engaged in the processing of data relating to EU citizens will have to comply.

Planned for

How Can You Comply?

Organizations and professionals that need to store personal data from clients in order to do business need to comply. Most companies that process customer data fall under the requirements of the Data Protection Act. The Data Protection Act can be complex and difficult to interpret. However it consists of eight key principles that organizations must adhere to.

8 Ways to Ensure Compliance with Current Legislation

1. Obtain and process information fairly

Example: Personal data will be obtained fairly by the tax authorities if it is obtained from an employer who is under a legal duty to provide details of an employee's pay, whether or not the employee consents to, or is aware of, this.

2. Keep it only for one or more specified, explicit and lawful purposes

Example: A not-for-profit chess club only uses personal data to organize a chess league for its members. The club is exempt from notification, and the purpose for which it processes the information is so obvious that it does not need to give privacy notices to its members. The specified purpose of processing should be taken to be the organization of the members' chess league.

3. Ensure that it is adequate, relevant and not excessive

Example: A debt collection agency is engaged to find a particular debtor. It collects information on several people with a similar name to the debtor. During the enquiry some of these people are removed. The agency should delete most of their personal data, keeping only the minimum data needed to form a basic record of a person they have removed from their search. It is appropriate to keep this small amount of information so that these people are not contacted again about debts which do not belong to them.

4. Keep it accurate, complete and up-to-date

Example: A journalist builds up a profile of a particular public figure. This includes information derived from rumors circulating on the Internet that the individual was once arrested on suspicion of dangerous driving. If the journalist records that the individual was arrested, without qualifying this, he or she is asserting this as an accurate fact. However, if it is clear that the journalist is recording rumors, the record is accurate – the journalist is not asserting that the individual was arrested for this offence.

5. Retain it for no longer than is necessary for the purpose or purposes

Example: A bank holds personal data about its customers. This includes details of each customer's address, date of birth and mother's maiden name. The bank uses this information as part of its security procedures. It is appropriate for the bank to retain this data for as long as the customer has an account with the bank. Even after the account has been closed, the bank may need to continue holding some of this information for legal or operational reasons.

6. Give a copy of his/her personal data to an individual, on request

Example: An individual makes a request for their personal data. When preparing the response, you notice that a lot of it is in coded form. For example, attendance at a particular training session is logged as "A", while non-attendance at a similar event is logged as "M". Also, some of the information is in the form of handwritten notes that are difficult to read. Without access to the organization's key or index to explain this information, it would be impossible for anyone outside the organization to understand. In this case, the Act requires you to explain the meaning of the coded information.

7. Keep it safe and secure

Example: An organization holds highly sensitive or confidential personal data (such as information about individuals' health or finances) which could cause damage or distress to those individuals if it fell into the hands of others. The organization's information security measures should focus on any potential threat to the information or to the organization's information systems.

8. Do not transfer it outside the European Economic area unless that country or territory ensures an adequate level of protection

Example: A multinational company transfers a list of internal telephone extensions to its overseas subsidiaries. The nature of the information makes it unlikely that the individuals identified would suffer significant damage in the unlikely event that an unauthorized source obtained the list. It is reasonable to decide that adequate protection exists.

How Can You Deal with the Upcoming EU Legislation?

Define your processes and understand them

At the core, the data protection principles will remain largely the same. But some new rights will be provided and a number of new responsibilities will be placed on Data Controllers and Data Processors. What organizations will need to do is probably being done already, but in an unstructured way. So this means formalizing processes. In practice this means that you will have to:

Start managing data in a structured way
This will involve managing data the way you manage other assets such as company cars, stationery or financial results.

Ensure your organization has a clear segregation of duties concerning governance
There will need to be an entity to ensure the right things are being done in the right way.

Keep documentation about the processing of personal data
Not having documented processes will be an offence which will incur a significant financial penalty.

Carry out document controls to monitor and manage compliance
You will also need to be able to demonstrate evidence of these controls actually working in the organization, or face a significant financial penalty.

Appoint a Data Protection Officer (DPO)
This will apply to organizations with over 250 employees or entities engaged in "systemic monitoring" of EU citizens or public sector structures. Not having a DPO will constitute an offence, with a significant financial penalty.

Put control structures into place
This includes asking the following questions about mailing lists:

- Where did we get the data from?
- Do we have the consent to use the information?
- Did we buy it from a reputable source or did someone give it to us on a memory stick?
- What are our governance policy and protocols around using the data?

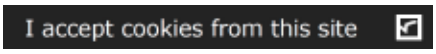
Cookies

An example of how European legislation is taking data privacy seriously is demonstrated by recent regulations that concern gaining consent from individuals for the placing of cookies on web browsers.

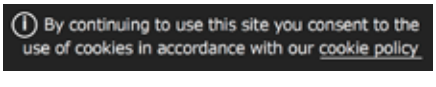
What are cookies?

- Cookies are small files that websites put on a computer hard disk drive when a user first visits.
- Cookies are used to maintain stated information as a user navigates between different pages on a website, or returns to the website at a later time by helping the web page server to recall the user's specific information
- Cookies let users store preferences and user names, register products and services, and personalize pages.

Legislation states that users must now consent to the use of cookies - The opportunity to opt-out is no longer sufficient. Consent may be obtained explicitly through the use of an opt-in check box which users can tick if they agree to accept cookies.



Consent may also be obtained by implication.



How will this Change Your Working Environment?

In a data-driven economy, ensuring governance and taking control of data will become increasingly important and the draft legislation provides you with a very clear mandate to do this. The governance issues will have knock-on effects throughout your entire organization and will encourage you to manage business document output in a much more structured way.

From a Human Resources perspective, the new legislation means that we are going to see an increase in the importance of training in new controls and procedures in order to educate and inform personnel. We are also most likely to see a trend towards the adoption of output management software and the inclusion of a data compliance policy in company handbooks.

Tight controls on company databases and the automation of business processes will also become important. An audit of the permissions according to the user profile across all ERP (Enterprise Resource Planning) & CRM (Customer Relationship Management) systems will limit the opportunity for a data breach to occur and protect all sensitive information related to customers. This will involve a review of the settings that each employee has on any database. For example, a salesperson will not need access to bank details in the financial module of an ERP system.

> *"Banks don't organize money, they manage data about finance. Logistics companies don't ship products, they manage data about products. Amazon doesn't sell books. It presents and processes data about books."*
>
> Daragh O'Brien
> Castlebridge Associates

The risk of getting it wrong

If organizations do not take data protection seriously this may lead to major financial and reputational costs. Sony, for example, was hacked nine times over a three-week period in 2011. People's personal details were exposed, costing the brand around $175 million (US), and this does not include the cost relating to brand damage.

A 2012 study by OVUM highlighted that for the average organization 30% of revenue is consumed by addressing data quality problems in the organization. This involves cross-checking data, fact-checking, correcting and responding to errors. In 2013 Adobe had a massive worldwide security breach and all subscriber details were comprised – costing the organization huge amounts in terms of crisis management and causing enormous damage to the brand in terms of image.

The new legislation includes penalties of up to €2 million or 5% of global turnover for getting data protection wrong. This will therefore be an opportunity for companies to improve their brand image by acting more professionally via data cleansing and enrichment. Enterprises will therefore be in a position to better manage one of their most critical assets – information.

Estimated amount of revenue consumed by addressing data quality problems in the average organization.

Key Challenges you may Face

The length of time it will take to change thinking about data

It will take 18 months to two years for organizations to put in place the necessary structures.

People seeing data protection as an IT or Marketing issue

But it's not. It's an enterprise asset challenge that needs to be addressed. All companies even small structures will need someone to have an oversight over all key assets, including data.

The future data protection landscapes

In a continuously challenging economic climate an extra effort will be required by everyone involved in data gathering, management and protection. Experts however believe that there will be effective protection for individuals wherever their data is located, including cloud storage. There will be a much stronger focus on stewardship for holders of individuals' personal data. This means enterprises will start treating personal data as they would financial data and ensure that it is protected wherever it is located. We are also likely to see more penalties for those who fail in their stewardship duties. For companies involved in marketing and customer relations the future privacy landscape will offer opportunities for those willing to invest in providing what consumers want and finding innovative ways to reach them.

Conclusion

Organizations that focus on the idea that the draft legislation is going to make it more difficult for them to obtain consent to use data are missing the real potential of the regulation. This legislation offers organizations many opportunities if they start to think of information holistically and treat it as an asset. If companies are able to put a proper governance process into place to deal with data protection they will then be able to ensure that the right things are being done in the right way.

Compliance checklist

1. Clarify who is in charge
2. Define what has to be done and by whom
3. Make sure people are doing the right things in the right way (for example extracting data or using marketing analytics)
4. Start including EU Data Protection/Privacy compliance requirements in your Data Governance regardless of where you are globally.
5. If you are in the EU, get your Data Protection, Data Governance, and Information Quality teams talking (and ideally co-located or merged) and start looking at what needs to change in your organization.

Main contributor

Daragh O'Brien
Founder and Managing Director, Castlebridge Associates, Ireland

Castlebridge Associates provides coaching, consulting, mentoring, and project management services to organizations struggling with Information Quality challenges, Data Governance difficulties, Data Protection Compliance issues, or just finding it hard to hammer out their Information Strategy.

Other sources

- TDAN (The Data Administration Newsletter)
- ico.org.uk (ICO - Information Commissioner's Office)
- Neopost's 2011 Privacy Seminar
- OVUM (provides independent and objective analysis that enables organizations to make better business and technology decisions)
- Hillicon Valley -The Hill's Technology blog
- The Office of the Data Protection Commissioner, Ireland ehow.com

Send
Receive
Connect

About Neopost

Neopost is a global player with a local presence in business solutions for the postal, parcel delivery and related digital world of tomorrow. We have an intimate understanding of physical and electronic communications and work in collaboration with over 800,000 enterprises around the world. Our business has evolved to meet the growing demands of a technology-driven environment. This means we can help our customers successfully make the transition from physical mail to quality multichannel communications management.