Keep in Line
Comply with data regulations

An Experian QAS handbook

November 2008

Contents

 This guidance note is intended for just that purpose and should not be relied upon as compliance or legal advice. Independent legal advice should be sought in this regard.

1. Introduction : The compliance minefield

Each year, Experian QAS conducts global research which reviews data management practises across the world. In January 2008, the topic of data compliance was investigated. Only 27% of organisations thought they were 100% compliant with database-related regulations. This figure has dropped from 37% three years previously.

So, is data compliance getting harder? Well, there could be a number of reasons for this backward trend. Over the past few years the volume of regulations that organisations have to comply with has increased. There have also been changes to regulations and licensing rules which have to be digested and implemented. This has all been set against a back drop of limited prosecutions. Until recently, for example, very little action had been taken by the Information Commissioner's Office (ICO) against firms that do not abide by the Preference service laws.

But the landscape is now changing. In May 2008, the ICO got its 'teeth' and now is in a position to impose substantial fines on organisations that breach the Data Protection Act (DPA). A number of fines have also been issued by the Financial Services Authority (FSA), where organisations have failed to implement the correct procedures to establish their customers' identity. In addition, there have been changes to the way that address data should be collected, formatted and licensed that can't be ignored. With all this change, it is no wonder that compliance with data regulations can seem like a minefield!

The purpose of this handbook is to provide a simple overview of some of the rules, regulations and licensing agreements that affect contact data management. Within each section there are tips, recent updates and information on where you can go for full third party legal advice.

My overall piece of advice to you, however, would be to think about what data you are collecting, how you are using it and what you are using it for. Compliance shouldn't be seen as a barrier, more as a checklist to ensure that your customers' information is managed in the right way.

Look after your data and ultimately it should lead to better relationships with your customers.

Best regards

Stuart Johnston
UK Managing Director
Experian QAS

2. Rules, regulations and licensing

2.1 Data Protection Act

Enforced by:
The Information Commissioner's Office (ICO)

Sectors affected:
All sectors – any organisation that processes personal information

The Act:

The Data Protection Act 1998 came into force on 1 March 2000 and replaced the Data Protection Act 1984. It gives individuals ('data subjects') a general right of access to 'personal data' (i.e. personal information) about themselves held by 'data controllers' within the United Kingdom. It also lays down principles for the way personal data must be managed.

The Information Commissioner promotes public access to official information and protects personal information. The ICO is an independent body with specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

Main Principles:
Before you can process personal data, one of the following conditions must be met:

- consent has been given by the data subject
- it is for entering or performing a contract with the data subject
- the data controller is under a legal obligation, other than under contract
- it is to protect the vital interests of the data subject
- it is for the administration of justice, exercising functions under an enactment, exercising of government functions, or the exercise of any other functions of a public nature in the public interest
- it is for the pursuit of the legitimate interests of the data controller

Any organisation that processes personal information must comply with eight principles that make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection

Recent updates:
In May 2008, the Criminal Justice and Immigration Act received Royal Assent creating tough new sanctions for the privacy watchdog, the ICO. This new legislation gives the ICO the power to impose substantial fines on organisations that deliberately or recklessly commit serious breaches of the Data Protection Act.

"This change in the law sends a very clear signal that data protection must be a priority and that it is completely unacceptable to be cavalier with people's personal information. The prospect of substantial fines for deliberate or reckless breaches of the Data Protection Principles will act as a strong deterrent and help ensure that organisations take their data protection obligations more seriously."

David Smith, Deputy Information Commissioner, 9th May 2008

Tips and advice:
Ensure data is accurate, up to date and gathered / protected fairly and securely

In a recent feature on the Data Protection Act in the Marketer, Phil Jones, Assistant commissioner at the ICO, offered the following tips for compliance:

- Organisations must ensure personal data is processed fairly and securely
  Failure to adequately protect personal data can result in personal or sensitive data falling into the wrong hands and can ultimately damage trust.

- Any data held on customers must be accurate and up to date
  ICO research shows that 70 per cent of organisations are aware of this and we continue to raise the awareness of those that aren't, raising awareness of their responsibilities under the Act.

- Organisations must only retain information as long as it is necessary in relation to the purposes for which it was originally collected
  And if organisations wish to share marketing lists with other companies they should be open with individuals from the outset about how their information will be used and to whom it will be passed.

- Individuals have the right under the DPA to opt out of providing information for marketing purposes
  Organisations must comply with any such request and be open and clear with consumers when gathering their personal information

Achieving the above and improving data quality can seem like a daunting task but it's all about having the right people, processes and technology in place. A formalised data strategy, with buy-in from the top, will give you confidence that all employees are managing your organisations data correctly, in line with your policies.

Click here for Experian QAS' Top Ten Tips on how to get started.

2.2 Money Laundering Regulations 2007

Enforced by:

There are a number of supervisory authorities listed in the Regulations, including the Financial Services Authority (FSA), HM Revenue & Customs (HMRC), OFT (Office of Fair Trading).

Organisations affected:

a) credit institutions
b) financial institutions
c) auditors, insolvency practitioners, external accountants and tax advisors
d) independent legal professionals
e) trust or company service providers
f) estate agents
g) high value dealers
h) casinos

Overview:

September 11th 2001 put global focus on anti-money laundering. Since then we have seen a wave of UK legislation designed to combat money laundering and terrorism, most recently the Money Laundering Regulations 2007.
From 15 December 2007, the Money Laundering Regulations 2007 required certain businesses to have systems in place to prevent money laundering and to report suspicious activity. These systems include:

- Assessing the risks of your business being used by criminals to launder money
- Identifying customers and beneficial owners and verifying their identity
- Monitoring customers' business activities and reporting suspicious activity to the Serious Organised Crime Agency (SOCA)
- Retaining records; and ensuring you have appropriate internal management controls

Main Principles:

The regulations set out the key principles that an organisation must follow. Those that are related to data and identity are:

1. Customer due diligence

"Customer due diligence" means identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source

2. Application of customer due diligence measures

You must apply customer due diligence measures when you:
a) establish a business relationship
b) carry out an occasional transaction
c) suspect money laundering or terrorist financing
d) doubt the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification

You must also:
a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction and;
b) be able to demonstrate to your supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing

3. Timing of verification

You must verify the identity of the customer (and any beneficial owner) before the establishment of a business relationship or the carrying out of an occasional transaction. Such verification may be completed during the establishment of a business relationship if:

a) this is necessary not to interrupt the normal conduct of business; and
b) there is little risk of money laundering or terrorist financing occurring

This is provided that proof of identity is established at the first possible opportunity.

4. Casinos

(1) A casino must establish and verify the identity of:

a) all customers to whom the casino makes facilities of gaming available
i) before entry to any premises where such facilities are provided; or
ii) where the facilities are for remote gaming, before access is given to such facilities
b) if the specified conditions are met, all customers who, in the course of any period of 24 hours-
i) purchase from, or exchange with, the casino chips with a total value of 2,000 Euro or more;
ii) pay the casino 2,000 Euro or more for the use of gaming machines;
iii) pay to, or stake with, the casino 2,000 Euro or more in connection with facilities for remote gaming

5. Enhanced customer due diligence and ongoing monitoring

Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures:

a) ensuring that the customer's identity is established by additional documents, data or information;
b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

6. Policies and procedures

There is an obligation to determine whether the customer is a politically exposed person

2.2 Money Laundering Regulations 2007 Continued

Tips and advice:

The Regulations specify the circumstances when you must identify and verify the identity of your customers and obtain additional information about the nature and purpose of your business relationship.

Traditional methods of proving identity were using paper documentation – the passport / driving license, utility bill. This, in practice, is not the most convenient way of doing business. Despite the fact that these documents can be easily forged or intercepted by fraudsters, the biggest downside of paper is that it doesn't work with online transactions – and the internet is growing, fast. There is nothing more inconvenient than having to send paper proof of ID mid way through an online account opening process, etc

Bodies such as the FSA now approve electronic authentication as a compliant alternative. The principle behind electronic authentication is to use a variety of data sources to establish that an individual exists in society. The data is then analysed to highlight any suspicious activity that might indicate identity fraud or money laundering.

Grosvenor casinos, ING Direct and Westminster City Council are examples of Experian clients that are using electronic authentication to comply with money laundering regulations.

More information can be found here.

2.3 Treating Customers Fairly

Enforced by:

The Financial Services Authority (FSA)

Sectors affected:

Financial services

Overview:

The TCF ('treating customer fairly') principle aims to raise standards in the way firms carry on their business by introducing changes that will benefit consumers and increase their confidence in the financial services industry.

Specifically TCF aims to:

- **help customers fully understand the features, benefits, risks and costs of the financial products they buy**
- **minimise the sale of unsuitable products by encouraging best practice before, during and after a sale**

The FSA has outlined six core consumer outcomes that it wishes to see as a result of the TCF initiative.

These are:
Outcome 1 - Consumers can be confident that they are dealing with firms where the fair treatment of customers is central to the corporate culture

Outcome 2 - Products and services marketed and sold in the retail market are designed to meet the needs of identified consumer groups and are targeted accordingly

Outcome 3 - Consumers are provided with clear information and kept appropriately informed before, during and after the point of sale

Outcome 4 - Where consumers receive advice, the advice is suitable and takes account of their circumstances

Outcome 5 - Consumers are provided with products that perform as firms have led them to expect, and the associated service is of an acceptable standard and as they have been led to expect

Outcome 6 - Consumers do not face unreasonable post-sale barriers imposed by firms to change product, switch provider, submit a claim or make a complaint

Recent updates:

According to an FSA survey of nearly 100 companies, almost nine in ten firms missed the end of March 2008 interim deadline to have management information in place to test whether they are treating customers fairly. Financial services firms are therefore under pressure to meet the next deadline in December 2008 when they will be expected to demonstrate both internally and externally to the FSA that they are consistently treating their customers fairly.

Tips and advice:

To demonstrate TCF compliance, you must hold up-to-date communication details for your clients. In particular, the quality of the addresses held must be a priority, including whether the address on record is still current for the client.

TCF Outcome 3 states that 'consumers are provided with clear information and are kept appropriately informed before, during and after the point of sale'. If customer records and communication details are not kept accurate and up to date then it becomes difficult for an organisation to provide a good level of customer services and comply with TCF regulations.

Having the following processes in place should help

- Have standard processes in place for managing data across different departments
- Regularly clean and suppress customer data
- Validate new data entering systems
- Keep on top of duplicate records

Following the above will help achieve a consolidated view of data is vital to avoid poor customer service and to comply with the spirit of TCF. It also has real, tangible business benefits. Accurate data means that you can gain a better picture or understanding of customers through a 'single customer view'. This makes cross-selling and up-selling much more effective.

To find out more about how Experian QAS can help, click here.

2.4 Royal Mail Postcode Address File (PAF) Licensing

Enforced by:
The Royal Mail

Sectors affected:
All sectors that use the Postcode Address File (PAF)

Overview:

The Postcode Address File or PAF contains all known UK residential and business delivery addresses and postcodes. The file was originally designed to assist the delivery of post by the Royal Mail. Usage has grown and it now forms the basis for address management solutions in the UK. PAF is licensed by the Royal Mail and royalties for its use are collected either directly from the customer or via resellers such as Experian QAS.

Recent updates:
The previous license for use of PAF came into force in the 1990's. Business models have changed in subsequent years, especially with the introduction of the internet. As a result, the Royal Mail identified that the license was in urgent need of updating.
Over the past few years, the Royal Mail has been conducting a lengthy review of the license, in conjunction with the PAF Advisory Board.

The new license is designed to be more straightforward and to reflect actual usage of PAF. It is intended that these changes will make PAF more accessible to SMEs looking to get up and running with PAF. However, it will have additional liabilities for heavier users of the file. The Royal Mail anticipates that the changes in licensing will be revenue neutral – i.e. it doesn't expect to make money from the process in the long term.

The Royal Mail's timetable for change is as follows:

2008
Tuesday 4 November
Publication of formal consultation document on the new PAF licence and consultation period opens

Wednesday 24 December
Last chance to input into the formal consultation on the new PAF licence and consultation period closes

2009
April
Publication of the new PAF licence

September
Start of migration to the new PAF licence

Key principles:
i) The Royal Mail currently licenses on a 'legal entity' basis but it is also looking at ways of providing flexibility for businesses that wish to work together for a common purpose.

ii) The proposed changes include a reduction of the 'per user' fee, the introduction of multiple user bands and unlimited internal transaction licensing, reduced data supply prices and extended user group options.

iii) Under the terms of the new licence, you will have the option to pay for certain usage of PAF internally within the company on a 'per click' basis or on the number of users.

iv) Organisations operating in a small geographic region will also be able to buy PAF data for individual postcode areas.

The Royal Mail also provides the following statements that relate to specific usage:

Corporate Groups
- We will continue to encourage Corporate organisations to licence across their Group to reduce admin burden and encourage increased use of PAF

Government licensing
- It is our intention to license all Government entities directly and therefore create a truly level playing field for Solutions Providers when selling into the Public Sector

Bureaux
- We intend to have a single charge for being a Bureau and user charges for internal use.

Postzon
- We intend to license Postzon using a separate licence, to avoid overburdening the PAF licence with clauses specific to Postzon

Tips and advice:
Both the Royal Mail and value-added resellers of PAF (such as Experian QAS) can provide you with tips and advice. By reviewing the way that you currently use PAF and your future plans, they will be able to recommend the license that suits your individual business model.

For example, here is a basic tip offered by Giles Finnemore, Head of Marketing at Royal Mail's Address Management Unit:

'You could 'mix and match' users and clicks. So if an organisation has three heavy users and two light users you can licence three users and buy blocks of clicks for the other two.'

For further information, please e-mail address.management@royalmail.com or info@qas.com.

1 The PAF Advisory Board was created in 2007 to give independent advice to the Address Management Unit of Royal Mail on behalf of PAF users. Its members cover independent postal operators, value added resellers of PAF, web based companies, mail users and public sector users.

2.5 BS7666 – The National Land and Property Gazetteer (NLPG)

Enforced by:
BSI British Standards

Sectors affected:
Government organisations

Overview:

For the Public Sector, the BS7666 standard was introduced to standardise all data being uploaded to the National Land and Property Gazetteer (NLPG). The purpose of the NLPG is to create a 'single, unique source of address data linked to consistent national reference number for each property unit. This will enable the unambiguous identification of land and property.

The local government has spent a significant amount of time and money collecting the data that makes up the NLPG. As a result, the NLPG file now contains over 300 million records and many previously non-addressable items such as playing fields. Below is an overview on how to conform and subsequently how to get the best from NLPG data.

Recent updates:
Underpinned by British Standard BS7666, the local authorities had a very specific list of how their data was to be produced, documented and exported to the national hub (NLPG). Those that failed to meet the BS7666 standard by October 2007 faced fines.

Key principles:
Each address record has to be standardised and consist of the following elements:

- Basic Land and Property Unit - A piece of land or property. No entry can exist in an LLPG without a corresponding BLPU
- Unique Property Reference Number A nationally unique number assigned by the NLPG to local authorities in order to give a unique identity to a BLPU
- Unique Street Reference Number - The street address, it is the identity given to the BLPU. It must contain at least a PAON (see below) and every BLPU must have at least one LPI (although a BLPU can often have more than one LPI).
- Primary Addressable Object Name - Part of the LPI, usually a building name or street number.
- Secondary Addressable Object Name - Part of the LPI used when describing the likes of flats or sub-units. A SAON cannot exist without an associated PAON
- Street Descriptive Identifier Structure - All LPIs must contain a reference to a street in the street gazetteer. If a property does not lie on a suitably identifiable street, then one must be created. Unusual examples include islands in the middle of the Thames
- PostCode - Optional as many addresses are not "addressable", meaning they do not have postboxes. Postcodes are assigned to properties by the Royal Mail

Once the data has been transformed into the format above, it must be transferred from each Authority to the NLPG in the Data Transfer Format (DTF). The DTF is either a comma separated value (csv) or XML file format.

Tips and advice:
A fact sheet on BS7666 and information on where to go for sample data files can be found here.

Once the data has been submitted to the hub, then it is important that your organisation starts using the data in daily operations. The NLPG is an extremely comprehensive dataset and in order for the data to be compressed and used across systems such as finance, CRM, etc, it may be necessary to use software solutions.

Click here for information on how Experian QAS is helping London Borough of Brent, Manchester City Council and Surrey County Council get the most from their gazetteer data.

3. Resources

The Data Protection Act

Further information on the Data Protection Act and how to comply can be found at:
http://www.ico.gov.uk/what_we_cover/data_protection.aspx

The ICO also offers tips and advice on how to ensure that your data is secure. These can be found at:
http://www.ico.gov.uk/Home/for_organisations/topic_specific_guides/Data%20security%20tips.aspx

Here is information on data security breaches:
http://www.precisionmarketing.co.uk/Articles/257985/Data+breaches+rocket+in+number.html

Money Laundering Regulations 2007

For further advice on how to comply with the Money Laundering Regulations 2007 please visit:
http://www.hm-treasury.gov.uk/Search.aspx?terms=money+laundering

Treating Customers Fairly

An overview ofTCF regulations can be found here:
http://www.fsa.gov.uk/Pages/Doing/Regulated/tcf/index.shtml

Here is an summary of the findings of the FSA on non-compliance withTCF:
http://www.out-law.com/page-9250

Royal Mail PAF Licensing

Information on the new license can be found at:
ftp://ftp.royalmail.com/Downloads/public/cmwalk/doc/active/doc33000003/DEU_New_PAF_Licence.pdf

General information on PAF can be found at:
http://www.royalmail.com/portal/rm/jump2?mediaId=400085&catId=400084

BS7666 – The National Land and Property Gazetteer (NLPG)

Information and resources on the NLPG can be found at:
http://www.nlpg.org.uk/nlpg/link.htm?id=2012

Other legislation

Experian is committed to helping its customers meet regulations and has a website dedicated to compliance. Click on one of the links below to find out more about the listed regulations:

- Civil Partnership Act 2004
- Companies Act
- Consumer Credit Directive
- Consumers
- Credit Scoring
- Data Protection
- Electoral Register
- Enterprise Act & Scottish Debt
- Fair Obtaining clauses
- Gender Recognition
- Money Laundering
- Data Sharing
- The Principles of Reciprocity
- Searches
- Third Party Data

Experian QAS
George West House
2-3 Clapham Common North Side
London
SW4 0QT

T 0800 197 7950
info@qas.com

www.qas.co.uk