eCRM: 360° Management of Customer Data

cabestan

CONTENTS

INTRODUCTION

I.   Why eCRM?

In July 2010, Marketing Week Magazine featured a round table discussion entitled **Gathering Intelligence is the Secret to Success**. The following quote from Martin Duffy, Head of Marketing, Business Events – FT Business, stood out:

In my experience, marketers are naturally business-minded and inquisitive. If you are not switched on to that way of thinking, you will always look at what you are pushing out rather than stepping back and listening to your customers.

Our commodity is information and we have to know what our customers are looking at; they need it quickly and it has to be of value. There is no point in us having what someone else does because they won't come back to us or a pay a premium for what we do. It comes back to the crux of marketing – understanding customer demand and satisfying them profitably.

The "crux of marketing"

How often do you come back to the "crux of marketing"?

Depending on your business, probably not often enough. Understanding customer demand is paramount to marketing - if you can decipher what your customer wants (the hard part) then you can move on to satisfying them profitably (not without its challenges, but definitely easier).

When we get into trouble, when our sales figures take a nose dive, is when we try to sell without understanding what the customer is looking to buy first. Today's consumer is quick to change the channel if you aren't consistently answering 'what's in it for me?' If the customer sees no value in your communication, they lock the door - cutting you off from them.

The key to unlocking these doors starts with building a relationship with the customer - a relationship that moves beyond the dated 'batch and blast' mentality and embraces eCRM.

eCRM addresses the crux of marketing by treating each customer as an individual. Gathering as much data about them as you can from a variety of touch points (store, website, email, call centre, mail, etc) and coupling this with sociodemographic info allows you to quickly build up a much clearer picture of who your customer is and what they require.

This approach moves you away from seeing your customers as one homogenous group and instead facilitates segmentation. Only then can you sell to their specific needs and concerns.

Why choose an eCRM solution?

1. eCRM gives you an opportunity to create a real relationship with your client. A two-way relationship, not a dead-end street. One where you can poll them, engage them, question them and take note of what

they have to say and how they react to your messages. Their response allows you to shape future communications.

2. eCRM allows you to build a 360˚ SCV (single customer view) compiling an accurate and extensive portrait of your customer. This SCV can then be filtered through geographic profiling, market research and testing to further refine your data and plan your marketing campaigns. Behavioural intelligence, gained from tracking user interaction with your emails and website allow you to continually add to your SCV.

3. The e in eCRM means that you can interact with your customer regularly without the prohibitive costs of traditional mail-based marketing.

Embracing cost-effective tools like SMS and email allow you to send highly targeted communications/offers to different segments of your database on a regular basis.

In this white paper we are going to be looking in more depth at eCRM examining how this powerful marketing tool can boost customer engagement, brand loyalty and your bottom line.

After all, isn't that the 'crux of marketing?'

II. What is eCRM?

Before we go into a deeper exploration of eCRM, we need to come to a common understanding of what this little group of letters actually means.

In its simplest form, an eCRM is a CRM which is delivered electronically.

But let's break that down a bit more.

In order to understand this better, we need to step back to 1983 when Leonard Berry coined the term R*elationship Marketing*. Relationship marketing focussed on how you could attract, keep and enhance relationships with your customers over time.

Working with new customer-focused models, they began to plan marketing campaigns which were more interactive in nature and focused on customers' individual needs rather than treating them as a homogenous unit. As new technologies allowed easier access to customers, they began to present new marketing channels. With the advent of websites, email, and SMS/text messages, you could relate to customers in ways you never could with traditional mail marketing.

As they utilised IT services to manage these customer relationships, RM morphed into CRM, or *Customer Relationship Management*, which harnessed the powers of technology to implement strategies of *Relationship Marketing*.

eCRM is simply using the available electronic tools to deliver your *Customer Relationship Management* programme.

How is this relevant today?

Think for a minute about all the different places that you come into contact with your customer: how can you use those interactions to convert new customers and deepen relationships with existing customers?

For instance, in-store, on your website, through email, via post or when they are speaking with your call centre, all present opportunities to build your understanding of your customer, track their preferences, actions and responses to your offers.

It might be capturing their email address and postcode at point-of-sale. Or maybe you track the pages they visit most frequently on your website. All of this provides you with vital data which allows you to segment your customer.

With a segmented database you are far more likely to deliver the information your customer wants, in their preferred format, at a time that suits them. If you speak to them in language they understand, you are far more likely to move them further along your sales funnel.

Use of eCRM encourages brand loyalty, increases purchase values and encourages repurchasing which has a positive effect on RFM scores (Recency, Frequency and Monetary value of customer's purchases).

That's a lot of marketing power resting on the shoulders of four little letters.

Chapter 1 MULTIPLICITY OF DATA SOUCES

I. Capturing Customer Data – What and Where?

We've already established the value that a robust **eCRM** program can have for maximising your customer relationships, so now we move on to the specifics of how you go about setting one up.
Your ability to speak to your customer and address their specific needs starts and ends with the quantity and quality of information you hold about your customer. The more high quality data you have, the better you can anticipate and address their buying needs.

So where does this information come from?

There are a multiplicity of data sources available to you, the eMarketer - the question becomes *what data should you capture and use to engage with your clients and where do you get it from*?

What?

Let's start with what data you should be looking to collect.

This is really one of those 'how long is a piece of string' questions. The more data you can gather about your customer, the better you can understand them. But you walk a fine line. If you ask too much from the customer too soon, you risk them closing the door to you. If you ask too little, then you don't have sufficient data to be able to fully understand their buying patterns.

The key is to be strategic in what you ask for. Don't ask for any information that you don't have need for. Also, prioritise the information you request so you can capture the key demographic information up front and fill in details over time as your customer trusts you.

Skeleton Information

Your basic customer data might include:

- email address
- first name
- last name
- postcode
- age
- marital status
- income
- gender
- mobile phone number
- permission (you want to capture their permission to allow you to contact them via email/text in order to avoid spamming)

Even with only some of this information, you can begin to construct a comprehensive picture of your customer.

How?

How do you get your customer to give you this information? You could offer them a newsletter to subscribe to, send them a catalogue or run a contest. Sometimes you tease the information out of them with games, quizzes or vouchers.

Once you've obtained basic information on your customer, you can flesh out their profile through further customer interaction with your brand.

The other way you can go about this is through *email appending* where you take an email list to a data warehouse to purchase data to further flesh out your list.

Where?

Now that you understand what sort of information you want, you need to figure out where you are going to capture it. There are several options available for capturing basic data and developing it over time.

POS

When your customer is face to face with one of your sales associates is a perfect time to try and capture information from them. Point of sales contact can be a time to gather email addresses or to encourage your customer to sign up to your loyalty card scheme. However, be aware of human error which can creep in when data is captured manually.

Point of sale contact also allows the computer or cashier system to record your purchase, the retail price and the date of purchase and store that information in your customer account.

In this way, you can define your customers' tendency or inclination towards a certain product or brand. This is useful information in the future for cross-selling or upgrading opportunities.

An example would be if you bought an outdoor patio table at a garden centre and later received an email with an offer for an umbrella or barbeque.

Loyalty Cards

Many of the supermarket chains have achieved great success with loyalty card schemes. By signing up to the scheme, your customer collects points from their purchases which they can redeem for future savings or rewards. From your point of view, if you get them using their loyalty card you can track their purchases. This allows you to build up a comprehensive profile of what your customer buys.

Do they buy nappies every week? It's a pretty good assumption that they have a baby at home and might be interested in vouchers for baby shampoo, etc.

You may have to use *profiling* to determine if, for instance, a husband and wife are both sharing the same card which could skew your data. With profiling, you might create sub-profiles within a main profile.

Call Centre

Your call-centre staff are able to further expand on your customer's profile. A few simple questions can confirm address details or fill in missing data from an incomplete profile.

They can also ask the customer to partake in a brief survey or offer a subscription to a newsletter or catalogue.

Social Media

You can capture plenty of customer data utilising Social Media. *Facebook Connect*, which saves your customer the trouble of filling out your form by populating it with their Facebook information, also gives you permission to access much of their Facebook data which you can import to your own database.

Website

Web Analytics allow marketers to track your customers' browsing habits. If your customer signs into your site, or if you have a cookie tracing their activities on their computer, you can gather data based on what areas of your website they look at or any items they put into their shopping cart. Logging how web traffic arrives at your site is another valuable web tool. Tracking banner ad response, Google AdWords campaigns, and use of companion sites are also frequently utilised by eMarketers.

Email

Email allows you to send sales messages directly to your customer. Open rates are one way of roughly determining the effectiveness of your campaign; however click-through rates are an even better barometer of your customers' interest. Again, all of this is useful data which is added to your customer profile.

SMS/Text

SMS/Text messaging, while a useful tool to connect with your customer, is best used in conjunction with another tool such as email. You can only track bounce rates and click through rates, so it isn't the most accurate measurement of customer engagement.

ERP

As you collect all this customer information, you feed it into your ERP system. The ERP (*Enterprise Resource Planning* system) is your database or repository for all your customer data.
Next, we'll look at how to create a flexible database which will be the engine driving your **eCRM** activities.

Chapter 2 CREATING A FLEXIBLE DATABASE

I.   Case Study: The Beautiful Game (Listening to 3 Million Fans)

The Problem

Imagine for a minute that you work in the Marketing Department of one of the largest football clubs in the world. You've got over 3 million fans who are busy engaging with their favourite team on a regular basis:

- Buying tickets (online + in person)
- Purchasing team merchandise (online + in person)
- Exploring your website
- Watching interviews and match replays on your web TV channel
- Using their team loyalty card
- Visiting your home stadium
- Posting comments in online forums
- Evaluating photos on your website
- Responding to email and text message campaigns

As they do, they are leaving footprints all over your brand.

But what if you aren't fully capturing all this activity or using it to tailor your communications with your fans?

That is the situation that the French football club Paris Saint-Germain found themselves in when they approached Cabestan in 2002 to help them overhaul their multi-channel relationship with their broad customer base

The Solution

When we looked at their set-up, it became clear that the flat database structure that Paris Saint-Germain (PSG) were using just wasn't cutting the mustard when it came to dealing with the complex data which was available to them.

The issue wasn't just the flat database structure, but the multiplicity of databases - each system had its own database and database structure. And to make matters worse, this data wasn't necessarily cross-referenced.

The solution involved selecting the right data from each database to meet marketing objectives and feeding it into a central database.

The difference was that the central database was set up as a *relational database* in order to really handle the multiple, complex layers of data they were capturing from their fans.
The relational database stores all of the individual groups of data in separate tables which allows for greater flexibility in combining data. This provides the Marketing Department with the ability to combine a number of different data sets to hone and narrow down their large database into specific subsets and direct their

communications accordingly.

This allows PSG to streamline their communications and engage with each of their fans on a more personal level.

This diagram below gives a visual understanding of how the process works:
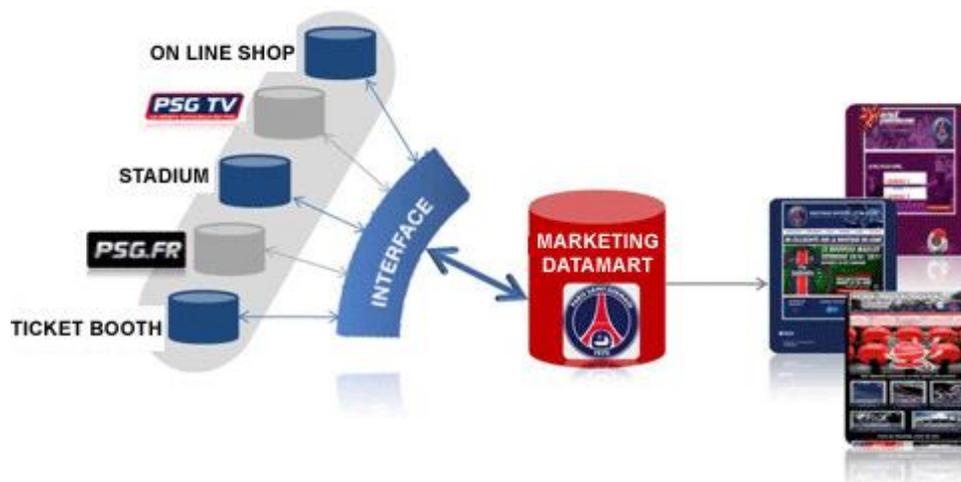
The Outcome

The PSG marketing datamart benefits from real-time synchronisation with the Cabestan marketing campaign management tool, including the segmentation engine.

In layman's terms, it means the PSG Marketing Department receives real-time updates of their fans' activities. This allows them to send out more sharply targeted communications to their 3 million plus supporters.

Switching to a relational database has enabled Paris Saint-Germain to:

- Develop deep customer knowledge, gained by capturing multi-channel behaviour, allowing PSG to propose new products and services to their fans

- Deploy a genuine online customer relations programme

- Consistently increase their sales

All of this came about through the use of a more sophisticated database in order to have a true 360° view of their customer base.

What PSG have learned is that the more you understand your customers, the more targeted your communications with them can be, which results in greater loyalty to your brand.

Loyalty to your brand, played out as loyalty to your favourite football team, can not only result in a unified fan

base, but makes for pretty good business.

So, what can you learn by listening to 3 million fans?

Quite a lot.

II. Database Keys

How do you define a unique client record? This is an important thing to get right – no customer likes having their details incorrect or receiving multiple marketing communications.

Unique Record

A database is a way of holding data collectively in one place, but how do you identify each unique record?

Through the use of a *primary key*.

A primary key is assigned to each record as a unique identifier, linked only to that record. This allows you to sort and identify data.

Consider this sample database:

Customer ID	Surname	Name	Town
0123	Smith	John	Leeds
0124	Smith	Sally	Leeds
0125	Smith	Fred	Manchester
0126	Smyth	Fred	Manchester

What is unique about each of these records?

The only thing unique about each record is the Customer ID number, so that would be used as the primary key. In this way, we know that customer 0123 is always John Smith of Leeds. The other data fields have duplicate data, so they wouldn't be a unique identifier.

If we searched in our database for Smith, we would come up with duplicate records. If we searched for Manchester, we would come up with duplicate records.

But there is only one customer 0123. That is the unique identifier and is our primary key.

Choosing a Primary Key

Selecting what to use as a primary key is a very important decision for any new database. You must ensure that whatever is used will always be unique.

Ask yourself whether there is any chance of a past, present or future record sharing this attribute. If there is any possibility of this, then it is not good for a primary key.

For this reason, something like postcodes would not be a good primary key.
There is a possibility at some point in the past, present or future that someone in your database might have the same postcode, so it doesn't identify them in a unique way.
A birthdate could be shared and even an email address isn't good since many people have multiple email addresses.

Good practice is to use an automatically generated number which is unique for each new record. This eliminates the risk of duplicate identifiers.

Once you have identified the primary key, the database management system will ensure that this field remains unique and will cause any duplicate entries to fail.

Flat Database

A *flat database* has only one record per line with one primary key. It is the format of many basic databases (think of any Excel spreadsheet which is a flat database structure).

As long as you are looking to store simple information or retrieve it in straight forward ways, it is perfectly acceptable. However, if you are looking to delve into your database to create segmented subsets, it is limited in the amount of profiling you can do.

It's also ripe for containing duplicate records.

Duplicate Records

The only field which won't allow duplicate information is your primary key field. So if you are automatically generating customer numbers, you could end up with the following database:

Customer Id	Surname	Name	Email	Street
0123	Smith	William	William.smith@hotmail.com	12 Sunshine Street
0124	Smith	W	Wsmith@gmail.co.uk	12 Sunshine Street
0125	Smith	Bill	Smith_bill@yahoo.com	12 Sunshine St

What's the likelihood that these are the same customer who has just registered with multiple email addresses since he can't remember which one he set the account up with?

When you send out your newsletter, he likely receives it three times.

How do you avoid the duplication of data? How do you recognise a unique client?
A database with more than one primary key helps to eliminate some of the potential duplication within your database.

Relational Database & Foreign Keys

It became apparent that a new kind of database structure was desirable which allowed for multiple keys and more interplay between data.

In order to run more complicated queries of your database to come up with more narrow subsets you need to be able to search and refine the data in different ways. It was for this reason that *foreign keys* were introduced.

A foreign key is used to create a relationship between different tables.

Look at this example:

Customer Table		
ID No.	**Name**	**City**
0123	Smith	Leeds
0124	Jones	London
0125	Field	Norfolk

Sales Rep Table		
City	**Team**	**Salesperson**
Leeds	C	Jim
London	A	Alice
Norfolk	B	Ted

In this example, both the ID No field in the Customer Table and the City field in the Sales Rep Table are primary keys. They are unique to that record.

The highlighted column, the City column in the Customer Table, is the foreign key field as it refers to the Sales Rep Table.

This field does not have to be unique as there can be more than one customer living in Leeds; however the relational database enforces referential integrity in the foreign key field to guarantee that each of the entries in this City column correspond to a primary key entry on the Sales Rep Table.

More tables are added to contain other pieces of information such as previous customer orders, responses to email campaigns or whether they have signed up for your loyalty card scheme.
In time this customer record is fleshed out with both declared data and behavioural data to create a more detailed customer portrait.

Composite keys

In order to further define one unique customer record, in a relational database you can make your key up from data from multiple columns.

We could have a composite key which is made up of first name, last name and loyalty card number (for instance) which would give you a much greater probability of identifying a unique customer and eliminating duplicate information.

What are the advantages?

Using a relational database, with multiple keys linking the data allows you to:

- Combine data
- Run complicated queries using SQL (Structured Query Language)
- Segment your database

In the example above you can see how Alice, your sales representative in London might use this database to find out details of local customers who haven't had a sales call or who have ordered a high end item and would welcome a follow up call. Or determine who hasn't ordered from you in some time and might warrant a discount voucher.

Identifying your unique customers allows you to market to them in a more unique way which can have a positive

impact on the success of your company.
Connecting Various Information Systems.

III.   Connecting Various Information Systems

What Data? What Rules?

Imagine these scenarios:

1. You subscribe to car insurance. In order to process your application, the insurance company generates a contract number which is used as your customer ID in their CRM.
Six months later you decide you also need to take out house insurance and you go back to the same company and apply online for house insurance.
Like many people you probably have several email addresses and you use a different email account on this new application.
A new contract number/customer ID number is generated for you for your home insurance. They now hold two records for you with many of the same details: address, name, credit card details, but two different email addresses. When the time comes to send you their newsletter, which email do they use?

2. You hold an account with a major online retailer where you order books and video games.
From time to time, your wife uses your account to sign on and order DVDs, CDs and books in areas that interest her.
When prompted, she enters her own email address as a confirmation email address, but it is   still under your account.
So what happens when they send out emails to suggest products you might be interested in?
Do you receive offers for high heel shoes and baby books or for Playstation games and football annuals?
Should their system flag up the anomalies in purchasing patterns and confirmation emails and delineate two separate users under the same account?

3. When shopping instore you are offered a loyalty card, which you duly sign up for by giving over your email address.
The store is then tracking your instore purchases in their database.
At a later date you go onto their ecommerce website where you set up an account.
Two things might happen: you might remember you already have a loyalty card and use that number (although you might provide a different email address) or you might forget your existing loyalty card and set-up a new online account.
Either way this information will be stored in the ecommerce database. Now when the data is poured into the datamart (central database) they have multiple data for one customer.
If they go to run an email campaign, which email address do they use? If the customer has signed up for two accounts with the same email address, can they identify this? How do they remedy this?

Human behaviour

All of these scenarios flag up the fact that human behaviour is inconsistent.

While databases are built on structure, unique identifiers and relationships between data, human behaviour is a bit messier.

We forget. We get mixed up. We do things too quickly. Our circumstances change.
People are inconsistent, while databases love consistency.

How do you bridge the gap?

It comes down to planning what data you are going to use for your marketing campaigns and what rules you are going to apply to that data. This is where an experienced and knowledgeable service provider can really help you to plan your marketing campaign effectively. Experience is the teacher of what data to use and what rules to apply to it in order to maximise your customer data.

Let's look at a few points in relation to data selection. This diagram can help us to understand what is happening:
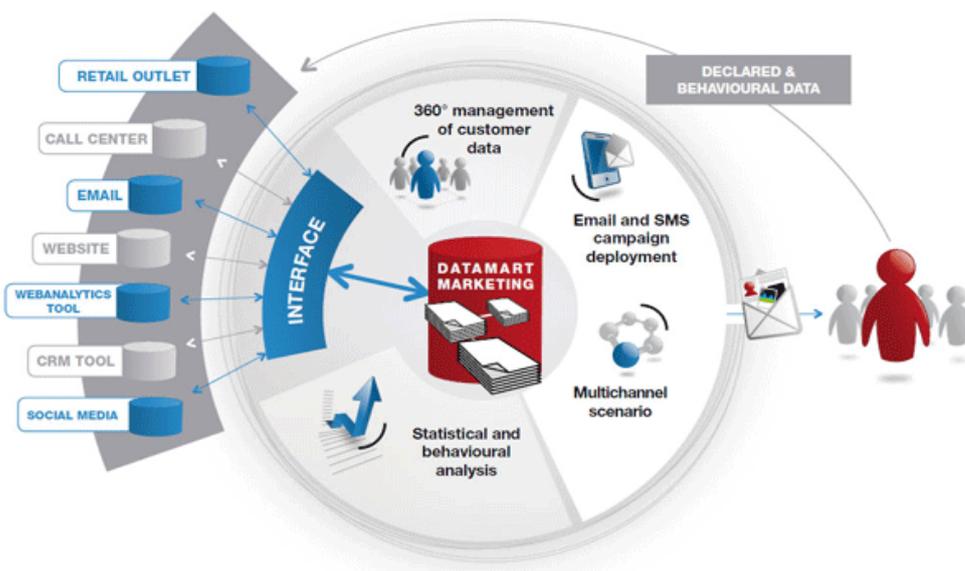
ETL

Extracting data

To the left of the diagram are some of the contact points where you might be gathering data from your customers. Each of these contact points likely saves information to its own database. Each database may have a different structure or code the data differently.

Your first decision is what data you are going to extract. This will depend on the desired outcomes of your marketing campaign. Right data, right time will be determined by your marketing scenario.

Rules are then set up in the marketing campaign management tool as to what data is extracted from which database.

Transforming data

The next step is transforming the data. This step looks at what rules will be applied to the data so that it becomes useful for your scenario. As the data may not be stored in the same way from one database to the next, you may need to look at transforming it so that you are comparing apples with apples rather than apples with oranges.

At this point, you may also want to look at deduplication of the data – a process which helps to eliminate duplicate data in your database and solve many of the problems highlighted in our opening scenarios.

This is achieved by running queries for groups of records which share similar traits and examining them further to see if they are duplicates. For example you could run a search comparing last names and addresses looking for duplications. If that came back with too many records you could add telephone number to the mix as a way of refining the results to be able to find and eliminate duplicate records. You need to test for the right combination of comparisons in order to get the best results.

This process can also flag up anomalies in records such as multiple email addresses. A rule can then be set as to which email address will be used. This will depend on your marketing scenario. If you were looking to push online sales, then you might favour emails collected through your ecommerce site, whereas if you wanted to push store sales you might favour emails collected instore.

Loading data

Converted data is now entered into your marketing datamart ready for your marketing campaign.

With automation, and the right skills to set it up, this process can happen quite quickly and before you know it your raw customer data is ready to drive your next marketing campaign while dealing with some of the inevitable pitfalls mentioned in our scenario cases.

Chapter 3 LEGALITIES OF HOLDING CUSTOMER DATA

I. Case Study: 2.3 Million Reasons To Take Data Protection Seriously

If you are holding any customer data, you need to give serious thought to issues of security. It's vital that you make provisions for the secure handling, storing and transport of this sensitive customer information.

Think you can blag your way through it? Then read on…

Zurich Insurance

Zurich Insurance's UK arm was recently slapped with a fine of £2.3 million by the Financial Services Authority (FSA) after they lost 46,000 customers' personal details. The information was en route to South Africa for data storage when it went missing.
In some cases the personal details included customer bank account and credit card information. Shockingly, Zurich didn't detect the loss until one year later, at which point they had to notify customers.

Chief Executive, Stephen Lewis admitted, "this incident was unacceptable."

The FSA's damning report states: "Zurich failed to take reasonable care to ensure it had effective systems and controls to manage the risks relating to the security of customer data resulting from the outsourcing arrangement. " The report added that, "the firm also failed to ensure that it had effective systems and controls to prevent the lost data being used for financial crime."

Mr. Lewis of Zurich said that the unfortunate incident "served to remind us of the need to strive to continually to improve the ways in which we seek to protect customer's data.
" By admitting their mistake, and settling during an early phase of the investigation, Zurich benefitted from an adjustment of their original £3.25 million fine down to the still hefty £2.3 million.
"Zurich UK has let its customers down badly," said Margaret Cole, the FSA's Director of Enforcement and Financial Crime. She added that Zurich "failed to oversee the outsourcing arrangement effectively and did not have full control over the data being processed by Zurich SA.

So What?

This is not an isolated case. Previously the FSA have fined HSBC, Nationwide and Norwich Union for their own data loss incidents.

The FSA aren't the only ones dishing out fines for mismanaging of customer data.

From April 2010, the Information Commissioner's Office (ICO) have the right to issue fines of up to £500,000 for serious breaches of the Data Protection Act. This is a big jump from their previous maximum fine of £5,000. However, the Information Commissioner asked for a jail sentence to be available to them for the mishandling of customer data – although it wasn't granted at this point in time, it is a suggestion of the seriousness with which they take this issue.

What this illustrates is that the watchdogs are getting serious about companies' obligations when it comes to the handling of customer data.

EU Regulations

The UK still falls short of EU regulations when it comes to data protection standards and the European Commission has given them a strict directive to increase privacy regulation and privacy protection or face appearing at the Court of Justice.

European data protection is covered by the Data Protection Directive of 1995. The UK is missing the mark on two crucial fronts:

1. The UK doesn't have sufficient authority to check other countries' data protection practices. It is imperative that they have the necessary bite to do this before they allow international data transfers.

2. The UK doesn't have the authority to make random checks on people or data processing/holding organisations. When fines are levied, they don't have the authority to enforce them.

These are both issues which must be addressed in order to further protect UK customer data. A fundamental right within the EU Charter, and backed in the Lisbon Treaty, is an individual's *right to privacy and protection of personal data.*

Serious Issue

A recent survey carried out by Cyber-Ark Software found that 65% of City workers are unaware of fines for 'deliberate and negligient' breach of personal data and 64% carry data on mobile devices, with only 12% using encryption.
In 2007 HM Revenue and Customs hit the headlines when they were forced to admit that they lost two CDs containing child benefit records of 25 million people in their internal mail service. The records included names, addresses, employment and bank details. Not only did the blunder result in a spectacular amount of negative press for HMRC, but it cost its Chairman his job.

This Relates To You

Whether you're a mom and pop shop or a major online retailer, these are issues which you must get to grips with.

II.   Legalities of Capturing and Storing Customer Data in the UK

We've seen that there are serious reasons to be aware of issues relating to the capturing and storing of customer data, so we will look more closely at the legalities surrounding personal data.

Areas of Concern

There four main areas concerning customer data which we need to be aware of:

1. Collecting personal details online (for instance via an application form or creating an id)

2. Use of cookies and tracking IP addresses to target content to individuals

3. Use of collected personal data to market goods and services

4. Use of cloud computing in the processing of customer data

Data Protection Act

Summary

The Data Protection Act (DPA) of 1998 places legal obligations upon organisations for the collection and handling of customer data.
(Note that these are the minimum legal requirements - next we will consider best practices which go above and beyond these bare requirements.)

The DPA applies to *personal data which allows you to identify a living individual.* The main provisions of the DPA require that:

- Info is only collected for a particular purpose
- Data is kept secure
- Data is relevant and kept up to date
- You only collect as much data as you need and only hold it for as long as you need it
- Once data is no longer required, it is deleted or disposed of securely

The customer has the right to access personal data held about them, the right to correct this data if it contains errors, and the right to stop this data from being used for marketing purposes.
You must comply with any such requests from a customer within a reasonable amount of time (up to 40 days).
You must comply with the DPA from the moment you collect customer data through to when it is returned, destroyed or deleted.

Data Controller

If you and/or your company are handling customer data, you may need to register with the Information Commissioner's Office (ICO) as a data controller. This is a statutory requirement and failure to do so is a criminal offence. Once registered, you will need to renew it annually. Most organisations who handle personal data are required to register - there is an online assessment at www.ico.gov.uk which will help you determine if you are exempt.

The data controller (whether an individual or representing an organisation) is responsible for all held data and if it is determined that the Data Protection Act has been breached, it is the data controller (or his/her organisation) who will be subject to either prosecution or enforcement action.

It has become increasingly common to use a third-party provider for all, or some, of your data handling requirements; however, if you do so, you are required to have a written contract in place and the supplier's

security provisions must meet or exceed your own data protection procedures (meaning meet or exceed the DPA requirements). You are liable for any breaches of the DPA carried out by a third party handler.

If you outsource handling of data to any organisation outside of the European Economic Area, there must be an adequate level of security in place. This applies both to the transport and handling of data.

Specific Wording

The DPA (1998) states the following eight responsibilities:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

If you are planning any electronic marketing campaigns you should be aware of the Privacy and Electronic Communications (EC Directive) Regulations Act of 2003 which states that you can only engage in unsolicited marketing if you have received the recipient's permission.

The exception to this rule is the 'soft opt-in' which allows you to send marketing communications if the following criteria have been met:

- You have obtained customer details during either negotiations or a sale with that customer
- The messages are for marketing your similar products and/or services
- They have the chance to refuse your marketing when their details are taken AND there is a simple way

for them to unsubscribe in all communications.

The final requirement is that when you contact them, you must tell them who you are and provide a clear way for the customer to contact you.

An Ounce of Preparation....

While this might seem a bit daunting, a bit of preparation and a small amount of monitoring should keep you the right side of the law.

The main thing is to be sure that your collection and handling of personal data is always fair, transparent and acceptable to the person whose details you hold.

Next, we'll look at how you can implement some of these legalities through best-practice behaviours.

Further Advice

There is plenty of excellent advice available on the website of the Information Commissioner's Office at www.ico.gov.uk.

III.   Best Practice Guidelines for Collecting, Storing and Using Customer Data

We've looked at the legalities of data holding / processing and those related to direct marketing. Now we will look at best practices which will ensure you keep your customers happy and stay on the right side of the law.

Data Protection Act

Best Practice Guidelines for the Capturing and Holding of Customer Data

Let's remind ourselves of the eight main principles (from the Information Commissioner's Office Guidelines):

Personal information must be:

- fairly and lawfully processed
- processed for specified purposes
- adequate, relevant and not excessive
- accurate and, where necessary, kept up to date
- not kept for longer than is necessary
- processed in line with the rights of the individual
- kept secure
- not transferred to countries outside the European Economic Area unless the information is adequately protected.

Collecting Customer Data

Best practice guidelines include:

- Personal data should only be collected when it is necessary. It is considered bad practice to ask for someone's name and email just to look at your website. You shouldn't collect personal data too early in the customer relationship.

- Be clear with customers what information is required and why.

- Likewise, make it clear what information is optional and what it may be used for.

- Information collected must correspond with your business needs. You should not collect information arbitrarily.

- From time to time, it is advisable to perform an information audit to determine if you require all the information you are currently collecting.

- If not, then you should remove those fields from your form and delete any existing information in those categories. You should not keep information which you do not require.

- Any surplus or out of date information should be deleted in a way that is secure and permanent.

- If you can carry out your business without holding information which specifically identifies an individual, then you should do so. For example, do you need to store their entire IP address or could you remove the last 8 characters (final octet) which identifies the specific computer? Can you work with partial postcodes instead of full addresses to give you general regional information rather than specific addresses?

- Have a clear privacy notice on your website which spells out in easy to understand language what information you are collecting and how it will be used.

- If your website targets vulnerable communities, such as children, you need to be very careful about collecting personal data where your respondent may not fully understand the consequences of what you are asking for - it may be appropriate to seek parental consent.

- Be open about your marketing techniques (including the use of cookies) and allow people to opt-out. Being clear about what happens when someone accesses your services, how information about them is collected / analysed and what it is used for will help you build respect and trust between you and your customers. Always treat them fairly.

- Let customers know how they can use their browser settings to set limitations on how much information they want to share.

- It's good practice to allow access to some of your website or services even if a visitor refuses your cookie or declines registering their details.

- Sharing customer data with other companies/organisations should not be a default setting – it should be an opt-in option.

- Default privacy settings should strike a balance between an individuals' right to privacy and the appropriate collection of data for customer segmentation. Err on the side of caution.

Storing Customer Data

The key is to make sure you've appropriate security measures in place to protect personal information against any unlawful or unauthorised use. You must also make provisions to prevent any accidental loss, destruction or damage to customers' personal details.

Some best practice guidelines:

- Know what data you possess so you can plan the appropriate level of security. If the data you hold cannot specifically identify a particular individual, or is information which is publicly available, then your security provisions don't need to be as stringent as where you hold identifiable customer details or details which are confidential, valuable or sensitive. You must consider the possible risk to the individual and/or your organisation if the data was lost / stolen and plan accordingly.

- Someone in your organisation needs to be responsible for this data. Make it within someone's responsibilities to plan for and monitor any storage and use of customer data. One of their first tasks is to plan and implement a security policy for how the organisation will handle and store customer data.

- Do periodic checks of your security systems to be sure they remain fit for purpose.

- Staff need to be trained in the appropriate handling of customer information including third-party requests for information and how to handle them.

- Do a check of the security of your IT infrastructure, but also the security of your physical premises. Are hard copies of personal data kept locked up? Are laptops and any portable memory devices secured and their use outside of the office regulated? Is data encrypted if it's being transported in any way?

- Do think about how you are deleting and disposing of sensitive data. Shredding paper and overwriting or destroying hard-drives are necessary steps.

- Are your firewall and virus software kept up to date?

- When staff leave, ensure you cancel their log-in access and collect any laptops and storage devices (including blackberries and smartphones).

- The ICO office has an excellent document titled "Data Protection Good Practice Note – Security of Personal Information" which is worth reading for further details and contacts.

Customer Access to Data

Your customer has the right to know what data you hold on them, to make any corrections and to stipulate if they don't want to receive any marketing contact, so it is in your best interest to make it as easy as possible for them to do so.
Best practice would suggest that, where practical, you allow your customer to access their own data online and make corrections. It's important to point out that this only works where they have a secure log-in and password.

If the user is only identified by a cookie on their machine, there is no way of knowing if multiple users are accessing the same computer. It's your obligation to ensure that any personal data is only revealed to the person who owns it.

If customers do contact you to access or update their personal data, you are allowed to charge them up to £10 as a processing fee and you have up to 40 days to handle their request; however, best practice would suggest that neither of these are practical or desirable for retaining satisfied customers. Make it easy for your customer to find contact details for your company and respond to their requests promptly.

Make it easy for customers to either opt-in/opt-out of further marketing contact. Also make it simple for them to change their preferences at a later date. If someone sends an unsubscribe request, it should be dealt with promptly.

Third Party Handling of Data

If you're going to use a third party organisation to process or store your customer data, you should follow these guidelines:

- Choose your organisation carefully, looking for appropriate guarantees and experience in the secure handling of customer data.

- Ensure that any contracts with data handlers are enforceable both within the UK and the country in which the handler is located.
- Verify that appropriate security provisions are being applied.

- Have all their staff been appropriately security checked?

- Regular audits of the third party handler and their work are essential.

- Make it a requirement that any security breaches are reported immediately, as are any investigations by foreign governments or legislating bodies.

- Have plans in place for how you will adequately deal with any issues or problems which might occur. Think of the worst case scenarios and prepare for them.

- Be sure that all data transfers are encrypted.

- Don't forget that you are held responsible for any breaches of your customers' data.

Privacy and Electronic Communications Regulations Act

Direct Email Marketing Guidelines

The following guidelines will not only keep you in compliance, but will win you the trust of your customers:

- Aim for permission based marketing only – your customers will be much more receptive to material that they actually want to receive.

- Let you customers know for what purposes you are collecting their data. Make this statement easy to find and easy to understand. It's a good idea to get your customer to tick a box that they've read and understand this statement.

- It will win you more trust if you work with opt-in policies rather than opt-out (see below for more info).
- Make it easy for your customers to unsubscribe to future marketing correspondence and deal with unsubscribe requests promptly.

- Take complaints from customers seriously. It's a good idea to track them and review on a regular basis to see if common complaints are emerging.

- When you receive an opt-out request it might make sense to keep them on a suppress list rather than deleting them. You can run any future emails against this list to ensure you are not contacting someone who has asked not to be contacted.

- Should you have any security breaches which affect customer data, or discover any viruses/malware attacks, it's best practice to inform your customers promptly. It's also advisable to notify the Information Commissioner's Office.

- Take a look at further details on the Information Commissioner's website at www.ico.gov.uk

Opt-in versus Opt-out

It's important to acknowledge that there's a difference between someone not opting out of receiving your marketing communications and someone actually consenting to receive them.
Opt-in, where someone specifically chooses to receive your marketing, is far better in the long run for building loyal customers than using opt-out where the default setting is for them to receive your materials unless they un-tick an already selected box. For many customers it seems a bit underhanded.

It's far better strategy to have your marketing materials go into the hands of people who actually want to receive them and might act on them. The customer who hasn't opted-out and receives your material is probably not that likely to buy from you anyway.

Focus your marketing energies on customers who are interested in what you are offering.

If you do choose opt-out, make the wording of your statement easy to understand. The sample wording provided by the ICO is quite clear:
"By submitting this registration form, you will be indicating your consent to receiving email marketing messages from us unless you have indicated an objection to receiving such messages by ticking the above box."
It's important that your customer understands clearly that they are giving their consent and what they are consenting to. Keep the process and the outcomes transparent at all times.

Be Clear

Be clear with your customers. Treat them fairly and trust that this will pay off in long-term loyalty. It's simply good business to act both ethically and within the limits of the law.

# APPENDIX

I.   About Cabestan

Cabestan is the specialist in consumer engagement by email.
Cabestan has a range of solutions that enable businesses to manage their entire customer relationship.
Cabestan solutions enable you to establish a 360° view of customer data and plan and automate personalized marketing actions, to achieve greater marketing effectiveness.

Cabestan platform, in SaaS mode, enables you to setup the following solutions:
- 360° client's data management
- EMAIL and SMS campaigns deployment
- Multi channel campaign management
- Statistical and behavioural analysis
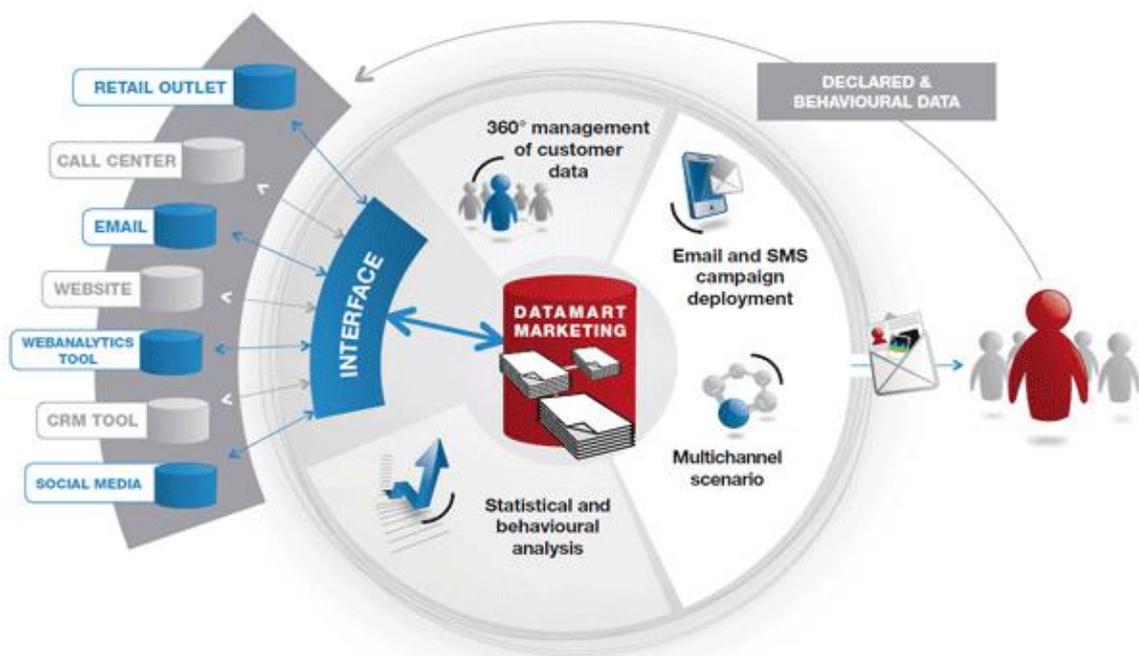
Some of clients' Cabestan: Axciom, General Electric, Toys'r'us, Estee Lauder, Cho yung, Symantec, Yves Rocher, Kiabi, SNCF, GDS SUEZ, NAF NAF, Renault...

To learn more:

CABESTAN Ltd
5 St John's Lane
London EC1M 4BH
Tel: +44 (0) 207 250 4749
Fax: +44 (0) 700 594 6759
builttoperform@cabestan.co.uk
www.cabestan.co.uk
http://blog.cabestan.com