

# Best Practice in Information Security

BEST PRACTICE  
CAMPAIGN PLANNING  
CONSUMER SAFEGUARDS  
DESIGN CONSIDERATIONS  
DMA COMPLIANCE  
LEGISLATION  
RAISING INDUSTRY STANDARDS

1st EDITION



# CONTENTS

FOREWORD	4
1. BACKGROUND & INTRODUCTION	5
1.1 DATA PROTECTION AND RELATED LEGISLATION	6
1.2 ENSURE YOUR ORGANISATION'S SECURITY MEASURES ARE APPROPRIATE	7
2. INFORMATION SECURITY AND THE ORGANISATION	8
2.1 RISK ASSESSMENT	8
2.2 SECURITY MANAGEMENT	8
2.3 CONTROLLING ACCESS TO INFORMATION	8
2.4 TECHNOLOGY INFORMATION SECURITY	9
2.5 ENSURING BUSINESS CONTINUITY	10
2.6 DETECTING AND DEALING WITH BREACHES OF SECURITY	10
3. INFORMATION SECURITY AND THE WORKER	11
3.1 STAFF SELECTION	11
3.2 STAFF TRAINING	11
3.3 DISCIPLINARY PROCEDURES AND DISMISSAL	11
3.4 ACCEPTABLE USE OF FACILITIES	11
4. INFORMATION SECURITY AND THIRD PARTIES	12
APPENDIX 1 – BEST PRACTICE GUIDELINES FOR DATA TRANSFER BETWEEN PARTIES	13
BEFORE TRANSFER	13
SECURE FTP (OR SFTP)	14
FTP	14
PHYSICAL TRANSFER BY COURIER OR POST	15
EMAIL (AS AN ATTACHMENT TO NORMAL MAIL)	15

Thanks to the members of the Information Security Working Party, and DQM, a data value management organisation, for their help in providing the data management guidance.

## FOREWORD

### **The Information Commissioner**

I welcome this guide. The DMA have made great efforts over the years to encourage their members to comply with data protection law. They are right to emphasise the importance of information governance in maintaining public trust. This guide should help DMA members minimise the risk of security breaches, breaches which can all too easily undermine public trust. I welcome, in particular, the emphasis they place on the secure transfer of data.

**Richard Thomas**

Information Commissioner

17 February 2009

# 1. BACKGROUND AND INTRODUCTION

## 1.0 Background and Introduction

The contents of this guide are about providing advice and guidance on how to raise standards above the minimum of what is legislatively demanded of us. This guide is designed to enable practitioners to greatly improve information security processes in an increasingly demanding and sensitive area.

Data is at the core of Direct Marketing. However, it is also at the core of many of the problems facing the industry. Badly managed, insecure data governance will lead to data losses, public insecurity, adverse publicity and the distinct possibility of increased regulation. It is important to remember that when dealing with marketing data direct marketers are, in essence, being trusted by consumers (the data subjects) to care for their personal details. Those organisations who view data security as a necessary evil of our business practice, need to consider data security as a basic fundamental of our day to day activity. This guide will help you to bring these issues into stronger focus and as a result, hopefully, better day-to-day data governance.

The aim is to give customers and prospects full confidence that their valuable personal data is secure at all times in the direct marketing process.

# 1. BACKGROUND AND INTRODUCTION

## 1.1 Data Protection and Related Legislation

The simple fact is that the direct marketing industry has to comply with the law. The Data Protection Act 1998 (the ACT) governs all that we do as business people, but if you happen to be in direct marketing it is one of the most important pieces of legislation. The legislation is designed to protect the rights of the individual and ensure that any personal data that is held on them is processed and kept in accordance with the Act. The Information Commissioner's Office (ICO) takes a strong stance on ensuring compliance and the courts have fined a number of organisations for breaches of the Data Protection Act 1998.

The Data Protection Act 1998 contains at its core eight key principles. These can be found in Schedule 1 Part 1 of the Act with further explanation in Schedule 1 Part 2.

### Eight Principles

Personal data must be:

- Fairly and lawfully processed
- Processed for specified and limited purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than necessary
- Processed in accordance with the rights of data subjects
- Protected by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction, or damage
- Not transferred to a country outside the European Economic Area unless it has adequate levels of protection for personal data

Any organisation that fails to comply with the Data Protection Act 1998 leaves itself open to enforcement action by the ICO and the risk of being fined by the courts. The ICO has recently been given new powers under the Data Protection Act 1998, although the relevant section is not yet in force, to issue monetary penalty notices for breaches of the eight principles in the Act. There is also the risk of a private civil action for damages and reputation/brand damage.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 contain additional requirements for electronic marketing (phone, fax, email and SMS).

# 1. BACKGROUND AND INTRODUCTION

## 1.2 Ensure your organisation's Security Measures are appropriate

The Data Protection Act 1998 gives some guidance on what needs to be taken into account in deciding whether security measures are “appropriate” in Schedule 1 Part 2 paragraph nine and ten. These are:

The measures must ensure a level of security appropriate to:

- The harm that might result from a breach of security
- The nature of the data to be protected
- The reliability of workers having access to personal data

The above should take into account the state of technological development at the time, and the cost of implementing any measures.

Recital 46 of the Data Protection Directive 95/46/EC states that the technical and organisational measures to be taken by organisations should be taken “both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorised processing.”

As a result of this clause the Information Commissioner's Office encourages organisations to consider the use of privacy enhancing techniques as part of their obligations under the Act. Please see [/www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/privacy\\_by\\_design.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx) for further information.

The Information Commissioner's Office also states that “It is clear that there can be no standard set of security measures that is required for compliance with the Act. The Information Commissioner's view is that what is appropriate will depend on the circumstances, in particular, or the harm that might result from, for example, an unauthorised disclosure of personal data, which in itself might depend on the nature of the data. Therefore, companies need to adopt a risk-based approach in determining what measures are appropriate to their organisation's individual circumstances.”

It is important to note that to ensure a secure data processing environment it is important to take technical and management/organisational measures.

Equal consideration must be given to the security of personal data contained in physical records (paperwork etc.) as well as electronic data.

Don't forget that ‘processing’ includes all operations from collection to disposal, so security must be looked at from a wide perspective and relevant measures should be put in place to meet all foreseeable security issues.

The ICO does acknowledge that there are many causes of security problems, including carelessness by employees and human error. Where such errors do occur DMA members are advised to contact the legal department to discuss how best to handle the specific situation. A detailed log and evidence trail should be recorded however in case the ICO does receive a complaint from an individual.

## 2. INFORMATION SECURITY AND THE ORGANISATION

### 2.1 Risk Assessment

The organisation should be capable of demonstrating that risks are routinely considered and subsequent remedies and controls are introduced where appropriate.

Standard risk assessment and risk management techniques involve identifying potential security threats to the system, the vulnerability of the data processing system to those threats and the counter-measures to put in place to reduce and manage the risk. In many cases, a simple consideration of these matters will be sufficient. However, should you require more detail, the Information Commissioner's Office details formal methodologies to assist organisations in the assessment and management of the security risks to the system. See [www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_complete\\_audit\\_guide.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_complete_audit_guide.pdf) for an example of a formal audit manual.

### 2.2 Security Management

The organisation should have a security policy setting out management commitment to information security within the organisation.

Individual responsibilities for the implementation of the organisation's security policy should be clearly identified and included in job descriptions.

Sufficient resources and facilities should be reasonably available to enable that responsibility to be fulfilled.

### 2.3 Controlling Access to Information

Access to the building or rooms where personal information is available should be controlled. Casual passers-by should not be able to read personal information off screens or documents.

Printed material containing personal information should be disposed of securely, for example, by shredding. If an outside contractor is used, then there must be a data processing contract in place. This waste material should also be disposed of securely and in an environmentally sensitive way, not put into landfill.

Access to personal information should be controlled through a central policy and as a basic principle user access should be limited to the minimum required for performance of duties.

User rights to information (both electronic and physical) should be routinely reviewed. Visitors to areas containing personal information resources should be accompanied by suitable staff at all times.

Personal data should only be retained for as long as is required – a policy should be in place to ensure that redundant personal data is removed from systems as quickly as is practicable.

## 2. INFORMATION SECURITY AND THE ORGANISATION

### 2.4 Technology Information Security

Passwords should be known only to authorised people and the passwords changed regularly. Ideally such password changes should be mandatory and should prevent re-use of a previously used password. Passwords should not be shared.

Passwords should give access to only those personal data with which that worker should be concerned, not to all levels of the system.

Passwords throughout the organisation should be “strong”, ideally containing numeric characters, a mixture of upper and lower case, not based on a dictionary word and a minimum of eight characters.

There should be a procedure for cleaning media, such as tapes and disks, before they are reused or disposed of. If an outside contractor is used, then there must be a data processing contract in place.

Old or redundant IT equipment that might contain data (such as old PCs etc) should be disposed of in a secure and environmentally sensitive way.

There should be a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data.

Personal data should not be stored locally on users hard-drives or other media. If this is unavoidable then these drives should be fully encrypted with regular key changes.

Laptop and other portable computers containing organisational information, including personal information relating to employees and customers, should always be encrypted.

Network devices (computers, laptops and servers) should be protected from virus and other malware attack by suitable software. This should be updated as frequently as necessary to retain good protection.

Devices should be set to automatically go into ‘locked mode’ if left unattended for more than a few minutes and require passwords to be entered for them to be unlocked.

Unauthorised devices should be prevented from attaching to the network by suitable end-point security software. These devices should include any device capable of storing data i.e. memory sticks, MP3 players and I-pods, cameras, mobile telephones etc.

Restricting physical access to wireless networks is difficult and therefore the use of such networks should be discouraged, but where implementation is unavoidable then strong encryption should be used with frequent key changes.

## 2. INFORMATION SECURITY AND THE ORGANISATION

Access and other security logs should be routinely reviewed so that unusual and unauthorised activity can be investigated.

IT systems should be adequately maintained. It is important that such systems have the latest security patches applied.

### 2.5 Ensuring Business Continuity

Precautions against burglary, fire or natural disaster should be adequate. Appropriate business continuity plans, including IT back-up plans, should be in place to cover total loss or damage to site and loss of workers.

The system should be capable of checking that the data are valid and initiating the production of suitable back-up copies. Full use should be made of these facilities.

Back-up copies of all the data should be stored separately from the live files, preferably off-site. Back-ups should be taken as frequently as is required and should always be encrypted and securely stored.

### 2.6 Detecting and dealing with Breaches of Security

Systems should keep audit trails so that access to personal data is logged and can be attributed to a particular person.

Breaches of security and potential breaches should be properly investigated and remedied; particularly when damage or distress could be caused to an individual.

Suitable controls should be put in place to ensure that a repetition of a breach should not be possible.

## 3. INFORMATION SECURITY AND THE WORKER

### 3.1 Staff Selection

Proper weight should be given to the discretion and integrity of workers when they are being considered for employment or promotion or for a move to an area where they will have access to personal data. Consideration should be given to checking references, curriculum vitae completeness and proof of professional qualifications when required.

### 3.2 Staff Training

Workers should be aware of their responsibilities towards information security.

They should have been given adequate training and their knowledge kept up to date.

All workers should have signed appropriate confidentiality agreements and fully understand them before signing.

Workers should immediately report security weaknesses and breaches as and when they may observe them.

All workers must clearly understand the procedure for reporting breaches of security (including malware, virus and all other types of breach).

### 3.3 Disciplinary Procedures and Dismissal

Disciplinary rules and procedures should take account of the requirements of the Data Protection Act 1998. These rules must be enforced.

A worker who is found to be unreliable or is no longer a worker in the organisation, should have his or her access to personal data withdrawn immediately.

### 3.4 Acceptable Use of Facilities

Workers should be aware that personal data about customers or workers must only be accessed for business purposes and not for their own private purposes.

An "Acceptable Use" policy must form part of the workers conditions and should be clearly explained to the worker.

There must be a procedure covering the temporary removal of personal data from the organisation's premises, for example, for workers to work on at home. This should detail what security measures individual workers are required to take in such circumstances. This removal of data should always be formally authorised.

## 4. INFORMATION SECURITY AND THIRD PARTIES

Responsibilities for security should be clearly defined between an organisation and its suppliers or customers.

The Data Protection Act 1998 introduces express obligations upon organisations where the processing of its personal data is carried out by another organisation on its behalf. In order to comply with this the organisation outsourcing the work ('data controller') must:

- 1) Choose a service provider ('data processor') that provides sufficient guarantees in respect of the technical and organisational security measures it takes.
- 2) Take reasonable steps to ensure compliance with those measures.
- 3) Ensure that the processing is carried out under a contract, which is made or evidenced in writing, under which the service provider is to act only on instructions from the organisation outsourcing this work. The contract must require the service provider to comply with obligations equivalent to those imposed on the outsourcing obligations by the seventh principle (security) of the Data Protection Act 1998.

Suitable best practice to help compliance with this must include:

A written outsourcing agreement detailing the parties' respective obligations under the Data Protection Act 1998 and including confidentiality obligations and responsibility for information security. If these points are not covered in the outsourcing agreement then a separate data processing agreement and confidentiality agreement must be put in place.

Audits or inspections of third party premises in order to assess the strength of information security should be undertaken before the work is outsourced and during the contract where appropriate.

Data transfer to be as secure as is possible (see notes in Appendix 1).

If the service provider is located outside of the European Economic Area (the 27 Member States of the EU plus Iceland, Liechtenstein and Norway) then the organisation must ensure that a suitable level of security for personal data will be provided by the service provider. This has to be evidenced by written contract and supported, if required, by suitable site audit and assessment. This level of security should be at least as strong as is required under the EU Data Protection Directive.

Suitable best practice to help compliance with this may include:

All data transferred into and out of the organisation should be logged.

Data tracking by the insertion of unique 'seed' addresses into every data or list extract is easy and strongly advisable. This is to monitor subsequent use of the data after transfer and highlight misuse quickly. It may also support any legal action that may follow.

# APPENDIX 1 – BEST PRACTICE GUIDELINES FOR DATA TRANSFER BETWEEN PARTIES

The following appendix has been prepared by the List and Insert Forum with guidance and support from a member company. They are intended to offer a minimum requirement for the technological processes that should be followed by DMA members for transferring data between two locations. Examples of the locations are in Appendix 1. The aim is to ensure that all parties in the chain of data transfer are following these basic minimum recommendations.

The document does not address legal, compliance or any other procedural legislation but is simply an attempt to provide some basic best practice advice on technological measures to protect the security of data transfer. This document only covers recommendations for data transfer for countries within the European Economic Area (EEA), the 27 Member States of the European Union (EU) plus Iceland, Liechtenstein and Norway. If the third party is outside of the European Economic Area (EEA) the 27 Member States of the EU plus Iceland, Liechtenstein and Norway, then members need to be aware of the eighth principle of the Data Protection Act 1998, which governs the transfer of data outside the EEA. To comply with the law, data will only be allowed to be exported outside of the EEA to countries that have an adequate level of data protection or where contractual arrangements are put in place between the organisations involved that ensures an adequate level of data protection. Members must not transfer personal data to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for individuals, or where an alternative means of ensuring adequacy exists, such as through an appropriate contract. A Safe Harbour Agreement currently operates between the US and Europe. US firms which have agreed to operate under the Safe Harbour Agreement pledge to protect data from European partners in accordance with European law. For up-to-date information about which countries have been granted adequacy status please visit [ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm). Members transferring data out of the EEA are strongly advised to consult the DMA's Legal Department or their own legal advisers.

## **Before Transfer**

Before the transfer of information is undertaken it is advisable to consider:

- Is the transfer really necessary? Don't move it unless you really need to!
- Am I transferring more than is needed? Reducing the amount of data moved reduces the risk and consequential damage if lost – this could mean sending only those records that are needed or only those fields that are required i.e. if the data transfer is for statistical analysis could it have any personal details removed prior to the transfer and still be used to complete the work effectively?
- Are we confident that the recipient of the data is authorised to receive and process the data?
- Do all parties have the correct Data Protection notification?

# APPENDIX 1 – BEST PRACTICE GUIDELINES FOR DATA TRANSFER BETWEEN PARTIES

Having ascertained that a transfer is required and reduced the data to the minimum necessary it is important to consider HOW the data is transferred. Many methods of moving data from place to place are available but the main ones to consider are as follows (they have been listed in order of preference for guaranteeing the maximum level of security):

## **Secure FTP (or SFTP)**

All the data is encrypted before it is sent across the internet or network. With SFTP, sending usernames and passwords in clear text is a thing of the past, as all transferred data is fully encrypted. Furthermore this is completely transparent to the user.

SFTP Software is available at reasonable cost from many suppliers.

It is recommended that the files to be transferred are compressed and separately encrypted before transfer, even though the transfer itself is encrypted, so that access to the data is still controlled once on the destination server.

Passwords used for both the SFTP session and the File Compression should be unique and strong – by that we mean at least ten characters, containing both numbers and letters and not based on a dictionary word. Ensure that passwords are exchanged separately and securely. Passwords should also expire after a suitable time period and data should be removed from servers as appropriate.

## **FTP**

This is the internet standard for transferring data from a client to a server. With FTP all data is passed back and forth between the client and server without the use of encryption. This does makes it possible for an eavesdropper to listen in and retrieve confidential information including login details.

This is not as secure as SFTP but if the guidelines below are followed is probably better than the remaining methods listed.

It should be mandatory that files to be transferred via FTP are compressed and separately encrypted before transfer – this is to protect the data if intercepted in transit in addition to the reasons listed above. It is even more important that the rules above relating to passwords and removal of data are followed.

# APPENDIX 1 – BEST PRACTICE GUIDELINES FOR DATA TRANSFER BETWEEN PARTIES

## Physical Transfer by Courier or Post

Cutting CDs and tapes and other media forms can mean that data gets misplaced or delivered to the wrong person. If this is the only method of data transfer available then the following guidelines should be followed:

- Ensure that the data is minimised (depersonalised if possible!)
- Protect the data with strong encryption
- Strong and Unique passwords sent separately to the recipient
- Use a courier with a specific data service if possible
- Have a good contract with the courier service – if this is to be regular and the data is high value consider asking to see the courier's security policies
- Advise the recipient when the data will arrive and by which carrier
- Confirm delivery with the client
- Ensure that signatures and receipts are readable and available quickly

## Email (as an attachment to normal mail)

This is not desirable and should be avoided if possible. The main problem with email is that in most cases the message is not transmitted directly from sender to receiver – there may be several server-to-server hops for the message – each one of which is a potential resting place for a copy of the original message. Additionally a copy of the data sent is likely to remain in the accounts of the sender and recipient and on the mail servers of the respective locations. If this kind of transfer is unavoidable then the following guidelines should be undertaken:

- Ensure that the data is minimised (depersonalised if possible)
- Protect the data with strong encryption before attachment
- Strong and Unique passwords sent separately to the recipient (preferably by telephone rather than another email message)
- Ask for a tracking receipt so you know when the email is opened
- Delete the attachments/sent email after the message receipt is confirmed
- If data is to be emailed then it should be sent to a dedicated data delivery address – data should not be delivered to a personal/named email account; organisations should have a specific email account for data with restricted access

The Direct Marketing Association (UK) Limited  
DMA House, 70 Margaret Street  
London W1W 8SS

T: 020 7291 3300  
E: [dma@dma.org.uk](mailto:dma@dma.org.uk)  
W: [www.dma.org.uk](http://www.dma.org.uk)

