Guide to Data Protection and Confidentiality

Introduction

The Data Protection Act 1998 was introduced in October 1998 as a direct result of European legislation to protect the rights and freedoms of individuals

Its purpose is to control and protect personal information held both on computer systems and certain manual information

This is achieved through eight data protection principles which cover issues such as the collection, holding and notification of information and customers' rights of access to this information

Of course, the confidentiality of information has always been important - however, during recent years there have been changes in the way we undertake our day to day business which impact on data protection

These include:

- widespread use of telephone, facsimile machines and e-mail
- increasing use of personal computers both at work and at home
- open plan offices

These changes together with increasing fraudulent activity and extensive media publicity regarding matters of confidentiality require us to be even more vigilant than previously

Each one of us has an individual responsibility to keep information about our customers and colleagues confidential

Where a breach of confidentiality takes place, the Information Commissioner may take action against both the bank and the individual employee who caused the breach

These pages explain how the data protection principles affect all of us and how we can ensure that data remains confidential at all times

You may also wish to refer to the data protection procedures included in the Data protection and privacy BIM and the mandatory on-line training available on the UKi Intranet site
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Principles</td>
<td>3</td>
</tr>
<tr>
<td>Confidential Information</td>
<td>4</td>
</tr>
<tr>
<td>Handling Information</td>
<td>5</td>
</tr>
<tr>
<td>Individual’s rights</td>
<td>7</td>
</tr>
<tr>
<td>Danger Zones</td>
<td>8</td>
</tr>
<tr>
<td>Summary</td>
<td>11</td>
</tr>
<tr>
<td>Contact Points</td>
<td>12</td>
</tr>
</tbody>
</table>
Guide to Data Protection and Confidentiality

Data Protection Principles

1 - Process information fairly and lawfully treating sensitive data with extra care
2 - Only use the information for the purpose it was collected
3 - Ensure the information is adequate, relevant and not excessive for the purpose
4 - Keep information accurate and up to date
5 - Do not keep information for longer than is necessary
6 - Process information in accordance with the individual's rights
7 - Keep data secure
8 - Ensure adequate protection of information is provided before making transfers of data outside the European Economic Area
Guide to Data Protection and Confidentiality

Confidential Information

What is confidential information?

Confidential information is information which, if disclosed to unauthorised people or third parties, would:

- breach the confidentiality of our relationships with customers or
- breach relevant law or
- damage HSBC's business or competitive position

All information relating to customers and staff must be treated as confidential - this includes account numbers, addresses, balances, transaction details, employment records, date of birth or marital status etc

Who are unauthorised people?

Unauthorised people or third parties include anybody who is not entitled to have access to the information concerned

For example:

- If you inadvertently allow a customer to overlook another customer's balance, you have allowed an unauthorised disclosure of confidential information
- If you advise, or even just confirm, to a third party that a customer has a relationship with us this is a breach of confidential information
- If a husband and wife both have sole accounts with a branch of the bank, they may not necessarily be aware of each other's account - if you mention the account of one to the other you have breached the bank's duty of confidentiality

Any of these breaches could have serious consequences for the bank.
Guide to Data Protection and Confidentiality

Handling Information

Collection of information

- When collecting information you must always explain to the customer why we need the information and what we will use it for, this will normally be self-explanatory e.g. if a customer is applying for a loan, we need details of employment, salary, mortgages etc. to agree the facility
- You must not request or process information from a customer if it is not necessary for the purpose it is being collected
- Do not assume that you have consent to use information for all types of processing - if in doubt, check with your line manager before using data for a different purpose

Recording information

- Record information accurately
- Update records when you are advised of changes, or as soon as possible afterwards
- Ensure information is factually correct; never assume
- If you are recording your opinion about a customer or employee, it must be described as such and should not be derogatory or defamatory - remember that customers and staff have access to this information
- Do not use abbreviations which customers may not understand
- Ensure manual information is correctly filed and automated information is accessible to others to retrieve
- If you obtain information about an individual from a third party, record the source of the data - customers may exercise their right to instruct us to correct anything that is found to be inaccurate - we will then be obliged to instruct the source to rectify any inaccuracy if this is found to have an adverse effect upon the individual
- Do not use information held for the payment of direct debits and standing orders for marketing purposes

Using computers

- Do not store or process bank information on PC equipment not owned by the bank - similarly, the company's equipment should not be used to store private information - any exceptions to this rule must have prior consent from senior management
- Carefully position computer screens located in public areas to prevent casual onlookers from viewing
- Protect access to automated information by using passwords
- Lock or log off computer systems when not in use

Maintaining security

- Keep customer information confidential, unless you have authority to disclose the information or there is a specific legal requirement - remember local councils and police do not have an automatic right of access to bank information - in most circumstances a court order will be required before disclosure of information can be made - unauthorised disclosure may result in criminal proceedings against the bank or you personally - refer any queries to your line manager
• Keep customer information secure at all times, particularly when it is removed from the office - such information should never be left in a car - friends and family should never be allowed to read such information
• Follow the 'clear desk' principle by ensuring that confidential information cannot be seen easily - at night, lock away all paperwork, printouts, diskettes, customer records and other confidential information
• Undertake regular housekeeping routines and do not hold information for longer than is necessary - delete old documents when there is no reason to retain them - this applies to word-processing and spreadsheet documents held locally as well as centrally held customer and employee files
• Follow procedures for the retention of old books, documents and papers

Processing 'sensitive' data

• Sensitive data includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sexual life, alleged or actual commission of an offence
• The customer must fully understand what we will use the sensitive data for and, on most occasions, give consent before processing takes place - if consent cannot be obtained from the customer do not process the item without seeking further guidance from the Group Data Protection Office (GDPO)
• You should only record such information in exceptional circumstances where it genuinely helps our relationship with the customer - refer to your line manager if in doubt
• Do not use sensitive data for marketing purposes
• You must never disclose sensitive information over the telephone and must take extreme care not to disclose sensitive information accidentally

Examples of acceptable use of sensitive data

• An employee supplying personal details such as ethnic origin which is necessary for us to monitor equal opportunities.
• A customer providing health details to enable the processing of a life insurance policy.
Guide to Data Protection and Confidentiality

Individuals' Rights

Right of access to personal information

- Individuals have a right of access to automated and certain structured manual files (for example, a file with a customer name or account number on)
- You must act promptly on receipt of a request for information as the bank has 40 days to respond
- A request for information may result from the refusal of a lending facility, a dispute about data passed to a credit reference agency or from a general grievance with the bank - providing the customer with relevant file notes or giving further guidance could resolve the issue quickly before the customer becomes more aggrieved - refer to Group Data Protection (GDPO) before providing copies of any information
- When providing printouts containing personal data do not disclose third party information - if in doubt, check with GDPO

Right to prevent processing for purposes of direct marketing

- Customers have the right to object to receiving direct marketing in any form including direct mail, e-mail, telephone, text etc - when a customer gives an instruction for you to stop sending marketing material, annotate the customer record immediately to prevent further marketing approaches being made

Right to stop processing likely to cause damage or distress

- If customers suffer damage and distress caused by inaccurate data, they have a right to have their information amended, the processing stopped or deleted and in some cases they are able to claim compensation - the issue must be reviewed and appropriate action taken to rectify the problem within 21 days - act quickly by referring the matter to your line manager

Rights in relation to automatic decision taking

- Individuals have a right of appeal where an automated decision might have a significant effect upon them - where an appeal or complaint is made, a manager must review the automated decision within 21 days to establish the accuracy and fairness of the decision
Guide to Data Protection and Confidentiality

Danger Zones

This section highlights situations in day to day business where you could wrongly disclose information to unauthorised people if procedures are not followed or due care and attention is not taken.

Each section highlights the most important points to watch out for and gives a reminder of the group's policy where applicable.

If you believe information has been disclosed or leaked to an unauthorised third party, advise your line manager immediately.

Correspondence including computer diskettes and other media

- Correspondence must be correctly and accurately addressed to prevent it being delivered to the wrong address and opened by unauthorised people.
- Ensure letters or enclosures for different customers do not become amalgamated with both going to one customer.
- Ensure confidential information cannot readily be accessed, opened or browsed without detection by unauthorised individuals - always place confidential information, which is leaving the control of the bank, in sealed envelopes - when using unsealed multi-trip envelopes for internal correspondence, ensure that any highly confidential information is enclosed within a sealed envelope.
- Do not place correspondence in post baskets or trays after the last collection as this can easily be intercepted and read by unauthorised people.

Conversation

- Never discuss customers' financial affairs outside the office with family and friends even when with other employees, it is very easy to be overheard and for confidential information to be inadvertently disclosed.
- If you meet a customer socially, or are visiting the customer's home or business premises, do not discuss the customer's financial affairs without the customer's clear consent or if you might be overheard.
- Take care when talking to customers in the office to ensure that your conversation cannot be overheard.

Telephones

- Never give out information at the telephone unless the authenticity of the caller (whether they are a customer or an employee) has been established beyond doubt.
- If security codes are used, only divulge the code if you have originated the telephone call.
- Even if you have originated the call to a customer, make sure that you are speaking to the right person before disclosing information.
- When returning a telephone call to another branch or company within the group, always use a number quoted in the HSBC Group Directory.
- When returning a telephone call to a customer always use a number held in the group's records or the telephone directory.
- When leaving messages on answering machines or with a third party, ensure you do not include any confidential information in the message - the name of the group.

INTERNAL
• company, name of the caller and return call number is the only information you should give
• When receiving a return call from an answering machine or other message you have left, satisfy yourself about the identity of the caller - it is not enough that they are returning your call
• Just because a caller already has some customer or group company information do not assume they are genuine – follow laid down procedures for verification before releasing any information
• Never discuss our security arrangements for verifying calls outside the company with non-HSBC people

Facsimile machines

• Similar controls to those used with telephones apply to facsimile (fax) machines - remember fax machines are open to fraudulent use
• If the message you are sending contains confidential information, warn the recipient and ensure they are available to receive the message
• Similarly, if a message containing confidential information is to be received, ensure the person duly authorised to see it will be available to receive it
• Never leave messages that have been received, or are waiting to be sent, sitting on the fax machine

Computers including laptops and personal digital assistants (PDAs)

• All computer screens and terminals, including those in the back office, must be positioned so that they cannot be overlooked and read by unauthorised people - when using PCs or terminals in customer areas, ask yourself the following questions:
  o Can the screen be overlooked by customers walking through the office?
  o When customers are queuing, are screens within their sight?
  o Can passers-by read screens through windows?

If you answered 'Yes' to any of the above move the screen to prevent it being read or overlooked

If this is not possible, refer to your line manager as the machine may need to be moved or partitions or blinds used

• When leaving a PC that is open to public access or view, always clear the screen of information and sign-off the terminal
• You must never leave unattended terminals logged on or leave disks, diskettes or printouts unattended
• Never access a customer's records without their agreement when in the presence of another customer

Passwords

• All employees should have clearly defined access authorities to computers and PCs
• Make sure you know and understand your own access authority and associated privileges
• Do not choose an obvious password which colleagues can easily guess
• Keep your password secret - do not write it down
• Do not use a colleague's password or access privileges or allow a colleague to use yours
Disposal of information

- You must dispose of confidential information in accordance with laid down procedures even if you no longer have any use for the information it is still confidential
- Offices should have separate waste bins for confidential paper - make sure you know which bins are for confidential waste and which are for normal waste
- Whilst confidential information is awaiting collection and/or disposal, ensure it is safe and that unauthorised people, for example workmen or cleaners, do not have access to it.
Guide to Data Protection and Confidentiality

Summary

- Process information in line with the eight data protection principles
- Familiarise yourself with the Data Protection Procedures in the BIM, particularly in relation to the requirements to process information fairly and lawfully - undertake the mandatory Data Protection on-line intranet training.
- Where possible, resolve customer queries about access to personal information at a local level - this may avoid the issue escalating to a formal request for information to be supplied under the terms of the Data Protection Act 1998
- Keep data confidential - if in doubt, do not give it out
Guide to Data Protection and Confidentiality

Contact Points

In the first instance refer any queries to your line manager.

If you have a data protection query or a request for customer information to be provided locally, please fax details to:

Group Data Protection Office
Retail Compliance
Griffin House, 4-01

INTERNAL: 790 27420
DDI: 0114 282 7420

Alternatively e-mail: Group Data-Protection-Account/HBEU/HSBC@HSBC

Group Data Protection helpline:

INTERNAL: 790 29269
DDI: 0114 252 9269