**3.24 Data Protection Breaches**

If you lose or suspect you have lost any confidential information (whether or not containing personal data), a laptop, blackberry, iPhone, iPad or any other device that contains or permits access to any of ICICI Bank's or individuals' confidential information, (whether or not the device is owned by ICICI Bank), you must take the following steps:

* notify the DPO througha telephone call or an email without any undue delay and under any circumstances not beyond 24 hours of discovery of a data breach incident;
* provide as much detail as you can about the information, data and/or device that has potentially been lost or stolen;
* obtain a crime reference number, if requested; and
* provide any assistance and follow any instructions requested internally.

ICICI Bank has a direct obligation to report any data security breach incident to the ICo within 72 hours of becoming aware of it.

**Consequences of failure to comply with the data protection requirements**

Any breach of the data protection requirements may result in reputational damage to ICICI Bank and the consequential loss of confidence in ICICI Bank's ability to process Personal Data responsibly and securely could lead to lost revenue which far outweighs the immediate legal or regulatory punishment.

Under Part 6 of the UK GDPR Act, there are two tiers of penalty that shall be levied on an enterprise for an infringement or violation of Part 3 of the Act -the higher maximum and

the standard maximum.

**Higher Maximum Penalty** - The higher maximum amount, is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher. In practice, the higher maximum amount can apply to any failure to comply with any of the data protection principles, any rights an individual may have under Part 3 or in relation to any transfers of data to third countries.

**Standard Maximum Penalty** -If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply, which is £8.7 million or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

With regard to the provisions of GDPR, there are a number of specific offences. Those most relevant to ICICI Bank are:

* Processing without notification;
* Failure to notify the Information Commissioner of changes to notification;
* Failure to comply with an enforcement notice or information notice issued by the Information Commissioner;
* Knowingly or recklessly making a false statement in connection with one of these notices;
* Intentional obstruction of, or failure to give reasonable assistance in, the execution of a warrant in relation to the above:
* Knowingly or recklessly obtaining or disclosing Personal Data or procuring the disclosure of Personal Data. Exceptions to this exist where it is necessary to prevent or detect crime, required by law, where the Data Controller reasonably believes he has a right to do so, or where it is in the public interest to do so;
* Unlawful selling of Personal Data; and
* Enforced subject access (forcing an individual to exercise his right of subject access as a condition of recruitment, continued employment or receiving goods, facilities or services).

All of these offences, with the exception of obstruction in the execution of a warrant, may be tried in a magistrate's court or crown court. Both ICICI Bank and the individual staff involved may be prosecuted, depending on the nature of the offence.

In addition, the nformation Commissioner may require ICICI Bank to undertake remedial action before it continues to process the Personal Data. Where ordered by the court or the Information Commissioner, ICiCI Bank will respond promptly to any order requiring the rectification, blocking, erasure or destruction of Personal Data.

**Data protection breach reporting process**

**Any suspected or actual data security breach should be reported immediately to the Line Manager, Head of the Business, Data Protection Officer and / or his designated Data Protection Manager.**

The Data Protection Officer will keep accurate records of all material data protection and security breaches, their impact and outcome. Any breach or suspected breach, even if it occurred sometime in the past and has since been rectified, should be reported to ICO without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals. There is a maximum of 72 hours after becoming aware of the data breach to make the report to the ICO.

The following scenarios are examples only, but typical of the incidents of which the Compliance Department and IT Security must be informed:

* A customer or non-customer complains that they have received an application and/or other documentation that belongs to another person;
* A customer complains that they have found a loophole in our security procedures;
* A customer complains that they are receiving unsolicited e-mails; and
* Incorrect personal information is showing when the customer services their account/receives documentation from ICICI Bank.

**Procedures for management of Data Breaches.**

All Data Controllers have a responsibility under the GDPR to ensure appropriate and proportionate security of the personal data they hold. When external organisations such as ICICI Bank limited (the Parent Bank) or other outsourced vendors process customer data on behalf of the UK Bank, they will normally act as data processors. GDPR places direct obligations on data processors. Alongside these obligations the data subjects (the customers) can enforce their rights directiy against data processors. The enforcement regime lays the non-compliant data processors open to sanctions and penalties.

The guidance provided below is designed to assist in deciding on an appropriate curse of action if a breach occurs.

1. A data security breach can ocCur in a number of ways, SUch as:

* Loss or theft of data or equipment on which data is stored.
* Inappropriate access controls allowing unauthorised use.
* Equipment failure.
* Human error in dealing with personal information.
* Unforeseen circumstances such as a fire or flood.
* Hacking attack on the Bank's IT systems.
* "Blagging offences where information ís obtained by deceiving the organisation who holds it.

2. The key elements for breach management are:

* Containment and recovery
* Assessment of on-going risk
* Evaluation and response

**Containment and Recovery**

* Data protection breach requires not just an inítíal response to investígate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from internal stakeholders across the bank such as Compliance, IT, HR and Risk.
* Any data protection breach should be reported in line with the Data protection Policy.
* The Head of Department (or his nominated Manager) where the breach has Occurred should take the lead on investigating and assessing the risks associated with the breach with the support of the Data Protection Officer or his designated Data Protection manager. In order to limít damage, the Head of Department should establish whether there is anything that can be done to recover any losses the breach can or might have caused. These could include making arrangements to isolate or close a compromised section of the IT network, recall any erroneously sent email, find a lost piece of equipment etc.
* The Data Protection officer or his nominated manager will inform the Police, if appropriate.
* The Data Protection Officer or his nominated manager will notify the Information Commissioner's Office (ICO) of the breach within 72 hours in line with guidelines under "Notification of breaches", in consultation with the Management Committee members. The Commissioner believes that "serious breaches" should be notified. There is no definition for "serious breaches", but the decision would be based on issues such as harm/distress caused to data subjects -e.g. identity theft through loss of details on passport; volume of data lost e.g. unencrypted laptop with personal details; and loss of sensitive data - e.g. manual file with financial records.
* The Head of department should make a report to the Management committee and the Board Risk Committee on the breach and the action taken by the Bank to address any shortcomings.

**Assessing the risks**

The Head of Department or his designated manager should undertake an assessment of the risks associated with the breach as a priority. The breach should be designated as a "High", "Medium'", or "Low" risk. In placing a breach into one of these risk categories, the assessment should consider:

* What type of data is involved?
* How sensitive is it? Is it sensitive personal details (e.g. health records) or other data types which are sensitive because of what might happen if it is misused (e.g. bank account details).
* If data has been lost or stolen, are there any protections in place such as encryption?
* If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
* What could the data tella third party about the individual?
* Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
* How many individuals' personal data is affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
* Who are the individuals whose data has been breached? Are they staff, customers, clients or suppliers?
* What harm can come to those individuals as a result of the breach? Are there risks to physical safety or reputation, financial loss or a combination of these and other aspects of their life?
* Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?

The risk category should be approved by the Data Protection officer.

**Evaluation and Response**

In all cases involving a breach, a root cause analysis should be undertaken. The Head of Department must provide a copy of the RCA, and any action taken to prevent future breaches, to the Data Protection Officer.

Data Protection Incidents and Breaches Flowchart :