ICICI Bank

ICICI BANK UK PLC

United Kingdom

Data Protection Manual July 2024

Table of Contents

1. 2.

PREVIEW.

YEAR 2022-2023 -A RECAP

3

3. DATA PROTECTION POLICY.

APPENDIX 1- PRIVACY NOTICE

APPENDIX 2- INTERNAL RECORD OF PROCESSING ACTIVITIES APPENDIX 3- DATA PROTECTION IMPACT ASSESSMENT (DPIA) APPENDIX 4- PROCESS NOTE FOR ACCESSING CUSTOMER DATA INTERNALLY APPENDIX 5- STANDARD SLA CLAUSES FOR OUTSOURCED VENDORS

APPENDIX 6- COOKIES POLICY.

4

24

32

32 e.se. 4O 41 51

**1. Preview**

The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). With the Brexit transition period ended on 31 December 2020, the EU GDPR being an EU Regulation no longer applies to the UK. Therefore, the Bank will comply with UK data protection law. Further, the GDPR has been incorporated into UK data protection law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations found in the UK GDPR. The EU GDPR may also still apply directly to the Bank if we operate in Europe, offer products or services to individuals in Europe, or monitor the behaviour of individuals in Europe.

Further, post the Germany branch acquiring the status of a third country branch, it has its own data protection policy which is governed by EU GDPR. A link to the Germany Data Protection Manual can be found on V-Komply.

The UK GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the UK. It also addresses the export of personal data outside the UK.

The regulation contains provisions and requirements pertaining to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the UK, and applies to an enterprise established in the UK or-regardless of its location and the data subjects citizenship-that is processing the personal data of people inside the UK. Controllers of personal data must put in place appropriate technical and organisational measures to implement the data protection principles.

"Data protection by design and by default", means that business processes that handle personal data must be designed and built with consideration of the principles and provide safeguards to protect data (for example, using pseudonymization or full anonymization where appropriate), and use the highest-possible privacy settings by default, so that the data is not available publicly without explicit, informed consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it done under a lawful basis specified by the regulation or unless the data controller or processor has received an unambiguous and individualized affirmation of consent from the data subject. The data subject has the right to revoke this consent at any time.

A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the UK. Data subjects have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities centre around regular or systematic processing of personal data, are required to employ a Data Protection Officer (DPO), who is responsible for managing compliance with the GDPR. Businesses must report any data breaches within 72 hours if they have an adverse effect on user privacy.

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.   
  
**2. Year 2022-2023 -A recap of key developments in the regulatory regime**

> In May 2022, the UK ICO issued a consultation paper, calling for views on Privacy in product design'.   
> In October 2022, the UK lCO issued detailed PECR guidance on direct marketing using electronic mail and live calls.   
> In October 2022, the UK ICO issued a consultation on draft employment practices guidance information about workers' health, which aims to provide practical guidance about handling the health information of workers in accordance with data protection legislation and to promote good practice.   
> In November 2022, the UK ICO published an update to its guidance on international transfers (Transfers Guidance), which includes specific guidance about transfer risk assessments or TRAS and a tool for undertaking TRAS (the TRA Guidance and TRA Tool, respectively).

**3 Data Protection Policy**

**3.1 Introduction**

The Data Protection Policy forms a part of the Data Protection Manual and outlines the requirements of data protection legislation and associated regulations including the UK General Data Protection Regulation ("Data Protection Legislation") and how to ensure ICICI Bank remains compliant with it (the "Policy"). If the guidance given here does not provide sufficient clarity for your situation, guidance should be sought from ICICI Bank's Data Protection Officer ("DPO").

The Bank needs to collect and use personal information and sensitive personal information about its clients, employees, vendors and others with whom it communicates. Personal Information must be dealt with in accordance with the relevant national laws.

This Policy applies to all employees, consultants and other staff ("Staff") who collect. possess, use, disclose, transfer, store, or by any other means have access to personal data. Any breach of this Policy will be taken seriously and may result in disciplinary action. This policy should be read in conjunction with the Clear Desk Policy, Information Security Policy and Record Retention Policy, which is owned by Head of Operations.

**3.2 Data Protection Terminology**

A number of terms in this Policy have strict meanings under Data Protection Legislation, and where these terms are used in this document they should be read as defined by Data Protection Legislation.

**Data subjects** for the purpose of this Policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. Al data subjects have legal rights in relation to their personal data.   
  
**Consent** a freely given, specific, informed and unambiguous indication of the wishes of a data subject in the form of a statement or by a clear affirmative action, signifying an agreement on how his/ her personal data should be processed.

**Personal data** means data relating to a living individual whom can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion about the individual. Information about companies or public authorities is not personal data. However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data. A name and a corporate email address clearly relates to a particular individual and is therefore personal data.

**Data controllers** determines the purposes for which, and the manner in which, personal information is to be processed. Note there can be more than one data controller in certain instances. ICICI Bank is data controller of certain personal data used in our business (such as that relating to its clients and staff).

**Data processors** means any organisation or legal entity that prOcesses personal data on behalf of a data controller (such as suppliers, service providers or other third parties). This may be an individual or an organisation and the processing may be carried out jointly or in

common with other persons.

**Processing** is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

**Special categories** of personal data (previously sensitive personal data) means information about a person's racial or ethnic origin, political opinions, religious or philosophical belief, trade union membership, genetic or biometric data, health, sex life or sexual orientation. While personal data relating to criminal convictions and offences or related security measures are treated separately under Data Protection Legislation, they shall be treated

as special categories of personal data for the purposes of this Policy.

**The Information Commissioner's Office (|CO)** The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICo has the power to enforce the Data Protectíon Legislation, investigate breaches and commence legal proceedings.

**3.3 Introduction to GDPR**

ICICI Bank needs to collect and use personal information and sensitive personal information (see definitions below) about its customers, employees, vendors and others with whom it communicates. Personal data must be dealt with in accordance with the Data Protection Legislation and includes personal information processed in any format, be it via computer (including e-mail, cookies, IP address and the internet), certain paper files, video, audio, telephone or other.

**Principles of the GDPR**

Where lCICI Bank determines how personal data is processed, ICICI Bank is likely to be a data controller and have a duty to comply with the principles of the GDPR relation to that personal data.

The principles are summarised as follows, personal data:

1. must be processed lawfully, fairly and in a transparent manner;

2. must be held for limited purposes in an appropriate way;   
3. must be adequate, relevant and not excessive in relation to the purpose(s) for which it is processed ('data minimisation principle);

4. must be accurate and, where necessary, kept up to date; 5. must not be kept for longer than is necessary for the purpose(s) for which it is processed ('storage limitation principles' ); 6. shall be processed in a secured manner to protect the data from unauthorised or unlawful process, accidental loss, destruction or damage ('integrity and confidentiality principle' ); and

7. shall not be transferred to a country or territory outside the UK unless the country or territory ensures an adequate level of data protection.

The data controller shall be responsible for and must be able to demonstrate compliance with these principles ('Accountability principle').

**3.4 Roles & Responsibilities for Data Protection**

ICICI Bank's DPO is Ms. Nalini Modi.

Article 39 of GDPR defines the tasks of the data protection officer"/duties as follows:   
  
1. The data protection officer shall have at least the following tasks:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or procesSor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;   
 c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 of GDPR;   
 d) to cooperate with the supervisory authority;   
 e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

**3.5 Conditions for Processing Personal Data**

**Managing Personal Data**All Personal Data processed by ICICI Bank must be accurate. A record which is itself inaccurate but which is an accurate record of information obtained from the Data Subject or a third party is not necessarily in breach of this principle, provided:

* the purpose for which it was obtained and processed has been taken into account and reasonable steps taken to ensure its accuracy; and
* where the Data Subject has notified his view that the Data is inacCurate, the fact of his notification is clearly recorded, even where the Data is not itself to be changed.

**Lawful grounds for processing personal data**   
Before personal data can be processed, any one of the following grounds listed under GDPR must be satisfied,

* the data subject must give an explicit consent to the processing;
* the processing must be necessary for the performance of a contract to which the data subject is a party, or with a view to entering into such a contract;
* the processing must be necessary to comply with any legal obligation to which ICICI Bank is subject, other than an obligation by contract;
* the processing is necessary for the purposes of legitimate interests pursued by lCICI Bank or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject; and
* the processing is necessary in order to protect the vital interest of the data subject (i.e. it is literally 'a matter of life and death').

Of above, option 2 is most relevant to the Bank. If you are unsure which condition is being utilised for the processing of Personal Data you should contact the Data Protection Officer/Compliance Department.

**Conditions for Special Category Personal Data**

Special category personal data, as defined above, may only be processed in limited circumstances and with stricter controls than other personal data.. There are additional conditions which must be met when processing sensitive personal data, of which the most relevant to ICICI Bank is that the data subject must give explicit consent to the processing when the personal data is collected, although there are certain other options for legitimising the use of special categories of data (such as if it is required by law). Explicit consent means the individual must consent to all aspects of the processing, and that the consent must be clear and unambiguous. ICICI Bank has determined that it holds special category data for its employees, such as racial or ethnic origin, health records, medical history and criminal records of employees under the Senior Management Regime and the valid lawful basis to collect and hold this data is fulfilment of contract. For more information refer the Employee Handbook. In certain cases, the Bank may hold special category data for its vulnerable customers to serve their specific needs post their consent. Refer customer vulnerability policy included in Compliance manual.

**3.6 Consent**

It should be noted that Data Protection Legislation sets a high standard for consent and it may not always be the easiest or most appropriate lawful basis to rely on for processing personal data.

Any consent obtained must be freely given, specific and informed. The individual giving consent must give an unambiguous indication of agreement with a clear, affirmative action. We must also ensure that, wherever consent is relied on, the data subject is notified of their right to withdraw such consent at any time, we must offer a simple way of doing so to that data subject, and we must act on withdrawals of consent as soon as we Can.

Freely given consent means that an individual has a genuine choice and control over how their personal data is used. If the individual has no real choice, consent is not freely given and it will be invalid. Consent should be kept separate from other terms and conditions wherever possible (e.g. a statement of consent in an employment contract is unlikely to be considered valid consent).

**3.7 Fair and lawful processing**

As part of ICICI Bank's obligation to act 'fairly' under the GDPR, the data subject must be informed about how a data controller processes their personal data, in a way that is free of charge, concise, transparent, intelligible and easily accessible. It might be written in clear and plain language. The most common way to provide this information is in a privacy notice. There are certain exemptions from these obligations to inform, for example where the data subject already has the information or where there is some legal or professional obligation restricting its disclosure.

ICICI Bank has a privacy notice in relation to the processing and collection of customer data (including through the use of the ICICI Bank website). The ICICI Bank privacy notice can be found on our website however please contact the DP0 if you require a copy. The ICICI Bank privacy notice has been approved by Compliance and it will be revised whenever there a change in processing. Privacy notices must appear on all retail applications whether it is internet or paper-based and must be positioned before any data is collected, or prior to the signature box on a paper application form.

The IClCI Bank privacy notice would be provided to customers to inform them of the purpose for which their personal data will be processed and give them the chance to withhold consent to marketing.

Refer **Appendix 1** for the Privacy Notice.

**3.8 Your responsibilities**

Each member of Staff agrees that they will:

* comply with the data protection principles as set out above at all times when accessing or otherwise processing personal data of which lCICI Bank is a data controller in the course of their employment;
* apply as relevant all other data protection obligations from time to time required of Staff by ICICI Bank in respect of ICICI Bank personal data;
* keep personal data confidential to the extent required;
* process personal data only as part of their duties to ICICI Bank and never for any other person or organisation or for their private own use;
* bring any suspected breach of Data Protection Legislation in respect of personal data to the attention of DPO and Compliance team;
* All documents (including spread sheets) containing personal data or sensitive data must be password protected, at all times
* adhere to the data retention and destruction timelines.

However, Staff must not:

* sell or otherwise provide copies of customer accounts data, our mailing lists/contact details to third parties (unless certain conditions are met);
* promote unrelated products and/or services;
* disregard the express wishes of data subjects (other than in limited circumstances such as where required by law); or
* process personal data in a way which we know the data subject will object to.
* Transfer personal data to their personal email id, their personal electronic device like laptop, pen-drive, etc.
* Store personal data (including customer data) on common drives.

**3.9 Cookies**

Cookies, IP addresses or similar devices must not be used unless the customer or the user of ICICI Bank's website:

1. is provided with clear, unambiguous and comprehensive information about the purposes of access, processing and storage of that information; and
2. has freely given his or her consent to enable non-essential cookies which includes analytics cookies too.

**Refer Appendix 6 for the Cookies Policy**

**3.10 Marketing**

The customer must be given the opportunity to opt out of receiving marketing by the Bank, Group and third parties. This should be by way of an opt out/opt in section on an application form and included in the promotional messages sent by the Bank. In addition,

customers may be reminded regularly in line with the Banking Conduct Regime (PSR & BCOBs). In case of direct marketing by email, the employee must consider the UK ICO guidance, detailed at Guidance on direct marketing using electronic mail | ICO.

**3.11 Internal Processing Record**

The GDPR replaces the obligation for data controllers to notify the ICO of their processing activities with a mandatory requirement for the maintenance of internal records of data processing activities by both the data controllers and processors.

The internal processing record should include but not limited to:

* details of processing activities and lawful grounds of processing;
* categories of personal data and data subjects:
* details of any recipients of personal data; and
* applicable retention periods and relevant processes.

The DPO is responsible for maintaining this record however it is the responsibility of all department heads to inform the DPO of any new processing or changes to its current processing activities.

Refer **Appendix 2** for Record of Internal Processing Activities.

**3.12 Data Protection Impact Assessment (DPIA)**

As per GDPR, DPIA should be done out before carrying out processing likely to result in high risk to individuals' interests. This is a key element of the focus on accountability and data protection by design, and a more risk-based approach to compliance. ICICI Bank has defined to carry out DPIA in case there is a change in the processes, new technology adopted, new product launched, analysis of individual behaviour or account activities is carried out, profile individuals or children, etc. Bank has prepared a separate note on DPIA which speaks of these scenarios in detail. The DPIA note specifies that it is the responsibility of the Process Owner to assess if the process change requires DPIA to be undertaken and in this process the Process Owner can seek guidance from the DPO. Further, the Bank has included the requirement of DPIA assessment in the PAC review process. The DPIA note is attached to this policy as Appendix 3.

**3.13 Records retention**

Personal Data should not be kept for longer than is necessary for the purpose for which it was being processed. Personal Data records should be periodically reviewed to assess whether it is necessary to continue storing the personal data. Following the storage limitation principle, the ICO states that it is also good practice to review your retention of personal data at regular intervals.

In this regard the Bank follows the ICO guidance on 'Deleting Personal Data'. The guidance states that the organisations should be absolutely clear with individuals about what they mean by deletion and what actually happens to personal data once they have deleted it. The ICO guidance is intended to counteract the problem of organisations informing people that their personal data has been deleted when, in fact, it is merely archived and could be re-instated.

**Difference between deleting and archiving**:  
 There is a significant difference between deleting information irretrievably, archiving it in a structured, retrievable manner or retaining it as random data in an un-emptied electronic wastebasket. Information that is archived, for example, is subject to the same data protection rules as live' information, although information that is in effect inert is far less likely to have any unfair or detrimental effect on an individual than live information. The key requirement is to put the data 'beyond use'.

Putting information "beyond use'

The ICO will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the data controller holding it:

* is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
* does not give any other organisation access to the personal data;
* surrounds the personal data with appropriate technical and organisational security; and
* commits to permanent deletion of the information if, or when, this becomes possible.

**https://ico.org.uk/media/for-organisations/documents/1475/deleting personal data.pdf**

**ICO Guidance for HR holding employee's personal data:**

An employer should review the personal data it holds about an employee when they leave the organisation's employment. It will need to retain enough data to enable the organisation to deal with, for example, providing references or pension arrangements. However, it should delete personal data that it is unlikely to need again from its records such as the employee's emergency contact details, previous addresses, or death-in-service beneficiary details.

https:/ico.org.uk/media/or-organisations/guide-to-the-general-data-protection-regulation gdpr-1-0.pdf

Please refer the Record Maintenance Policy of the Bank, available on Bank's Intranet.

**3.14 Security and confidentiality**

The safe handling of Data is essential to ICICI Bank's continuing operation, particularly as the business expands. The modern business environment requires ever more robust systems to ensure the security of Personal Data, and the implementation of such systems is a vital tool in the management of our business. By keeping Personal Data secure we protect the interests of the business, itS employees and its customers.

The Bank has an obligation to ensure that appropriate security measures are put in place to protect personal information against unauthorised and unlawful processing, accidental lost, destruction, misuse, disclosure or corruption.

Employees are responsible to ensure that personal information is held securely and is not disclosed to any unauthorised third party.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of personal data, defined as follows:

* confidentiality means that only people who are authorised to use the data can access it;
* integrity means that personal data should be accurate and suitable for the purpose for which it is processed; and
* availability means that authorised users should be able to access the data if they need it for authorised purposes.

Access to information and computer systems shall be on a strictly "need to know" basis, and the level of security that should be applied to confidential information, including personal data, will vary with the sensitivity of information in question.

Each business area must ensure that its electronically stored Personal Data is secure. Access must be restricted and files should be password-protected as appropriate.

Personal Data stored in paper form must be kept secure. It must be stored in lockable cabinets with possession of keys controlled and restricted as appropriate. Contracts with off-site archive facilities must contain adequate measures to ensure security and confidentiality.   
  
Refer the updated Information Security Policy of the Bank for further guidance on data security and confidentiality measured adopted by the Bank, available on Bank's Intranet.

**Data MIS requests to BIU and use of Hot Folder**

The Bank has Seclore based file encryption system as an automated process for transfer of data files from BIU server in India to a folder hosted in UK File Server. All staff members requiring simple read access need not install any Seclore client software for accessing data shared by BIU. However in case there are requirements to modify, delete and forward / store data, employees would need to install Seclore client.. Additionally, ICICI Bank UK has created a 'Hot Folder' on shared drive (172.24.40.27) with the name "Seclore\_UK" Any file placed in this folder will be Seclore protected. All staff members must use this folder to save the data generated irrespective of its source i.e. BIU, sales CRM, branch generated, etc.

Further, as per the process defined under the DPIA process, any data request being sent to BIU which includes personal data of customers needs to be first sent for approval to the DPO. Employees should attach the approval received from DPO when raising a Service Request (SR) in the system for BIU to extract the data. BIU to act on the SR upon verification of DP0 approval.

Refer Appendix 4 on the process note for accessing customer data internally.

**Test Data**

Live Data should not be used in systems testing unless unavoidable and with the knowledge and prior consent of IT Security and the Data Protection Officer.

**3.15 Outsourcing/Third Party Processors**

Due diligence should be undertaken by the relevant business owner before using third parties, to ensure that adequate data protection controls are in place.

Relationships with third parties should be clearly defined by a contract which states who is a data controller and who is a data processor, and should set out legal obligations with regard to ownership of the personal data during and at the end of the relationship. Data Protection Legislation is very prescriptive in relation to the content of the agreements between data processors and data controllers and so please contact the DPO and Legal department if you are contracting with a third party data processor.

Contracts with third parties must be reviewed regularly as necessitated by regulatory, legislative and business changes.

Refer **Appendix 5** for standard clauses on agreements with outsourced vendors.

**Transfers of Data outside the UK**

A transfer of personal data only occurs when the personal data moves to a third country outside the UK. The personal data is merely "in transit" if it travels via a server and the information is neither stored, accessed nor manipulated from that country. In that case,

the personal data is only deemed to be transferred to the country to which the server transfers it.

However, transfer does include merely accessing the personal data. For example, if yOu upload personal data to ICICI Bank's intranet or website and that personal data is then accessed by a person outside the UK, or a person outside the UK remotely accesses data on your systems, that data will be deemed to have been transferred to that country, regardless of whether you intended that person to access the website, of where the underlying servers are located or of the fact that the data technically stayed on you

system the whole time.

Transfers of personal data to a country, territory or sector outside the UK are generally prohibited unless the country is listed on the ICO or UK 'adequacy regulations' that provide adequate protection for the rights of the data subject, or an adequacy decision or appropriate safeguard can be applied to the specific transfer. UK "adequacy regulations" include the EEA and all countries, territories and international organisations covered by European Commission "adequacy decisions'" valid as at 31 December 2020. The UK intends to review these adequacy regulations over time. You must involve the DPO at the earliest opportunity in assessing whether or not adequacy applies in each case. Prior to authorising any such onward transfer, ICiCi Bank should then conduct the assessment set out in Data Protection Risk Assessment (DPIA) in respect of the third party.

When external organisations such as ICICI Bank India process customer data on ICICI Bank's behalf, they will normally act as data processors on behalf of ICICI Bank. As data controller, ICICI Bank retains accountability for this processing and must ensure that the required standards are met.

On 28 June 2021 the EU Commission adopted decisions on the UK's adequacy under the EU GDPR. The EU has found the UK to be adequate, which means that most data can continue to flow from the EU and the EEA without the need for additional safeguards.

**3.16 Appropriate Safeguards & Model Contract Clauses**

If the transfer of personal data outside the UK is to a country which is not on the ICO or UK 'adequacy regulations' that provide adequate protection for the rights of the data then ICICI Bank may be able to comply with Data Protection Legislation with respect to the transfer by putting adequate safeguards in place such as, Standard Contractual Clauses (SCCs or model clauses).

This can be also achieved by putting in place model contract clauses (template transfer clauses published by the E Commission) with the third party. In March 2022, the UK Parliament approved the following documents, which provide adequate protection relating to transfer of personal data outside UK

* An International Data Transfer Agreement ("IDTA") for international data transfers from the UK, to countries without "essentially equivalent" privacy laws "
* An international data transfer addendum (the "Addendum") which amends the new EU SCCs so that they work for international data transfers from the UK to countries without "essentially equivalent" privacy laws.
* "A document setting out some "transitional proisions" for the next couple of years.
  + Contracts signed on or before 21 September 2022 can continue to use the old SCC until 21 March 2024. Those clauses will still be deemed to provide "appropriate safeguards" for the purposes of the UK GDPR until that date. From 22 March 2024, the old SCC will no longer be deemed to provide "appropriate safeguards" for the purposes of the UK GDPR, and as such all contracts that use them will need to be amended or replaced to use the IDTA or the Addendum.
  + Contracts signed after 21 September 2022 will need to use the IDTA or the Addendum in order to be effective.

Bank will review the existing agreements (for any requisite changes) effecting international data transfer six months before the end of transition period (i.e. in October 2023).

I-memo ICBK/IP/OVRSEAS&NONBANKING COMPLIANCE/2024-2025/22735357 has been raised on completion of above activity on 22nd May 2024 As an eXception, a data subject can instead give their consent to the international transfer of their personal data. ICICÍ Bank should ensure that such consent is freely given, specific and is an informed indication of the data subject's wishes. The consent should be obtained in writing or in a format which can be recorded (i.e. by way of tick box on an application or order form, which includes a description of the way in which ICICI Bank proposes to deal with the personal data and is often described in a privacy policy). As a data subject can withdraw their consent at any time, ICICI Bank should include details of how consent, once given, can be withdrawn.

Before relying on an appropriate safeguard to make a restricted transfer, bank must be satisfied that the data subjects of the transferred data continue to have a level of protection essentially equivalent to that under the UK data protection regime. This should be done by undertaking a transfer risk assessment (Transfer risk assessments | ICO), which takes into account the protections contained in that appropriate safeguard and the legal framework of the destination country (including laws governing public authority access to the data). If the assessment is that the appropriate safeguard does not provide the required level of protection, bank should inlude additional measures. This assessment is undoubtedly complex in many situations. Hence, the UK ICO issued guidance on this topic (Transfer risk assessments| ICO)..

**3.17 Rights of data subjects**

All data subject requests need to be responded by the Bank within 30 days from the receipt and without charging a fee. ICO on their website have stated that the organisations should calculate the time limit from the day they receive the request (whether it is a working day or not) until the corresponding calendar date in the next month. Thus, the date of receipt of a request shall be treated as Day 1 for the purpose of calculating 30 days. Any such request, upon receipt shall be forwarded to the DPO without any delay. Data subjects have the right to:

* be informed about the processing of their personal data (i.e. for what purposes, what types, to what recipients it is disclosed, storage periods, any third party sources from it was obtained, confirmation of whether we undertake automated decision-making, including profiling, and the logic, significance and envisaged consequences);
* request subject access report to obtain a confirmation as to whether or not personal data concerning him or her are being processed or a copy of any personal data which ICICI Bank holds about them;
* rectification of their personal data, if they consider that it is inaccurate;
* the erasure of their personal data, if they consider that we do not have the right to hold it. The Bank has adopted a data retention and destruction policy (available on ICICI Intranet) as per which the data beyond the specified timelines would be destroyed from both physical and electronic records. The GDPR allows an exception to the erasure of personal data requirement under certain circumstances, out of which the most relevant to the Bank is when there is overriding legitimate ground to retain the data for a minimum period. Following this, the Bank would review each such request received from this perspective and then process the data subject request for right to be forgotten;
* object or withdraw their consent to processing where the firm has no legal grounds for processing;
* restrict processing of their personal data. On receipt of such request the DPO will assess data processed physically and automatically. This may require moving the data to a separate system; temporarily blocking the data on a website or otherwise making the data unavailable. If the personal data has been shared with external parties or processors then the DPO will notify the recipients about the restricted processing (unless this is impossible or involves disproportionate effort);
* data portability (moving some of their personal data elsewhere). This requires ICICI Bank to provide information in a structured, commonly used, readable electronic format. ICICI Bank can be required to transmit the data directly to another controller. The Bank has in place an account switching process which would take care of the data portability requirement. Portable data applies:
  + to personal data which is processed by automated means;
  + to personal data which the data subject has provided to the controller; and
  + only where the basis for processing is consent, or that the data are being processed to fulfil a contract or steps preparatory to a contract.

If the Personal data relates to more than one individual, ICICI Bank is under an obligation to state that the ported data is without prejudice to the rights of third parties. ICICI Bank will not port data to another controller (or to the individual) if breaches the rights of a third party.

* object to their personal data being processed in your particular situation, which Bank may exercise if we rely on the fact that the processing is necessary for the purpose of legitimate interests pursued by ICICI Bank in order to carry out that processing; and
* not to be subject to a decision based on automated processing and to have safeguards put in place if they are being profiled based on your personal data.

**3.18 Data Subject Access Requests (DSAR)**

A subject access request is a request by an individual for a copy of the information held about him on our records. ICICI Bank must provide the requested information free of charge unless where the Bank finds the request to be unfounded or excessive under GDPR.

During October 2020, the ICO has published guidance on handling of DSARS. The key changes introduced are as follows:

* The data subjects can raise a DSAR request seeking information on their personal data held by the Bank through any of the modes, including, oral, writing or through any social media site where ICICI Bank has a presence. Upon receiving such request, the Bank will respond to the data subject without undue delay and at the latest within one month of receipt of the request which can be extended by a further two months' period if the request is complex or a number of requests are received from the individual.
* The Bank can refuse to comply with the DSAR where it is manifestly unfounded or excessive, or it is repetitive, However, if it is concluded that the Bank need not respond to certain DSAR, We must to be able to justify our decision.
* In certain circumstances, while calculating the time available to respond to a DSAR, the clock can be stopped whilst the Bank is waiting for the requester to clarify their request.
* The Bank can withhold personal data sought under a Data Subject Access Request raised by a data subject, if disclosing it would "adversely affect the rights and freedoms of others"

Please refer to ICICI Bank's separate Standard Operating Procedure: Data Subject Access Request (DSAR) for more information, which was reviewed in October 2021.

**3.19 Complaints and Queries**

Customer data protection complaints are most likely to fall into the following categories:

* illegal or unfair processing of the customer's data;
* excessive information held on the customer;
* inaccurate or incorrect information held;
* information being retained for longer than is necessary;
* delays in responding to Subject Access Requests, or insufficient information being supplied;
* requests to cease processing due to the processing causing damage or distress;
* unauthorised disclosure of the customer's information; and
* a marketing opt-out having been ignored.

The DP0 should, in the first instance, handle any general data protection queries. Complaints should be handled in accordance with ICICI Bank's documented complaints procedure.

Complaints will be investigated by ICICI Bank's Complaints Team with guidance from the DPO or Data Protection Manager.

**3.20 Data Sharing**

The Bank abides by the statutory code of practice made under section 121 of the Data Protection Act 2018 which describes how personal data must be shared between organisations that are controllers. Data sharing can take place in a routine, scheduled way or on a one-off basis. Sharing data with a Processor is not covered by the Code.

As per the Code, when considering sharing personal or sensitive data:

* you must comply with data protection law;
* assess the risks and consider using a Data Protection Impact Assessment (DPIA), if required; and
* it is good practice to have a data sharing agreement.
* The data subjects can raise a DSAR request secking information on their personal data held by the Bank through any of the modes, including, oral, writing or through arny social media site where ICICI Bank has a presence. Upon receiving such request, the Bank will respond to the data subject without undue delay and at the latest within one month of receipt of the request which can be extended by a further two months' period if the request is complex or a number of requests are received from the individual.
* The Bank can refuse to comply with the DSAR where it is manifestly unfounded or excessive, or it is repetitive. However, if it is concluded that the Bank need not respond to certain DSAR, we must to be able to justify our decision.
* In certain circumstances, while calculating the time available to respond to a DSAR, the clock can be stopped whilst the Bank is waiting for the requester to clarify their request.
* The Bank can withhold personal data sought under a Data Subject Access Request raised by a data subject, if disclosing it would "adversely affect the rights and freedoms of others"

Please refer to ICICI Bank's separate Standard Operating Procedure: Data Subject Access Request (DSAR) for more information, which was reviewed in October 2021.

**3.19 Complaints and Queries**

Customer data protection complaints are most likely to fall into the following categories:

* illegal or unfair processing of the customer's data;
* excessive information held on the customer;
* inaccurate or incorrect information held;
* information being retained for longer than is necessary;
* delays in responding to Subject Access Requests, or insufficient information being supplied;
* requests to cease processing due to the processing causing damage or distress;
* unauthorised disclosure of the customer's information; and
* a marketing opt-out having been ignored.

The DP0 should, in the first instance, handle any general data protection queries. Complaints should be handled in accodance with ICICI Bank's documented complaints procedure.

Complaints will be investigated by ICICI Bank's Complaints Team with guidance from the DPO or Data Protection Manager.

**3.20 Data Sharing**

The Bank abides by the statutory code of practice made under section 121 of the Data Protection Act 2018 which describes how personal data must be shared between organisations that are controllers. Data sharing can take place in a routine, scheduled way or on a one-off basis. Sharing data with a Processor is not covered by the Code.

per the Code, when considering sharing personal or sensitive data: As

* you must comply with data protection law;
* assess the risks and consider using a Data Protection Impact Assessment (DPIA), if required; and
* it is good practice to have a data sharing agreement.

Also when sharing personal or sensitive data, you must follow the key principles in data protection legislation:

The accountability principle means that you are responsible for your compliance, and you must be able to demonstrate that compliance.

You must share personal data fairly and transparently.

You must identify at least one lawful basis for sharing data before you start any sharing.

You must procesS personal data securely, with appropriate organisational and technical measures in place.

The Data Sharing Request Form Template published by ICO may be referred where this Scenario applies.

**3.21 Substantial Damage and Distress Claims**

ICICI Bank will respond within as soon as possible of no later than a month to all claims made under Article 79 (right to prevent processing likely to cause damage or distress) of the GDPR. The Data Protection Officer will handle all such claims, with legal input if appropriate.

**3.22 Data Protection & Employees**

Employees ' and other Staff personal data falls within the scope of the GDPR in the same way as customers' personal data, and therefore all aspects of this Policy apply to ICICI Bank's employees.

HR should maintain employee data files and managers should not keep any information on employees other than that which relates to current live issues (e.g. disciplinary/poor performance/performance appraisal documents). All staff, especially line managers, should bear in mind that facts or opinions relating to employees contained in emails, electronic documents, spreadsheets, meeting and interview notes etc and any structured manual Data may need to be provided in response to a subject access request.

**The staff privacy notice should be shared with all employees. Refer employee handbook for details.**

**Staff Training**

All staff involved in processing of Personal Data should receive data protection training. As a minimum, staff members who have been mandated and therefore outside of the e learning exemption list must complete their Data Protection e-learning annually. The e learning exceptions list is approved by the Head of Compliance or the DPO each year.

**3.23 Notification to the Information Commissioner**

In order to process Personal Data, each legal entity in ICICI Bank UK must be registered with the Information Commissioner. Failure to notify is an offence, as is any processing not

included in ICICI Bank's Notification. The details of ICICI Bank's processing are entered in the Information Commissioner's Register of Data Controllers, which is available for public inspection on the Information Commissioner's website

http://www.ico.org.uk/esdwebpages/search

**Substantial Damage and Distress Claims**

ICICI Bank will respond within 21 calendar days to all claims made under section 10 (right to prevent processing likely to cause damage or distress) of the GDPR. The Data Protection Officer will handle all such claims, with legal input if appropriate.

**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 :

Coutroller detects de awue of a sty sncident nd estatlsies if eoual data beact bas occured

ls the breach hkelr

to result s) a nsk to

uIdit1duals 1gts

and feedous?

Tes

Is the breach lukely to

st i a hugh ask to

ndinals rcbis and

icedoms^

No

The controller becomnes "aware of a

personal data breach and as5esses risk

to md:1duals

No

No requueuletut lo botify super1sor auhoutv or Indiduals

Notefy copeent superisory uthontý

If the breich affecis mdrndLals i 110re 1lhan one Menber State. otify eacu conpeteit

supesoy auttoatty accosd1ngly

No requfeueut to nou

individua!s

Noniv aãected snd1rduals und. vthere cequred. pro:ide

unforation on steps they can take to p1otect tiemseles #on

consequences of the breach

Al breacses secordable ULde1 Article 33(5) Breacl sl1ould be docune1led asd

record miuntauned by the controller

**3.25 The Information Commissioner's Office (lCO)**

The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO has the power to enforce the Data Protection Legislation, investigate breaches and commence legal proceedings. 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 E17.5 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.

During 2021-2022, UK ICO has fined many UK companies regarding unsolicited/illegal marking calls/SMS messages in contravention to PECR regulations.

Maximum fines levied by ICO:

In July 2021, Amazon was hit with a ¬746 million fine for violating the GDPR. It was found to be tracking user data without acquiring appropriate consent from users or providing the means to opt out from this tracking - resulting in Amazon being hit with the largest GDPR fine to date.

In September 2022, the Ireland's DPC 0ssued a ¬405 million fine to Meta Ireland concerning the lawfulness of processing children's personal data in accordance with the legal bases of performance of a contract and legitimate interest. Meta failed to take measures to provide child users with information using clear and plain language, lacked appropriate technical and organisational measures, and failed to conduct a DPIA.

In January 2023, the Ireland DPC issued a ¬390 million fine to Meta lreland in connection to its Facebook and Instagram services. Meta changes its Terms of service, changing the legal basis from consent to contract and asked its users to accept new terms to access their accounts, otherwise the services would not be available to them. The DPC considered Meta violated the transparency principles.

In November 2022, the Ireland DPC issued a ¬265 million fine to Meta Ireland after personal data was found on an online hacking forum. The DPC noted the infringement of Article 25 (1) and 25(20 of GDPR (i.e. Data Protection by Design and Default).

In September 2021, Ireland's Data Protection Commission fined WhatsApp with this ¬225 million GDPR penalty after claiming that the messaging service had failed to properly explain its data processing practices in its privacy notice. The Irish DPA said that WhatsApp's somewhat opaque privacy notice was at fault here-the company should have provided privacy information in an easily accessible format using language its users could understand.

In December 2021, the French DPA (the CNIL) imposed a ¬150 million penalty on Google and ¬60 million penalty on Facebook (now Meta) for violations of French rules on the use of cookies. The CNIL's investigations concluded that the websites offered an easy way to consent to the use of cookies immediately after accessing the websites, but did not provide an equally easy way to refuse the use of cookies. Users had to select multiple options to refuse cookies, but only one option to provide consent to the use of all cookies. The CNIL also concluded that Facebook provided unclear and confusing instructions to users on how

to refuse cookies.

**Appendix 1-Privacy Notice**

In this Privacy Notice:

Data Protection Legislation means the General Data Protection Regulation ("GDPR") and UK Data Protection Act 2018; together with all other applicable and national implementing legislation relating to privacy or data protection; and where we use the terms "personal data', "data subject", "controller", "processor" and "process" (and its derivatives), such terms shall have the meanings given to them in the Data Protection Legislation.

INTRODUCTION

ICICI Bank UK PLC (ICICI Bank) is committed to keeping your personal data private. We shall process any personal data we collect from you in accordance with Data Protection Legislation and the provisions of this Privacy Notice. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

DATA CONTROLLER

For the purpose of the GDPR ICICI Bank is the data controller of your information. This means that we are responsible for deciding how we hold and use your personal data. We are required under Data Protection Legislation to notify you of the information contained in this Privacy Notice.

DATA PROTECTION OFFICER

We have appointed a Data Protection Officer (DPO) to oversee compliance with this Privacy Notice. If you have any questions about this Privacy Notice or how we handle your personal data, please contact the DPO at the contact details set out below.

**Ms Nalini Modi, The Data Protection Officer, ICICI Bank UK PLC, One Thomas More Square, London, E1W 1YN.**

COLLECTING INFORMATION FROM YOU

ICICI Bank will collect and process your personal data you provide us through application forms, our website, face-to-face and electronic communication (including telephone conversations) in order to provide our services to you.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

We may collect, store, and use the following categories of personal data about you:

* Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
* Date of birth
* Gender
* Employment status and salary
* Marital status and dependants
* Financial information