**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