**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.