**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.