MAURITIUS

KEY FACTS
DATA PROTECTION REQUIREMENT

SECTION 14 OF THE DATA PROTECTION ACT 2017 (DPA) ESTABLISHED A MANDATORY REQUIREMENT FOR CONTROLLERS AND PROCESSORS TO REGISTER WITH THE DATA PROTECTION OFFICE. THIS IS SUPPLEMENTED BY THE DATA PROTECTION (FEES) REGULATIONS 2020 AND THE DATA PROTECTION OFFICE'S COMMUNIQUE ISSUED IN RELATION TO SAME. THE REGISTRATION DEADLINE IS 1 DECEMBER 2020.

AIMS OF THE DPA

> To strengthen control and personal autonomy of data subjects[1] (individuals) over their personal data[2]

> To be in line with the European Union's General Data Protection Regulation (GDPR)

> To simplify the regulatory environment for business in our digital economy

> To promote the safe transfer of personal data to and from foreign jurisdictions

HOW IS THE MAURITIUS CORPORATION IN YOUR GROUP AFFECTED?

An assessment is to be made on:

> Whether the corporation is a data controller, which determines the means and processing of personal data of data subjects with decision-making powers

> Who is to be appointed as the data processor, which will process the data on behalf of the data controller

> Who will be appointed as data protection officer (DPO), who will be responsible for data compliance issues

WHAT IS TRIDENT TRUST COMPANY (MAURITIUS) LIMITED (TMAU) DOING TO HELP YOU COMPLY?

Since corporations administered by TMAU effectively meet the criteria of a data controller with decision-making powers resting with their board, they will need to register at least as a controller. TMAU has consulted with law firms and other stakeholders on the matter.

However, TMAU can assist both in the registration process, as well as in capacity of a data processor, even by providing a DPO.

WHO IS A CONTROLLER?

All public and private organisations, sociétés, partnerships, professionals such as doctors, lawyers, engineers, architects and notaries, and sole traders such as jewellers and bookmakers, and any other organisations processing or keeping personal data of living individuals, are required to register themselves as a controller with the Data Protection Office. The list is non-exhaustive.

Under section 15(3) of the DPA, any controller who knowingly supplies any information that is false or misleading in a material particular during registration will be considered to have committed an offence and will, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding five (5) years.

---

[1] Data Subject: An identified or identifiable individual (any data that can identify an individual), in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

[2] Personal Data: Any information relating to a data subject.

DUTIES OF CONTROLLER

Every controller must implement and adopt policies and implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in accordance with the DPA.

Such measures include:

> Implementing appropriate data security and organisational measures, and maintaining appropriate documentation

> Performing data protection impact assessment as per section 34 of the DPA

> Complying with requirements of prior authorization and consultation as per section 35 of the DPA

> Designating an officer responsible for data protection

WHO OR WHAT IS A PROCESSOR?

A processor is an organisation that processes personal data on behalf of a controller. There must be a contract between the processor and the controller clearly defining this relationship. The processor has no decision-making power regarding the personal data being processed. An example of a processor is a company that prepares the payroll of the employees of other companies (controllers) and performs all the functions of payroll as defined in the contract between the processor and the controllers. If some of your departments are processing the personal data of customers or employees, for example packing, printing, embroidery, transport or payroll amongst others, these departments are not to be considered as processors as they are part of the controller (i.e., your organisation).

Under section 15(3) of the DPA, any processor who knowingly supplies any information that is false or misleading in a material particular during registration will be considered to have committed an offence and will, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding five (5) years.

PRINCIPLES RELATING TO PROCESSING PERSONAL DATA

Every controller or processor shall ensure that personal data are

> Processed lawfully, fairly and in a transparent manner in relation to any data subject

> Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes

> Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

> Accurate and, where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data are erased or rectified without delay

> Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

> Processed in accordance with the rights of data subjects

MANDATORY DESIGNATION OF A DPO

The designation of a DPO is mandatory according to section 22(2)(e) of the DPA for both controllers and processors.

The DPO will be the contact point with respect to data subjects, the Data Protection Office and internally within the organisation.

CAN AN ORGANISATION HAVE MORE THAN ONE DPO?

Organisations need to determine the best way to set up the DPO functions and whether this necessitates a data protection team. If the organisation has a team, it should clearly set out the roles and responsibilities of its team members.

DESIGNATION OF A DPO FOR EACH SUBSIDIARY OR BRANCH

The DPA does not specify whether a controller or processor needs to have a single or different DPO(s) for its subsidiaries. It is the responsibility of the controller to determine this. For example, based on organisational structure and size, a single DPO may be designated for several subsidiaries.

CAN WE CONTRACT OUT THE ROLE OF THE DPO?

You can contract out the role of DPO via a service contract with an individual or an organisation. An externally appointed DPO should have the same position, tasks and duties as an internally appointed one.

QUALIFICATIONS OF THE DPO

A DPO is expected to have professional experience and knowledge of data protection laws and standards. The DPO should also have good knowledge of the controller's business, including how operations are carried out, information systems, and data security and data protection needs of the controller.

A DPO should be honest with high professional ethics. The DPO's main concern should be enabling compliance with the DPA, thus, the DPO should be chosen judiciously.

DUTIES OF THE DPO

The DPO should work independently, report to the highest management level and have adequate resources to enable the controller or the processor to meet its obligations under the DPA.

At a minimum, a DPO should carry out the following duties. However, the controller or processor can add more tasks to meet their business requirements:

> Inform and advise the controller or processor and its employees about their obligations to comply with the DPA and other data protection laws

> Monitor compliance with the DPA and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff and conducting internal audits

> Be the first point of contact for the Data Protection Office and for individuals whose data are processed (employees, customers, amongst others)

RESOURCES TO PROVIDE TO THE DPO BY THE CONTROLLER OR PROCESSOR

Depending on the nature of the processing operations and the activities and size of the organisation, the following resources must be provided to the DPO:

> Officially communicate designation of the DPO to all staff

> Active support of the DPO's functions by senior management, including financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate

> Sufficient time to fulfil duties

> Access to other services within the organisation so that DPO(s) can receive essential support, input or information

> Continuous training

IS THE DPO PERSONALLY RESPONSIBLE FOR NON-COMPLIANCE WITH DATA PROTECTION REQUIREMENTS?

No. DPOs are not personally responsible for non-compliance with data protection requirements. It is the controller or the processor who has that responsibility and is required to ensure and is able to demonstrate that processing is performed in accordance with the DPA.

Therefore, even though the DPO assists the controller or processor in monitoring internal compliance, the DPO is not personally responsible for any non-compliance with the DPA by the controller or processor.