

Data Privacy Day 2022

PRIVACY DAY

Privacy Day is celebrated annually on the 28th of January worldwide to raise awareness on data protection and to help individuals exercise their rights. This symbolic day marks a reminder that the right to privacy is in fact a fundamental human right that must be enjoyed by every individual.

On this occasion, BDO IT Consulting Ltd is issuing this newsletter to bring light to data privacy and its leverage, data protection laws as the driver towards securing data privacy rights of data subjects, data protection laws in Mauritius and global privacy updates.

This Newsletter includes:

- Significance of Data Privacy and its surge in the 21st Century, to contextualise the privacy issue faced by different organisations
- Data Protection: A denomination of data privacy, to understand the link between data protection and data privacy
- European Union General Data Protection Regulation Best Practices to ensure a robust data protection culture within organisations
- Data Protection Certification in Mauritius to allow Data Controllers and Data Processors to enforce the Mauritius Data Protection Act and to continuously assess their data protection frameworks
- Views of the Mauritian Data Protection Commissioner on privacy in Mauritius.
- Top Privacy News around the world to count down the most prominent international developments across countries

DATA PRIVACY: WHAT IS PRIVACY AND ITS SURGE?

“Data Privacy” is a term that has spurred great interest over the past decades, but the question we should be asking ourselves is: what is the root cause of this surge?

The strength of this term lies in the pressing need to protect the personal data of people, otherwise known as data subjects. The late, European Data Protection Supervisor Giovanni Buttarelli once said, “Data defines individuals and determines how they can be treated”.

Data Protection is a denomination of data privacy since it aims at protecting personal data and governs how data is collected, shared and used. We are currently living in an era where data is so tangible that its aggregation in the hands of powerful corporations would lead to archaic accumulation of power, to the detriment of data subjects who will eventually have little control over their personal data. Hence, the introduction of strict data protection regulation undoubtedly acts as a remedy and glimmer of hope to cure this issue.

THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

The European Union General Data Protection Regulation 2016 which came into force on 25th May 2018 skyrocketed through the imposition of strict Data Protection frameworks across the globe with one fundamental aim; which is to ensure the protection of the fundamental privacy rights of data subjects.

This year marks the 5th year since the GDPR came into existence and it is regarded as the strongest regulation on data protection and countries around the world are amending their laws to be in line with GDPR. The GDPR has as an EU-wide law, encouraged amendments in data protection laws and influenced rigorous data protection cultures across countries internationally.

GDPR BEST PRACTICES : 10-STEPS PLAN TO ENSURE A ROBUST DATA PROTECTION CULTURE WITHIN AN ORGANISATION

- **Appointment of a Data Protection Officer (DPO)**

Appointment of the DPO is the first step towards ensuring accountability when processing personal data. The DPO has the responsibility to assist in monitoring the company's compliance with the applicable data protection laws and regulations, advise the various stakeholders on same and act as a contact point between the company/ individuals and the data protection authority.

- **Maintain a personal data register**

Maintaining a personal data register (Record of Processing Operations) is one of the key requirements of most data privacy regulations worldwide. A 'data mapping exercise' needs to be conducted to tabulate all the processing activities of an organisation.

- **Notify purpose and seek consent**

With the introduction of GDPR, data subjects are now the lead actors when it comes to the processing of their personal data. Hence, organisations are required to clearly define their lawful basis of processing, when collecting and processing personal data and notify the data subjects of same. One among which, is seeking consent. If the processing activity requires the individual's consent, the organisation must collect clear and explicit consent of the data subject.

- **Respond to data subjects' request**

The GDPR birthed the principle of easy access to one's personal data and hence, organisations must implement proper mechanisms to respond to the requests of data subjects.



- **Enforce security mechanisms**

Organisations must implement adequate and effective organisational and technical security measures to protect personal data.

- **Privacy by Design (PbD)**

PbD is a proactive principle that stems from the GDPR and requires that controllers and processors embed data privacy into design of any new processing activity to ensure that data privacy is at the heart of the organisation.

- **Data breach Notification**

The infamous antagonist to data privacy are instances of data breach. Hence, every controller and processor have the responsibility to implement a proper data breach notification mechanism as a proactive measure to combat potential data breaches.

- **Manage third parties**

If an organisation engages a third party to process personal data on its behalf, it shall be liable if the third party violates any data protection laws. Therefore, before entering into any such agreement, the organisations shall ensure that the latter has adequate security measures in place to ensure the protection of the personal data and is aware of its role and responsibilities under data protection laws.

- **Data transfers**

The transfer of personal data outside one's jurisdiction is increasingly delicate. To comply with the GDPR, organisations must map and review their international transfers and make appropriate changes in time, including the implementation of the standard contractual clauses (SCCs) for the transfer of personal data outside the European Economic Area, issued by the European Commission.

- **Communication of data protection policies, procedures and practices**

Central to privacy and data protection is transparency. When collecting individuals' personal data, the organisation must provide them with clear information explaining why, what and how you're intending to process it and one way of achieving this is the implementation of unequivocal policies and procedures.

MAURITIUS: THE DATA PROTECTION ACT 2017

The Mauritian legislator spared no effort when it came to data privacy and the protection of personal data thereof. Running through it all is the insistence that our legislators focussed on as evidenced by the amendment in our data protection law, we are now guided by the Data Protection Act 2017 (DPA), which came into force on 15 January 2018.

The DPA finds its roots and objectives from the EU GDPR and plays a fundamental role in uplifting data privacy, securing data subject rights and fostering a privacy culture across organisations. Therefore, the above 10 steps plan are applied in Mauritian organisations today.

DATA PROTECTION CERTIFICATION IN MAURITIUS

A vital vacuum of accountability under the DPA lies under Section 48. This section laid down the essential technical standards to allow data controllers and processors to obtain the Data Protection Certification. Data controllers and processors can seek this certification, which is issued for a maximum period of 3 years and which may be renewed where the requirements continue to be met and withdrawn where they are no longer met.

Data Privacy is a mission greater than compliance and the Data Protection Certification requirement is an endorsement of that. Not only is the Data Protection Certification an essential part of the enforcement of the DPA and in creating a robust environment where data privacy is upheld but it also acts as a driving force, compelling data controllers and processors to continuously assess their data protection frameworks and prevent any form of privacy invasion.

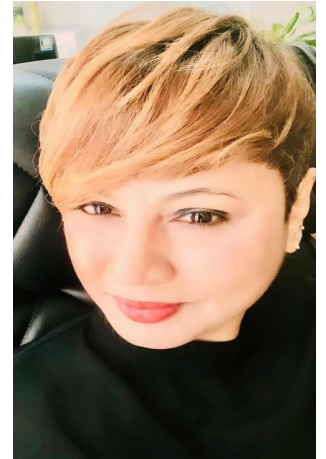


VIEWS OF THE DATA PROTECTION COMMISSIONER

What are your views on the privacy day 2022?

We will celebrate the 16th Data Protection Day worldwide and also the 41st anniversary of the Council of Europe Convention 108, which is the only international legally binding instrument on data protection.

The Data Protection Day will begin the year with a positive reminder of the importance to protect privacy rights of people. Privacy is a fundamental human right for each and every individual. Organisations are also reminded of their duty to protect personal data under their custody and to pay special attention to their data transfers across borders. The Data Protection Act 2017 has revolutionised the entire data protection landscape in Mauritius. Many new data subject rights, such as the right to object to automated individual decision-making, have been introduced. In addition to those, new obligations have also increased the accountability of controllers.



Mrs Drudeisha Madhub

Data Protection
Commissioner
(Republic of Mauritius)

Privacy is no longer a comfort but a necessity. It is, therefore, fundamental that all organisations commit to achieving a level of protection of personal data that corresponds to the changes linked to the rapidly-evolving technology. In an era of COVID-19, technology adoption has taken a quantum leap at the organisational, business, and individual consumer levels. It is thus imperative that privacy protections are reinforced at all levels.

Cross-border data flows will increase as the African continent adopts harmonised privacy and data protection policies and regulations in line with international standards. Therefore, building trust in the security of processing personal data operations is of paramount importance. On this special day, I would like to appeal once again to all controllers and processors to register with the Data Protection Office which is mandatory by law to avoid any risks of being prosecuted. It is also equally important that organisations designate a Data Protection Officer responsible for data protection compliance issues.

What are the activities the Data Protection Office is envisaging for 2022?

This year the focus will be mainly on enforcing data protection in Mauritius through prosecution with the collaboration of the police.

How many organisations are as of today certified with the Data Protection Office?

We are in the process of finalising the certification of one organisation and the process is a rigorous and lengthy one but credit worthy for certified organisations.

LATEST PRIVACY NEWS WORLDWIDE

Data Privacy requires a form of international coalition. It is not the responsibility of a single actor. In this era of global environment, all countries have to implement effective data protection and privacy frameworks. Our Data Protection Newsletter counts down the most prominent and recent international developments in this regard.

1. Kenya

The Office of the Data Protection Commission ('ODPC') has published the 2021 Data Protection Regulations comprising of three regulations, notably the Data Protection (General) Regulations 2021, the Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021 and the Data Protection (Registration of Data Controller and Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021. In this regard, the Regulations are now awaiting approval from the National Assembly, after which, provided no objections are made, the Regulations will come into effect.

2. Rwanda

The National Cyber Security Authority ('NCSA') issued, on 10 January 2022, a notice relating to the Protection of Personal Data and Privacy, regarding data subject rights. In particular, the NCSA noted that the data subject has, under Article 18 of the Data Protection Law, the ability to request a copy of their information, as long as this request is without prejudice to other relevant laws.

The NCSA also stated that the data subject can, under Article 19 of the Data Protection Law, request at any time for the controller or processor to stop processing their personal data, which causes or is likely to cause loss, sadness, or anxiety to the data subject, and also request the controller or processor to stop processing personal data for direct marketing purposes.

3. Zambia

The Electronic Communications and Transactions Act was enacted on 23 March 2021 by the Parliament of Zambia, with the aim of providing a safe and effective system for the use and protection of personal data. The Act promotes secure electronic signatures and facilitates the electronic filing of documents by public authorities.

4. Uganda

The newly operational Personal Data Protection Office ('PDPO'), following the passage of the Data Protection and Privacy Regulations 2021, is now requiring data collectors, processors and controllers to register on its website by December 2021. The PDPO highlighted that it will begin enforcement measures against organisations and persons who have not registered in January 2022.

5. South Africa

The Information Regulator noted that when processing the personal information of a voter, a political party must ensure that the processing complies with the provisions of the Protection of Personal Information Act 2013 ('POPIA'). It must specifically make sure that the processing complies with the right conditions for lawful processing, the security safeguards, measures and controls against loss, damage and misuse of voters' personal data, and the processing of special category personal data, such as political persuasion of voters, is done in accordance with Section 31 of POPIA.

6. Australia

The Office of the Australian Information Commissioner ('Oaic') has made detailed recommendations to ensure Australia's privacy regime continues to operate effectively for all and promotes innovation and growth. These recommendations include protecting consumers from individual and collective privacy risks and harms and supporting global interoperability and minimising friction to ensure consistency of protection across the economy and to protect personal information wherever it flows.

7. Israel

In January 2021, a Privacy Protection Bill was introduced in the Israeli Parliament for the first reading. The highlights of the new Protection Privacy Bill is the requirement of certain companies to appoint a data protection officer, the introduction of enforcement powers for the Privacy Protection Authority and refined definitions for key terms to reflect societal and technological developments, in line with the General Data Protection Regulation.

8. China

China's new data privacy law, the Personal Information Protection Law (PIPL) came into force on 1st November 2021. The fundamental objectives of the PIPL are to protect the rights and interests of personal information, regulate personal information processing activities, and promote the rational use of personal information. The PIPL is not only applicable to organizations and individuals who process personally identifiable information (PII) in China but also to those who process data of China citizens' PII outside of China.



DATA

The main provisions of the PIPL are as follow:

- Data subjects are given more rights over the use of their data. They can request to edit, remove, restrict the use of their data, or withdraw consent given previously.
- More stringent requirements on data sharing and data transfer, which your organization and any third-party joint data controllers may need to pass data related assessments.
- Penalties and fines on organizations for data breaches. Including increased fines (up to 50 million RMB), revenue confiscation (up to 5% annual revenue) and business cessation.
- Mandatory security controls to be applied when storing and processing the PII, and training to be provided to responsible personnel who handles the PII.
- Mandatory data localisation when the amount of PII exceeds the threshold set by the Cybersecurity Administration of China (CAC)



BDO IT CONSULTING LTD DATA PROTECTION SERVICES

Processing personal data by a data controller or data processor is a critical business requirement that is enforceable by relevant legislation such as the DPA and GDPR. Our data protection services are wide-ranging and can be tailored to our clients' needs.

Hence, whether you require a data inventory; a gap analysis; the implementation of a privacy framework; reviewing an existing framework, data protection audits or providing an outsourced Data Protection Officer (DPO), we can help you to be data protection compliant.

OUR TEAM

BDO has the right mix of highly qualified and experienced resources with absolute knowledge, skills and expertise in providing data protection consultancy services. Professionalism ranks high on our agenda and we endeavour to provide the best services to our clients.


Our team includes legal experts, IT professionals and project management consultants. They hold the following certifications:

- Certified Information Privacy Professional/ Europe (CIPP/E),
- Certified Information Privacy Technologist (CIPT),
- Certified Information Privacy Manager (CIPM),
- Certified Information Systems Auditor (CISA),
- One Trust Certified Professional - Privacy Management (OTCP).
- EXIN Privacy and Data Protection Foundation Certificate
- EXIN Information Security Foundation Certificate
- PECB Certified Data Protection Officer

Contact Information

BDO IT Consulting Ltd
10 Frère Felix de Valois
Street,
Port Louis,
Mauritius

 Sylvie Greco,
Partner

 +230 202 3007
+230 202 9897

 sylvie.greco@bdo.mu

