Data Privacy Trends in 2023

As the number of privacy laws worldwide continues to grow, businesses need to focus on privacy trends to protect users' personal information and comply with privacy regulations. Huge fines for breaching data privacy regulations are not the only reason companies must improve personal data security measures. As users' awareness about their personal data grows, handling personal data according to the law affects users' trust in businesses and influences the profit of companies. Here are the top data privacy trends and tendencies you need to understand in 2023 which highly impacts on businesses worldwide including Mauritius.

Global rise in data privacy regulations

The introduction of the General Data Protection Regulation (GDPR) in Europe in 2018 initiated the growth of data privacy regulations worldwide. Today over 100 countries have privacy or data protection laws, and the number of countries is growing. The global rise in data privacy regulations will continue to rise in 2023. By the end of 2024, it is expected that 75% of the global population will have its personal information covered under privacy regulations.

Companies will invest more in privacy technologies

Privacy-driven spending on compliance with privacy laws will continue to increase in 2023. As new privacy regulations are evolving constantly, companies will invest more in privacy technologies to get the trust of users and avoid fines. Currently, advertisers and marketing agencies employ business models that rely on sharing personal information. However, this is changing fast. Privacy-enhancing technologies took the center stage in 2022 and will continue to rise in 2023. In 2019 Google launched Privacy Sandbox and is currently working on Trust token API and other privacy technologies to replace third-party cookies.

In 2021 – 2022, big tech companies were charged with multi-million fines for the GDPR breaches. The total amount of fines appointed on Meta alone until the end of 2022 by the Irish Data Protection Commission for breaching the GDPR and ePrivacy Directive seeks nearly €1 billion. In addition, the Irish Data Protection Commission also has 40 open inquiries for other big tech companies.

This tendency will continue in 2023, and we should see more companies charged with big fines for breaches of privacy regulations, especially the European ones.

The privacy regulations and even cookies or other tracking technologies themselves are continually evolving, which means website owners should continuously update their current Privacy Policy and process personal information accordingly.

A cookieless future

A cookieless future is right upon us: with the increasing importance of first-party data and users' awareness of their personal data, third-party cookies are going away. Google has announced that by the end of 2023, it will officially stop supporting Third-Party Cookies on the Google Chrome browser. However, later it had to delay blocking third-party cookies until 2024 due to the full testing of technological solutions of alternatives.

The trend will continue for removing cookies in favor of consent-based data-collecting solutions. With the trend towards first-party data, advertisers and marketing agencies are increasingly interested in investing in direct partnerships with brands and businesses, that own the data.

Greater transparency in the collection and processing of personal data

User privacy survey shows that website users value data privacy, and over 50% of them would change service providers simply because of their data policies or data sharing practices. The trend will continue in 2023. Those businesses that handle the personal information of users seriously will see an increase in their active users and profits compared to their competitors.

Increase in requests and complaints of data subjects

Data subjects of the privacy regulations are becoming more aware of their rights and want to protect their personal information. As data subjects continue to exercise their right to know, update, delete, or otherwise handle the personal information businesses have collected about them, this will follow by a significant increase in data subject requests and complaints in 2023.

More data security and privacy job positions

Increasing and changing privacy regulations worldwide will lead to more data security jobs for humans in the coming year. The increase in related jobs in recent years dispels the myth that Data Science and Artificial Intelligence replace human labor.

Accordingly, new education programs in tech have been created in recent years to satisfy the demand for data safety positions. The need for experts in data security and legal advisers on privacy is increasing recently. The trend will continue in 2023.

The environment we face at the end of 2022 is increasingly uncertain amidst geo-political tensions and economic fragility, but new approaches and ideas born of technology and innovation continue to emerge, designed to enrich and enhance the way we live and potentially help respond to the challenges we face. A number of these technologies look set to dominate 2023 and drive new legal developments in data privacy.

The ongoing march of AI technology across all sectors will be shaping our societies in years to come, for good or ill. Likewise, there's much prominence given to the metaverse even if most of us are not yet clear how it will operate in practice and what the implications will be for people's privacy. The challenge in 2023 and beyond will be for companies and governments to act responsibly and for regulators to achieve a fair balance between encouraging the deployment of new technologies while protecting all of us from abuse, and the most vulnerable especially. While there are a number of international initiatives looking at how to meet these challenges, by far the most likely scenario is that piecemeal legislation will emerge, potentially starting with the EU's AI Act and (the new kid on the block) the AI Liability Directive.

The legislative juggernaut will gather pace in the EU which will impact countires outside Europe as well – including the Data Act and Data Governance Act – which emphasise that regulation of data is not just about personal data. The main theme is to improve access to and sharing of personal data and non-personal data, both on a business to consumer and a business to business level.

The European privacy laws are currently the world's most powerful data protection framework.

Extraterritorial applicability, conditionalities for personal data transfers, and multilateral treaties have helped spread European data protection laws worldwide. Two of the most prominent EU privacy laws you need to know: the ePrivacy Directive (ePD) and the General Data Protection Regulation (GDPR). The ePrivacy Regulation, under debate, aims to replace the ePrivacy Directive, which, among other things, demands the end user's consent for the use of cookies and tracking technology.

The Evolving Landscape of European Data Privacy Laws

- The GDPR is undoubtedly the most well-known and influential worldwide data privacy law to date, and it continues to affect current policies.
- According to the ePrivacy Directive, people must opt in before a corporation can send them communications.
- Digital Markets Act restricts large corporations from abusing their market power and allows new players to enter the market.
- Digital Services Act creates a transparent and safe online space to safeguard users from illegal content, online discrimination, and cyber assault.
- The Draft Data Act regulates the data created by IoT devices, ensures fair use and access, and gives consumers and enterprises control over their data.
- European Health Data Space (EHDS), Data Governance Act (DGA), Artificial Intelligence Regulation, and ePrivacy Regulation are examples of the evolving privacy landscape in the EU.

MAIN ACHIEVEMENTS OF THE DATA PROTECTION OFFICE

1. **Fact sheet on Legitimate Interest**

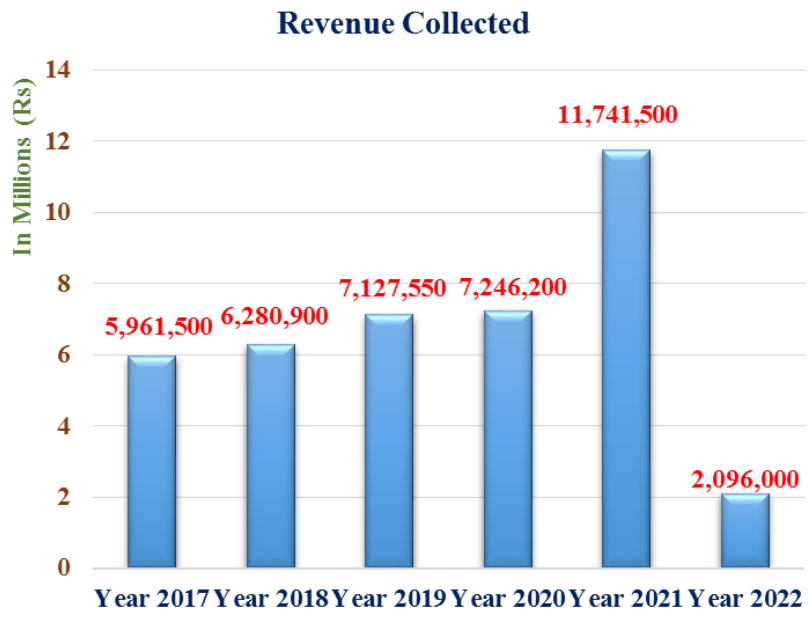
   The office published a fact sheet on “legitimate interest” to assist controllers and processors understand what this terminology means as per the provisions of the DPA and how it can be applied in their business operations. The fact sheet covers the following main aspects:

   - Lawful processing of personal data
   - Legitimate interests as a lawful criterion for processing
   - Criteria of legitimate interest
   - Steps to consider when performing the legitimate assessment
   - Examples

   The fact sheet is published on the website of the office

2. **Revenue collected**

   The DPO collected a total revenue of **Rs 11,741,500** in 2021 and **Rs 2,096,000** as at September 2022.



3. **Working visit in Rwanda and other African Countries:-**

4. **Revision and modernisation of SADC Data Protection Model Law**

   Southern African Development Community (SADC) developed the SADC Harmonised Cybersecurity Legal and Regulatory Framework in 2012. The Framework consists of three model laws including the SADC Data Protection Model Law.

   An assessment which began in 2018 established that the Data Protection Model Law needed revision and modernisation with due consideration among others to the national and regional context for privacy to ensure the safety and security of SADC citizens. The overall objective of the assignment was to review, revise and modernise the model law which would result in an enhanced Data Protection Model Law.

5. **Revision and modernisation of SADC Data Protection Model Law (CONTD)**

The Ministry of Foreign Affairs informed this office that the SADC Data Protection Model Law was being reviewed by SADC Secretariat and a consultant was recruited to conduct the study and would be engaged with member states on initiatives relating to data protection laws and regulations.

The Data Protection Commissioner was nominated as focal point by our parent Ministry to assist the consultant in this exercise. In July 2022, the Data Protection Office completed the questionnaire sent by SADC which aimed at gathering inputs on the description of data protection law in Mauritius.

6. **New Computerised System**

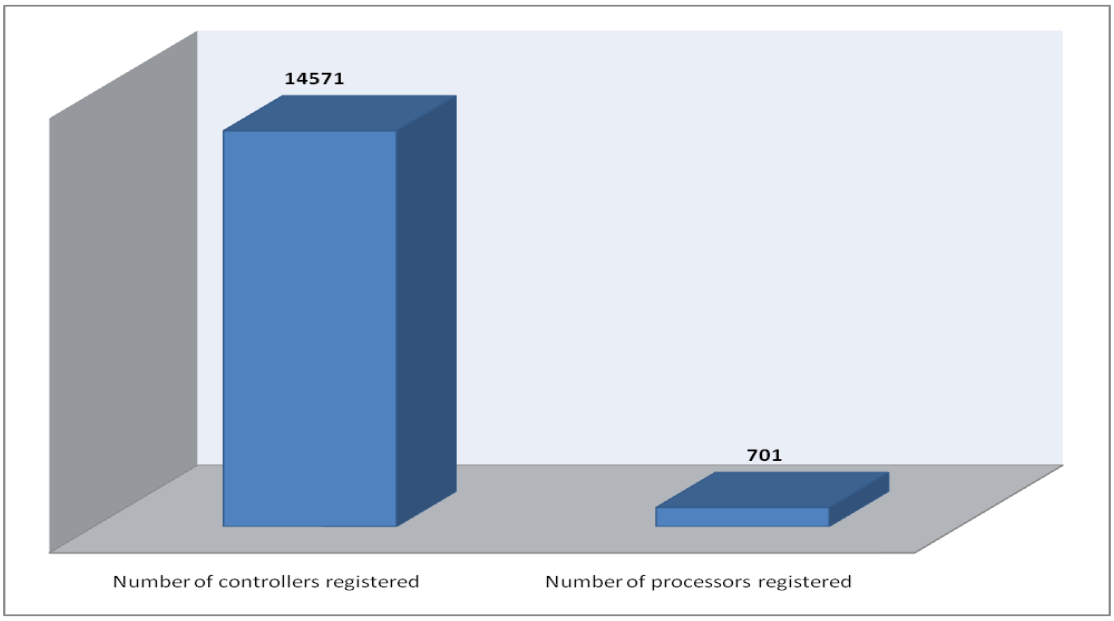
The DPO has embarked on a project to computerise its services to the public which will allow for the online submission and e-payment of controller/processor applications, the automatic generation of certificates of registration, the electronic submission of complaints, authorisations of transfer of personal data abroad, data protection impact assessments, certifications, data breach notifications and compliance audits. The new computerised system is expected to go-live in December 2022.

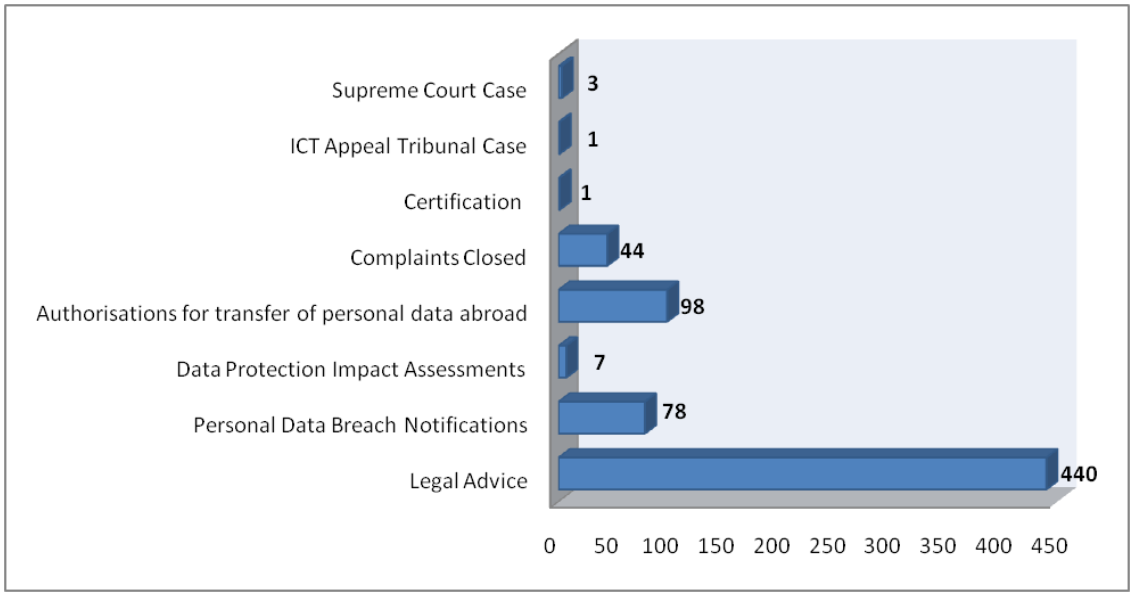
7. **European Union Adequacy**

In conjunction with the adequacy requirements established by the European Union, the office prepared and submitted a report to the European Commission (EC) Directorate for its study and perusal with a view to a subsequent adequacy finding for Mauritius. The report aims to provide an overview of the Mauritian system in order for the EC to conduct an objective assessment.

This office had several online meetings with the EC and submitted various documentations upon their request. The office is awaiting further update from EC.

8. **Enforcing Data Protection Statistics 2021 – 2022**





9. **Statistics & Nature of Cases/Complaints**

For the year 2021 to October 2022, 135 complaints have been received at the DPO.

Out of the 135, 34 complaints have been resolved. 101 complaints are still ongoing which are classified as per table below:

Nature of Complaint	Total
CCTV Cameras	**125**
Fingerprints	**1**
Unlawful Disclosure of Personal Data	**8**
Rights of Data Subject Access	**1**