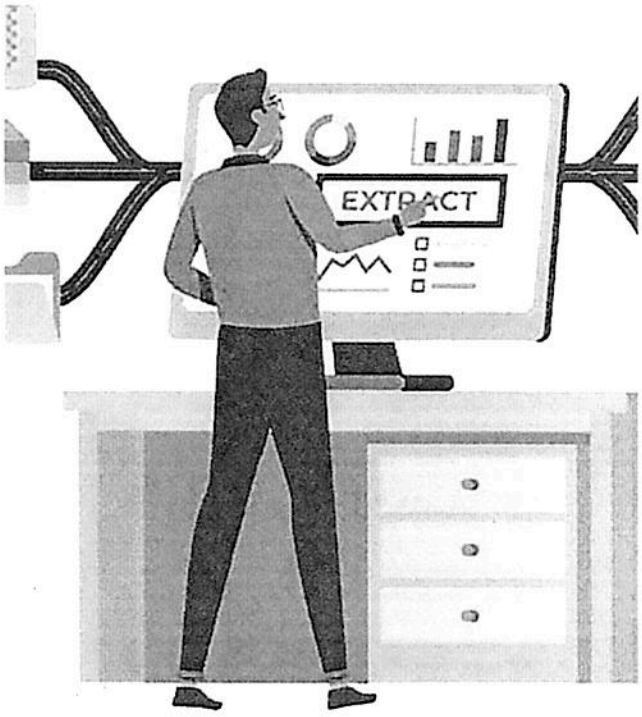
DATA PROTECTION FROM A BUSINESS AND ECONOMIC PERSPECTIVE

BY DRUDEISHA MADHUB,
Data Protection Commissioner



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 lawfully will influence users' trust in businesses and their profits. Here are the top data privacy trends and tendencies that one needs to understand in 2023, which are and will highly impact businesses worldwide including Mauritius.

Data processing has taken on a critical role with the rise of an ever-expanding digital economy. The proliferation of data in the economy presents a tremendous opportunity to boost growth through efficiency and innovation. Rights and obligations over data must be clarified for the market to function efficiently, and the way in which these are effected will impact growth and equity. Data has long been of value in economic activity. The collection of personal data has always involved a trade-off between respecting the individual's desire for privacy and reaping the commercial and social benefits that can be derived from its collection and dissemination.

Effective data policy requires an integrated perspective to balance competing objectives: promoting growth and competition through data access, ensuring incentives exist for data to be collected and processed, promoting stability by adequate investment in cybersecurity and data protection, and ensuring that individual privacy preferences are respected. Organisations and individuals increasingly generate, collect and process personal data. A strong data protection framework helps foster consumer trust and increased use of digital tools, which in turn can incentivize investment, competition and innovation in the digital economy. They seek to identify specific attributes of a data protection framework that can help policymakers and regulators build a digital economy that includes — and serves — everyone.

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 for breaches of personal data. Currently, advertisers and marketing agencies employ business models that rely on sharing personal information. However, this is changing fast. Privacy-enhancing technologies took the centre stage in 2022 and will continue to rise in 2023. 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 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. The European privacy laws are currently the world's most powerful data protection framework.

These privacy regulations and even cookies or other tracking technologies themselves are continually evolving, which means website owners should continuously update their current privacy policies and process personal information accordingly. A cookieless future is therefore 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 favour 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.

In light of the above, businesses that handle the personal information of users seriously will see an increase in their active users and profits compared to their competitors. Data subjects are becoming more aware of their rights and want to protect their personal information. As individuals 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. Increasing and changing privacy regulations worldwide will lead to more data security jobs for people in the coming year. The increase in related jobs in recent years dispels the myth that Data Science and Artificial Intelligence has replaced human labour.

The ongoing march of AI technology across all sectors will be shaping our societies in years to come, for good or ill. Likewise, there is much prominence given to the metaverse even if most of us are not yet clear how it will operate in practice and what are its implications 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.

With increasing reliance on cloud and online transactions, many organisations are handling more and more data. Bad actors, outside an organization and inside of it, constantly look to compromise an organization's data security for their own ends. Data breaches often aim to steal information from a company, selling it to others, or using it to commit acts of fraud. Since organisations handle a great deal of personal identifiable information from their customers, employees, and stakeholders, a data breach can do a great deal of harm. Some of the most potentially damaging effects come from data breaches that steal especially sensitive information, such as social security numbers, driver's licenses, and passports. If a bad actor gets their hands on this information, they can do a significant amount of damage to an organisation and anyone who has given the organisation data.

Most organisations have established business ethics policies, or a code of ethics. Even those that have not, still need to follow ethical practices if they expect to stay in business for any length of time. Such ethics policies typically indicate something to the effect that confidential information will be handled responsibly, not used in business activities in ways that do harm as a result, and used only as indicated for business purposes. By implementing security controls for personal data, breaches that negatively impact data subjects can be avoided.

Our mission is attaining ever-greater importance locally, regionally and across borders. Ensuring adequate data protection is proving day by day an increasingly essential prerequisite for any respected democracy to work healthily and fundamental rights and freedoms to be made real. It is imperative that privacy protections are reinforced at all levels and that all organisations commit to achieving a level of protection of personal data that corresponds to the changes linked to rapidly evolving technologies. Getting assurances that our data is protected and safeguarded is fundamental in order to prevent new technologies from becoming a threat - turning us all into the inhabitants of an out-of-control, disquieting technological world. Being aware of the demands for national security which fathers the claim for increasingly pervasive surveillance tools, the risks that society might jeopardise its own freedom and thus, its very soul, must be balanced with the need for defending itself in cases of emergency.

Privacy has become a necessity. The protection of personal data is no "luxury" or "decorative" item one can do without. It is actually indispensable in a world where using data is a vital precondition for economic growth, indeed for the very survival of businesses. Data protection, privacy and cybersecurity breaches are on top of the agenda of corporate and national data protection oversight agencies worldwide.

As we have seen, the environment we faced 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.

WHAT YOU NEED TO KNOW

The Data Protection 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.
Number of Registered Controllers: 15337
Number of Registered Processors: 721

During the year 2022, the following were accomplished:
Complaints Resolved: 36
Personal Data Breaches Processed: 22
Authorisations for Personal Data Transfers outside Mauritius: 72
Data Protection Impact Assessments processed: 3