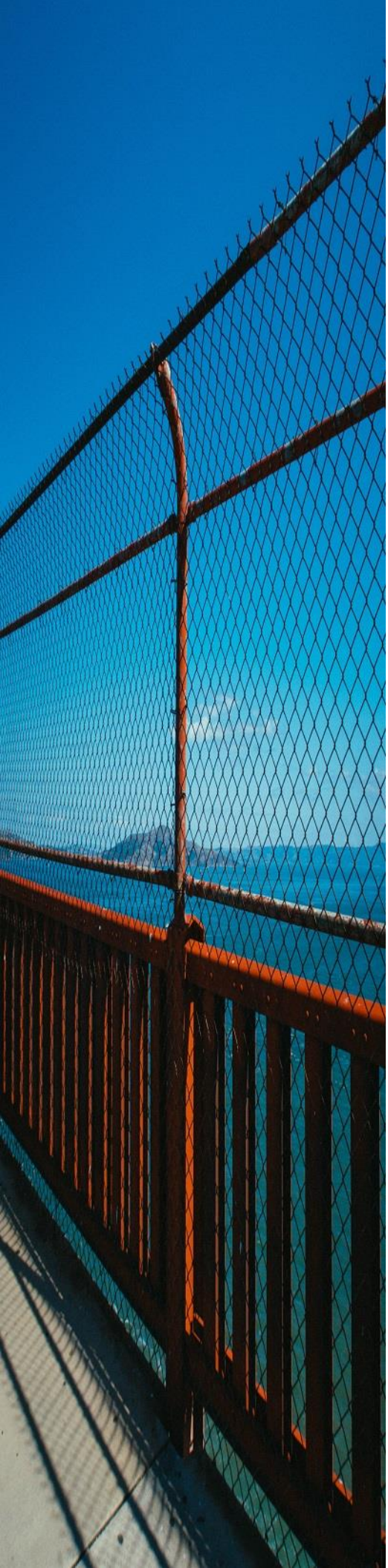
KPMG

Data Privacy

What does it mean for Organisations?

kpmg.com



Privacy is no longer as it used to be in the past. Traditionally, Privacy to a larger extent has been an individual responsibility however with the advancement and increased use of technology in recent times, a new phenomenon of data privacy has arisen and this has less to do with individual responsibility but more to do with responsibilities of organisations handling individual's personal data and the individual's rights as far as that data is concerned. Personal data is defined as information about an individual or group which means that any information relating to an individual that can be used on its own, or in combination with other information to identify an individual.

What is considered private and personal data may differ according to the society and the individual however there is now some global convergence in defining what is deemed private and the various pieces of legislation in various jurisdiction is showing this. It has become key for organisations in various sectors to also be proactive in putting measures to protect private data especially in an era where cybercrimes are on the rise. The points below give an overview of what data privacy is, its impact and how organisations can ensure a healthy privacy operational environment.

What is Privacy and Personal Data?

Privacy is the ability of an individual or group to seclude themselves, or information about themselves (personal data), and thereby express themselves selectively.

Personal Data includes:

- ❑ Your name
- ❑ Race or Ethnicity
- ❑ Email Address
- ❑ Physical Address
- ❑ Sexual Orientation
- ❑ Date of Birth

Privacy and Personal Data

There are other items which may not immediately look like personal data but when combined with other data or the above, become personal data for example when one signs up for competitions or customer loyalty cards information below may be collected and become personal data when combined with the above:

- Type of toothpaste you use
- Type of Milk you buy
- Number of times you buy alcohol in a month, to mention a few.

Because personal data relates to an individual, or allows identification of an individual, it needs to be carefully protected. However there is a subset of personal data known as sensitive personal data. Sensitive Personal Data includes Personal Data revealing an individual's:

- Race
- Ethnicity
- Political Opinions
- Religious or philosophical beliefs
- Criminal Background
- Trade Union memberships
- Health or sexual orientation
- Biometric or Genetic information (according to the General Data Protection Regulation)

This category requires extra care when handling or storing.

Data privacy in this case entails the preservation and protecting any personal information, collected by any organization, from being accessed by a third party. Personal data can be maliciously used and it is imperative for organisations to prevent this from happening as it may have long term consequences. Some of the principles of data privacy below provide guidance to ensure privacy and fair processing of personal data:

Principles of Data Privacy

- **Transparency**
  Being informed about the purposes for which one's data is being collected and used is important to ensure that processing is fair.

- **Purpose**
  Limitation An individual may choose not to consent providing their information where an organisation uses data not known to the individual or where it discloses an individual's information to any one else.

- **Data Quality and Proportionality**
  Personal data collected should be reasonable, kept accurate, up to date and should not be excessive in respect to the purposes for which it is collected.

- **Security and Confidentiality**
  Reasonable precautions such as technical, physical and organisational security measures must be taken to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

- **Access, rectification, deletion and objection**
  Individuals should have access to their Personal Data held by organisations, where those requests are reasonable and permitted by law or regulation. Individuals should also be able to object to the processing of their Personal Data if there are legitimate grounds relating to their circumstances.

- **Sensitive Data**
  Additional measures should be put in place to protect sensitive data.

- **Data Minimisation**
  Data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy

DATA BREACHES

These occur when private or confidential information pertaining an individual is accessed, collected, used for use other than which it had been originally collected for or in the case of organisations that have privacy policies, the use or access of data contravenes the policy.

Breaches occur either intentionally or unintentionally, however, the effects are equally devastating to the affected parties. Intentional breaches include hacking, phishing, ransomware and insider threat and are explained as follows:

- **Hacking** is unauthorized intrusion into a computer or a network. It is normally used to attack financial institutions with the intention of financial gain. As financial information is stolen, so is personally identifiable or confidential information and the information may be sold to thieves who will pay good money for it.

- **Phishing** is when emails or phone calls that seem authentic are used/or outright deception in the form of these is used on individuals in order to have access to personal information.

- **Ransomware** is when computers are locked by malware and payment demanded in order for access to be returned to the affected party. The affected party is notified of the breach or attack and given instructions on how to recover from the attack, usually, upon payment.

- **Insider threats** are perpetrated by individuals within a business or organisation who have information on the organisation's practices.

Unintentional breaches are normally caused by poor judgment or failure to follow company policy which subsequently results in exposure of confidential information. These type of breaches occur as a result of for example clicking links of phishing emails or losing storage media (which is unencrypted) or hard copy files containing sensitive information.

EFFECTS OF DATA BREACHES

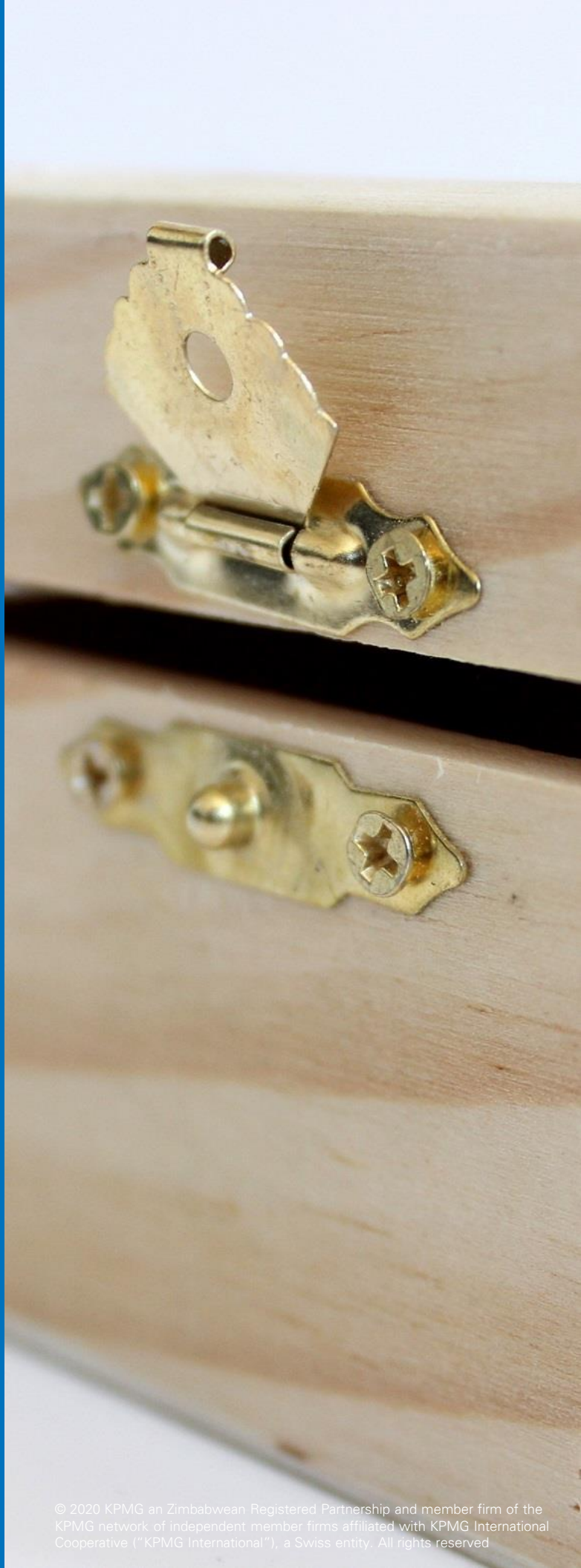
There are a number of consequences that come with data breaches and this has overall negative impact on organisations handling the data. The impact of a breach is tied to the type of data involved. Breaches of privacy can expose individuals to risks such as embarrassment, loss of employment opportunity, loss of business opportunity, physical risks to safety and identity theft. In worst case scenarios for individuals, if personal and financial details of staff and customers are breached, the affected individuals are left open to the risk of identity theft. In as much as organisations are affected, the effect is equally devastating to the affected individuals. At times when an organisation's confidential data has been exposed, it can have catastrophic effects. Some of the impacts of data breaches are detailed below:

❑ Regulatory/Legal affirmative

Lawsuits are on the rise and breaches may lead to a variety of private suits. Employees, customers, clients, and patients whose information is exposed may bring individual or group action suits under many causes of action, including breach of privacy, negligence, breach of contract, and violations of state statutes. In addition, shareholders may bring derivative suits against directors alleging breach of fiduciary duty and corporate waste.

The European Parliament and Council passed the General Data Protection Regulation (GDPR) in May 2018 with the aim of protecting European Union (EU) citizens'data privacy and creating consistency of data privacy laws across Europe. All organisations within or outside the EU processing personal data of data subjects residing in the EU will be required to abide by the regulation. Breach of the GDPR may result in fines of up to €20 million, or 4% of the worldwide annual revenue of the prior financial year.

While the EU has one regulation covering all EU citizens, the United States of America implemented sector specific data protection laws and regulations that work hand in hand with state-level legislation for example the Health Insurance Portability and Accountability Act (HIPAA) created to secure protected health information (PHI) by regulating healthcare providers and NIST 800-171 released by the National Institute of Standards and Technology aimed at protecting Controlled Unclassified Information (CUI) in non-federal information systems and organisations. Breaches apply and in an instance where the HIPAA has been breached a minimal fine of USD 50,000 and up to one-year imprisonment may be imposed.



KPMG

EFFECTS OF DATA BREACHES

❑ Reputation / Brand Name

A security breach can impact much more than just an organisation's short-term revenue. A good reputation is often a company's most prized asset as a business must work constantly to build and maintain the integrity of its brand. However, one compromising episode like a data breach can tarnish even the best of reputations. An instant error such as a data breach that could have been prevented can cause an organisation to lose a good customer base. This subsequently results in a potential disaster for a customer-focused business strategy.

❑ Lost customer trust

Potential customers will hesitate to trust the organisation in fear of their personal information/data being exposed as they value their privacy too. Clients share their sensitive information with businesses frequently, assuming the businesses have the proper security measures in place to protect their data. As soon as a data breach occurs, customers will question the amount of trust they have put into a business. Rebuilding trust is then often a challenging task regardless of how an organisation has been performing financially.

❑ Financial

Financial Impact may not always be as significant or transparent as initially thought but however it increases over time. The loss of customers results in lost revenue and lowered investor confidence also results in lost market value. Once businesses are aware that there has been a data breach internally or a system housing identifiable information has been infiltrated by an outsider, the most common course of action is to stop or slow operations until a solution is found which means revenue slowly flows in. Implementing defensible data privacy practices is not cheap and opting out is definitely expensive. Organisations will have to incur costs of trying to implement corrective measures to ensure there are no future breaches.

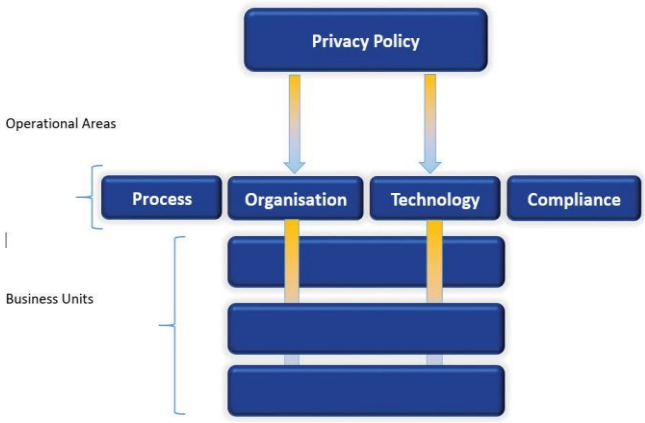
KPMG

What can Organisations do to maintain Data Privacy?

A

Just like any other operational environment, there needs to be a policy governing the operations within a business. Do not share is the ideal, but not a pragmatic option for some companies hence having a Privacy Policy would be a value-add proposition for customers and for companies. However, before coming up with a policy it may be necessary to come up with a questionnaire to identify whether the business/organisation will collect, use, retain, disclose, secure or dispose of personal information and the type of information involved.

Once we have identified the personal information and forms of sharing information within and outside the organisation, a Privacy Policy is then established to cover all these aspects and it is important to note that data privacy is everyone's responsibility. The diagram below depicts the flow of privacy from establishing a policy to implementation by business units.



At operational areas, it is imperative to map the flow of personal information in all formats, from creation or collection, until final disposition including compliance to regulatory requirements where applicable, for example, secure destruction or transfer to appropriate archives. From the information flow assessments, business units will have to implement controls that will reduce probabilities of information leakage.

Other solutions of ensuring data privacy include:

- ❑ Ensuring that staff are properly trained and are aware of the potential privacy impact and appropriate privacy-protective measures to be followed;
- ❑ Creating retention periods that only keep information for as long as necessary and planning the secure disposal of information and
- ❑ Minimising collection of certain types of personal information.

Conclusion: An organisation's success has also become reliant on how well vigilant it is in protecting personal information as Data Privacy seems to be dictating business operations. The world is looking at how each business is handling privacy and that includes infiltrators.

KPMG

Contact us

Chamunorwa Madziwa
Manager IT Advisory
KPMG Zimbabwe
Tel: +263 242 303700/ 302600
Email: cmadziwa@kpmg.com

Faith Maraire
Manager IT Advisory
KPMG Zimbabwe
Tel: +263 242 303700/ 302600
Email: fmaraire@kpmg.com

Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.