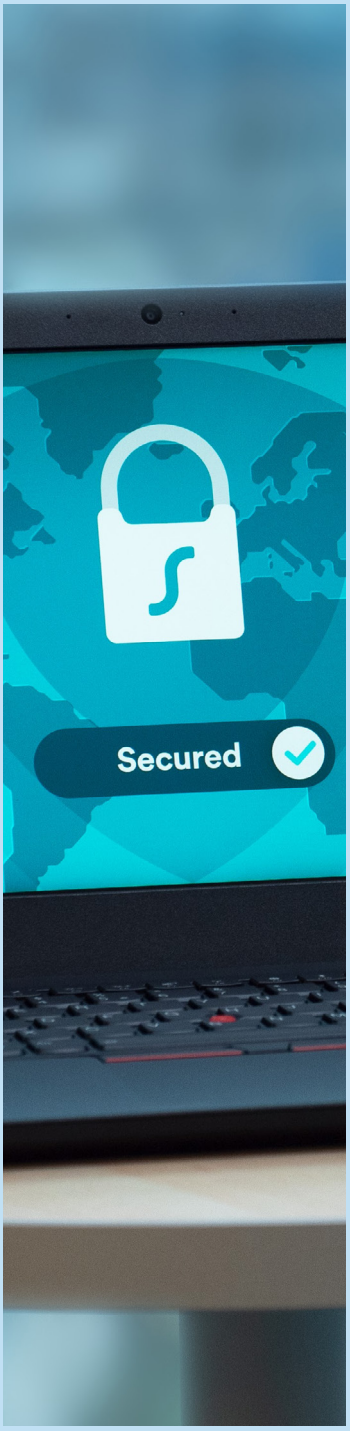
VIEW POINT



EMBRACE DATA PRIVACY TO FOSTER CUSTOMER'S TRUST

Infosys®
Navigate your next

'Data is the new Oil', this quote coined by a British mathematician in the year 2006 has proven correct in this digital age where data runs major businesses and holds tremendous value. Nowadays, companies are collecting voluminous customer data, with or without their consent. They are investing heavily on data analytics to fuel their marketing strategies but often end up mishandling this data.

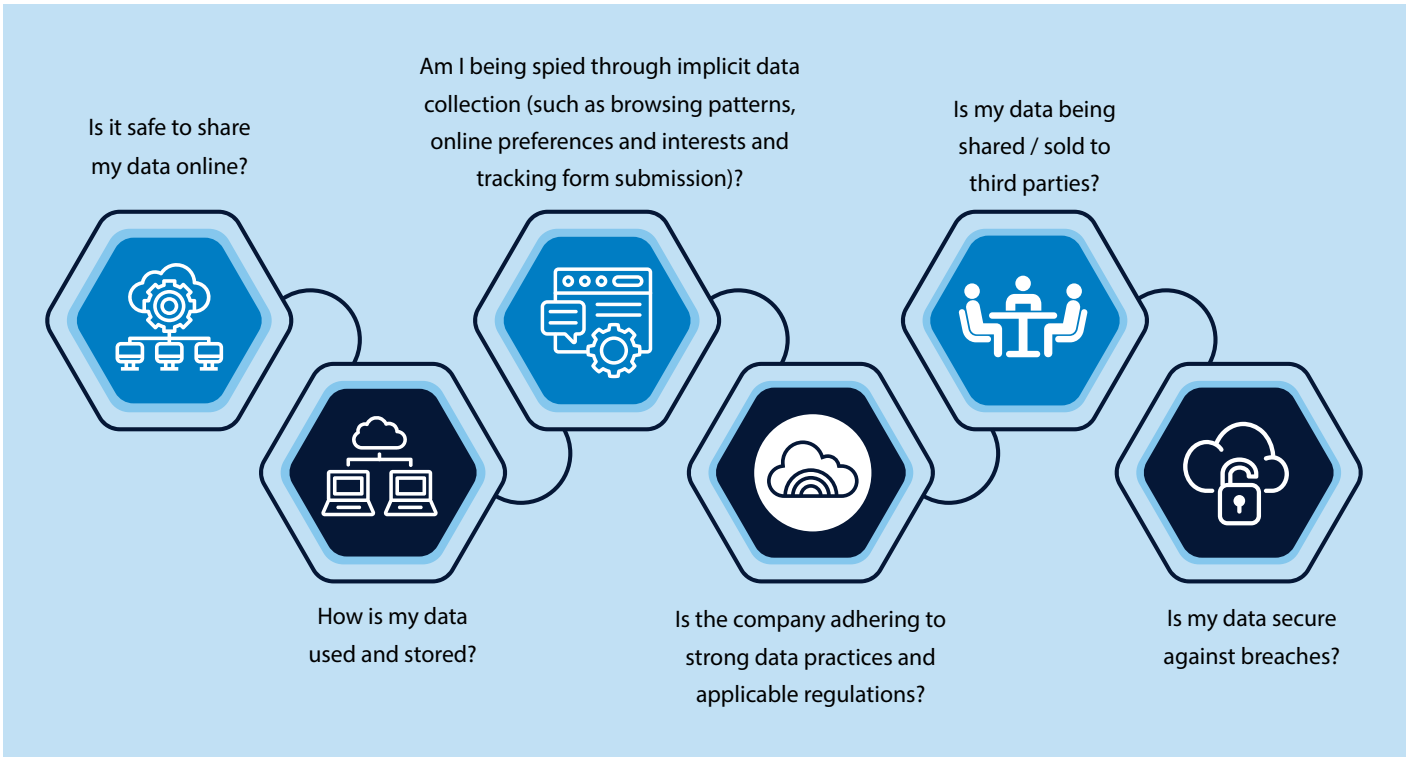
With the increased sensitization on data privacy and enforcement of stringent regulations, consumers are becoming aware and concerned about their data and often feel hesitant to share it with an untrusted company. Hence, opaque data handling practices and misuse of customer's private information may not be a sustainable strategy for a company. It is high time that companies focus on building strong data privacy and security practices to foster customer's trust. Data privacy should not just be viewed as a risk management issue, but a prominent factor to gain competitive advantage and stand out as a reputed customer-centric brand.

External Document © 2022 Infosys Limited

Customer's Data Privacy Concerns

According to a recent survey conducted by Cisco, nearly half of the customers feel that they are unable to protect their data effectively. A major reason behind this concern is lack of transparency and clarity of company's data handling practices. Customers also feel that companies are not adhering to the stated policies. This distrust has forced them to terminate long-term relationships with companies. In March 2017, personally identified data of millions of people was stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States. Not only did the company face hefty penalties and financial loss, but also lost its trust and reputation amongst the customer base. Needless to say, there is a growing concern on the usage and security of personal data held by companies.

Some of the key concerns of customers are:

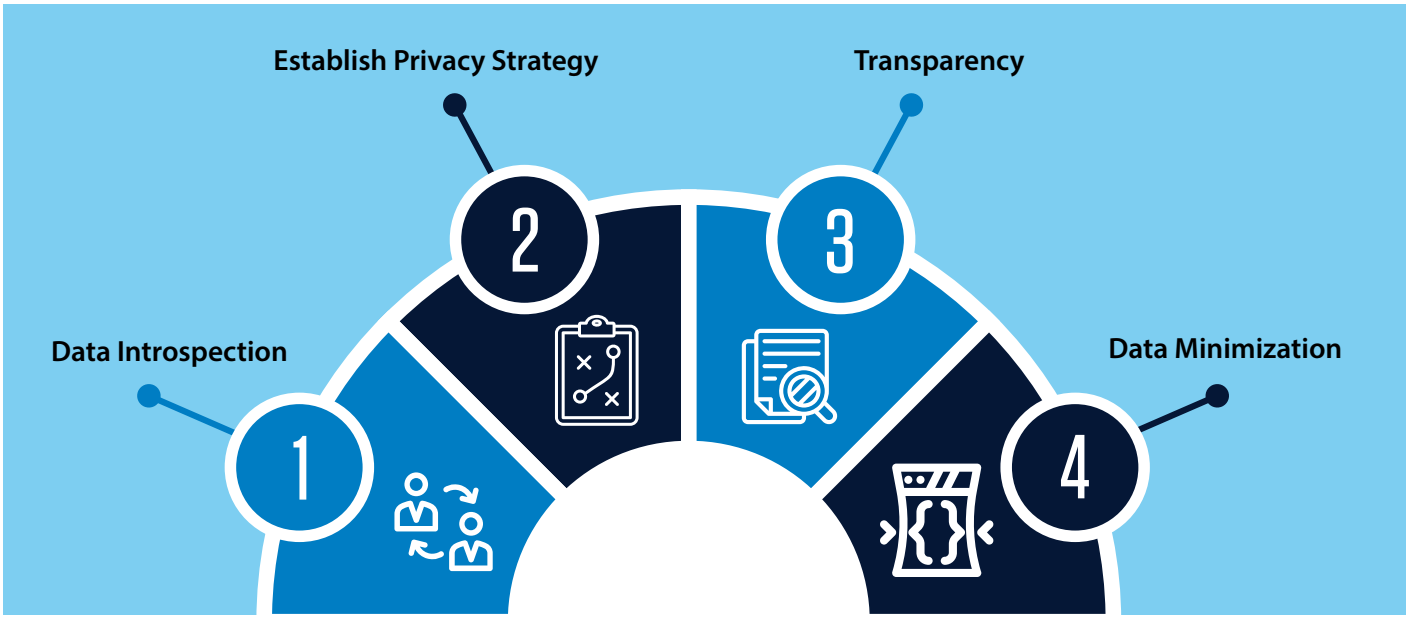


External Document © 2022 Infosys Limited

Holistic Approach to Strengthen Data Privacy

In a survey of 250 business leaders conducted by KPMG, 70% say that their companies have increased collection of consumer's personal data over the last year. 62% of the leaders strongly feel that the organizations should focus on safeguarding data privacy and assuring customers that their data is secure.

Focus Areas



Data Introspection

Starting with creating a data inventory that records all data points from collection till deletion will provide a visibility of what we should strive to protect. This exercise will create a baseline of data privacy strategy and will provide answers to questions such as:

- What type of data is being actively collected?
- What data is actually being used?
- Where is this data residing and for how long?
- Is this data being shared with third parties?

Establish Privacy Strategy

Once data inventory is created, company will understand what strategic controls needs to be implemented considering the nature of products and services as well applicable privacy laws and regulations.

A comprehensive privacy policy should document what data is collected, why it is being collected, how will it be used, whether it will be shared with third parties and how it will be secured. Organizations should make their privacy policy available to public in concise and simple language in order to showcase transparency and commitment towards data privacy.

Creating a privacy organization headed by Chief Privacy Officer is now being widely adopted by companies who are concerned about data privacy.

Transparency

It is important for organizations to maintain transparent communication with customers on why and how they intend to use and manage their personal information. This can be achieved by adding data privacy in their value propositions and proactively communicate about preferences and consent.

It is important to establish communication channels to address customer's concerns, queries as well as requests regarding their data. A dedicated email id or helpline number provides an assurance and comfort to customers that support is available to resolve their concerns.

Data Minimization

In the process of data introspection, organizations may also realize that they are collecting more data than needed. As a rule of practice, organizations should collect required data with the consent of customers and provide them an opportunity to opt out of sharing personal information. The customers should also be able to control their personal information by stating what information can be shared with third parties.

External Document © 2022 Infosys Limited

Data Protection Controls

As an organization's privacy policy is established, the next step is to identify appropriate processes and controls to align with the strategic objective. As data is being handled by multiple internal employees across different departments and functions, it becomes challenging for organizations to enforce the controls uniformly. Further, remote working has diluted some of the stringent controls implemented in physical workspace as employees located in different geographies access data over the internet, sometimes using unmanaged devices.

In order to understand the appropriate level of controls required to safeguard data, organizations should conduct two important exercises – data classification and risk assessment.

Data Classification

Data is classified into various categories such as public, confidential, internal or sensitive based on factors such as its purpose and business impact if data is lost or stolen.

Risk Assessment

Identifies all the possible threats to data, assess the risk of these threats and its impact to the organization.

Organizations adopt widely known and acknowledged information security standards to design their security frameworks and practices. This provides an assurance to the customers that their data is being adequately safeguarded against cyber-attacks and breaches.

Data Masking, Encryption and Pseudonymization

These mechanisms protect against advertent or inadvertent disclosure of sensitive data at rest (storage), in transit (communication channel) as well as in use (Application, temporary storage, memory). Pseudonymization techniques when applied to personal data, makes it impossible for anyone to attribute to a specific person without the use of additional information.

External Document © 2022 Infosys Limited

Zero Trust Architecture

Zero Trust model brings "never trust, always verify" strategy. This process verifies each request whether its coming from users or devices connected through organization's/private network or through internet/public network. It makes no difference if we have accessed the network before or how many times — identity is not trusted and needs to be verified again and again. Access to confidential and sensitive data should be restricted only to authorized individuals on need basis e.g. HR team should have access to only HR systems, files & folders based on individual's roles and responsibility. Multi-factor authentication and condition-based access control should be implemented to mitigate the risk of data breach. Conditional access helps in defining controls to restrict or grant access to corporate data based on user's role, device type, location, suspicious behavior, device settings, and a host of other variables. Access logs can be maintained to perform periodic audit and review of user activities and revoke unnecessary or suspicious access.

Data Leakage Prevention

As employees work on customer data, there is a potential risk of stealing or misusing this information by leaking it on internet, personal devices or other media. In order to prevent data exfiltration, organizations are now investing in Data Leakage Prevention (DLP) solutions that monitors and prevents data from leaving company's managed network or devices.

Information Rights Management

Information Rights Management (IRM) solution enables organizations to have better control on their data by defining granular permissions for authorized users. It is very useful solution for organizations that share data not just amongst the internal functions but also beyond company's perimeter with third parties.

External Document © 2022 Infosys Limited

Conclusion

Businesses are driven on customer's data - machine learning data models, targeted marketing campaigns, personalized customer experience and advertisements are data-intensive processes to continuously improve services and expand foothold in the market. With the increasing dependency on personal information to thrive the business, it is imperative for companies to maintain transparency about their data usage and handling practices and strengthen their data privacy and protection framework to safeguard customer's personal information. Data privacy is more than complying with laws and regulations, it is about enabling customers to have control over their personal information and providing assurance that their information is secure against unauthorized access or breach.

External Document © 2022 Infosys Limited

About the Author

Saurabh Sharma
Saurabh works as a Data Privacy & Protection Consultant with Infosys Cyber Innovation Strategy and Excellence team which dwells into next generation cybersecurity solutions and strategies.

He has 12 years of experience in consulting, assessment and implementation of Data Protection and building Data Privacy solutions. He has extensive knowledge and experience in Infrastructure and Cloud Security domains as well.

References

1 https://www.researchgate.net/search/publication?q=Information%2BPrivacy&page=4

2 https://www2.deloitte.com/us/en/insights/topics/risk-management/consumer-data-privacy-strategies.html

3 https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust

4 https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

5 https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

6 https://www.cpomagazine.com/data-privacy/kpmg-reports-lack-of-corporate-data-responsibility-eroding-consumer-trust-preventing-users-from-sharing-data/

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2022 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.