ENHANCING DATA PRIVACY

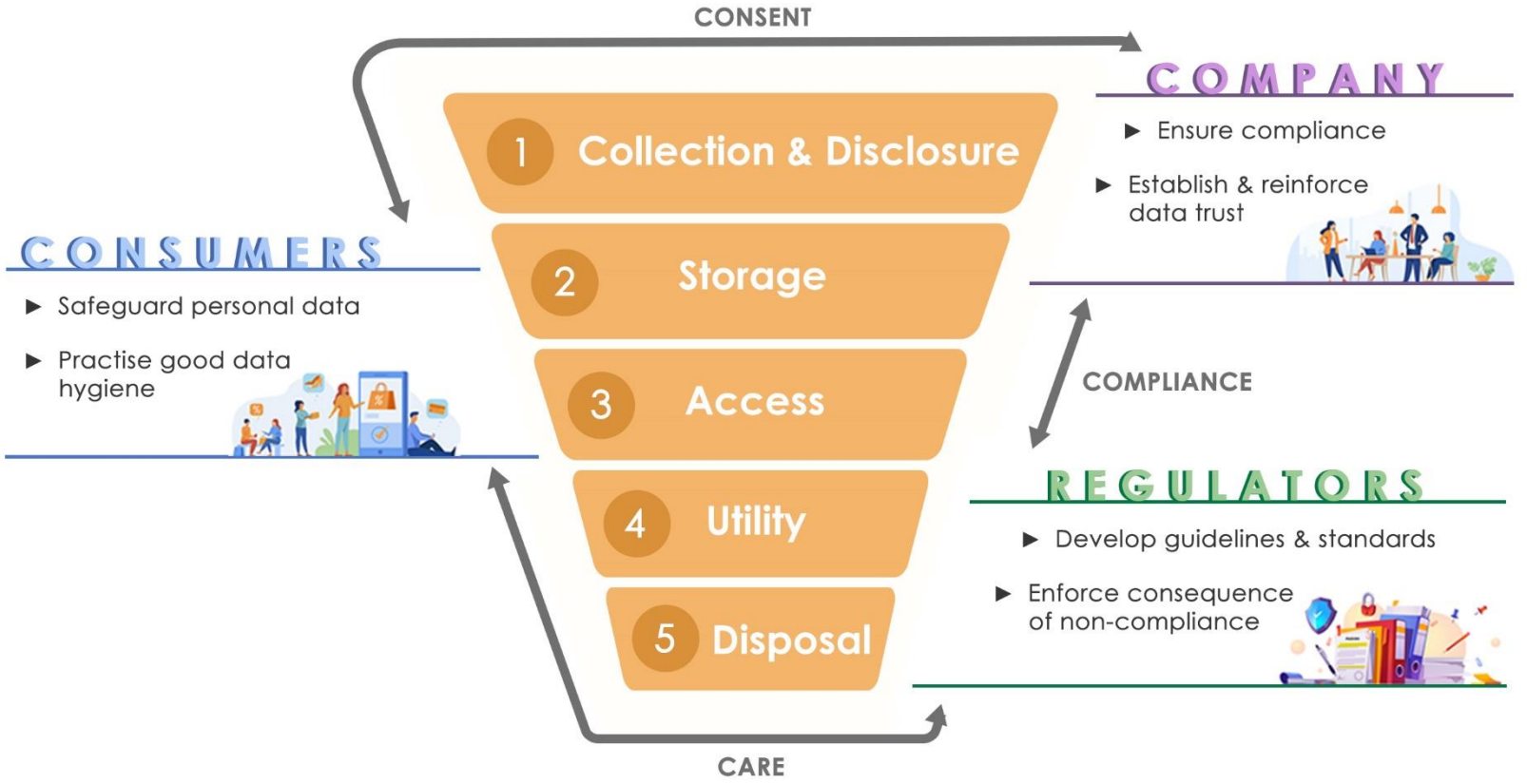
THE KEY TO CONSUMERS' TRUST

Data privacy concerns are coming to the fore, with increasing consumer interest around how identifiable and sensitive personal data is being used, or even abused[1].

Consumers need a sense of security when sharing their personal data, and organisations that address these concerns early will be able to gain consumer confidence and mitigate potential corporate risks such as public backlash, fines, financial loss, damage to stakeholder and corporate reputation, and more[2].

The organisations that are able to build and maintain trust throughout the data lifecycle (from collection to disposal), while concurrently managing key stakeholders, such as regulators and consumers, will be in prime position to realise the full value of the consumer data they have on hand.

THE QED DATA TRUST & PRIVACY ASSESSMENT & TRAINING TOOL



	KEY AREAS		CONSIDERATIONS	IMPLICATIONS
1	COLLECTION & DISCLOSURE	• Collection entails defining or revisiting your data strategy (intentions for collecting data and their use cases) *before* collecting consumer data • Disclosure deals with ensuring transparency with consumers through your disclosure policies; that they cover the reason(s) for your data collection	• Do you have a data governance / collection policy? Is it easily available across all your customer touch points e.g. company website, app? • How well defined are your data collection intentions (presently and for the future)? • Do you update your disclosures and inform your customers when the nature of your data use changes? • Is your data collected fit for purpose?	• A lack of transparency results in loss of consumer trust[3] • Consumers may challenge the use of their data regarding undisclosed use cases / propositions • Your organisation may possess consumer data with inadequate disclosures → Results in regulatory implications / breaches • Your organisation may be over-collecting (or undercollecting) data currently, thus limiting your future growth
2	STORAGE	• Storage relates to having a clear strategy to secure and retrieve data from where it is stored	• Do you have a clear data storage strategy e.g. on premises vs. cloud? • Do you have a comprehensive consumer data storage policy and capability? • Do you have personnel looking into the security of your data?	• Data lying in different systems create multiple points of breach, exposing data to theft and manipulation[4] • Without comprehensive data storage, useful data can get lost
3	ACCESS	• Access pertains to which persons are able to access customer data and how are they able to do so	• Do you know who has access to your customer data? • Do you have clearly defined access rights for your employees?	• Illegal entry by bad actors as a result of insufficiently defined access points[5]
4	UTILITY	• Utility concerns how data is used to drive business growth and optimisation in organisations	• Are you transparent to consumers and employees about how you use data to make business decisions? • Do you have a comprehensive understanding of all the use cases of your data? • Does your data use impact consumers negatively e.g. surveillance? • Is your data usage abiding by the 9 PDPA obligations?	• Consumer trust is lost when their data is used for undisclosed purposes, and they may raise their objections to regulators • Employees may use data to drive decision-making without being transparent or considering biases • Organisations may commit regulatory breaches resulting from the misuse of consumer data[6]
5	DISPOSAL	• Disposal deals with how data are purged permanently when customer relationships end, ensuring no unauthorised recovery of deleted data	• Do you dispose of expired, over-retained or unused data sets? • Do you have a consumer data disposal policy, and do you have personnel responsible for its implementation?	• Data is open to misuse if retained longer than necessary[7] • Data retained post-conclusion of customer relationships may not be aligned with PDPA guidelines

Contact us to find out how you can build and establish consumer trust in areas of consumer data privacy.

If you face gaps in two or more of the Consideration areas listed in the Data Trust & Privacy Assessment & Training Tool, consider closing these vulnerabilities before they become significant issues of corporate concern.

Please get in touch

- dataprivacy@qed.sg

Ryan Lim
Principal Consultant & Founding Partner,
QED Consulting

Ryan advises senior management teams of some of the world's leading businesses and brands on extracting business value and mitigating risks in their investments in digital, marketing and communications. He has been a digital marketer for over 19 years, and is a pioneer in social media marketing.

Natasha Zhao
Partner & Senior Consultant,
QED Consulting

Natasha advises & builds strategies for Fortune 500 Multinational Corporations & Small to Medium Enterprises that leverage digital mediums to drive their business in both local and regional markets. She has over a decade of experience in digital communications.

Sandeep Bhalla
Senior Advisor, Boston Consulting Group
Advisor, QED Consulting

With over 20 years' experience in financial services, Sandeep has managed large and diverse P&Ls and delivered digital transformation to front line business units in consumer banking, payments, risk management, and loyalty. Sandeep was formerly Chief Analytics Officer of NTUC Group and Chief Executive Officer of NTUC Link.

Ang Peng Hwa (Prof.)
Professor, Nanyang Technological University
Advisor, QED Consulting

Prof. Ang teaches and researches law, policy and ethics around media and the Internet at the Wee Kim Wee School of Communication and Information, Nanyang Technological University. He served as director of the Singapore Internet Research Centre at the School where he was also the Chair. He has consulted for the governments of Singapore, Thailand and Bhutan. Currently, he is affiliated with Goodwins Law Corporation for data privacy.

References

1: Reuters (2020), 'Singapore's use of facial verification in ID scheme stirs privacy fears'
Nikkei Asia (2020), 'Singapore-Apple app spotlights Asia's health-privacy tightrope'

2: The Straits Times (2018), 'Shock, anger and worry about stolen data being misused'
Vulcan Post (2019), '2019 Is A 'Fine' Year: PDPC Has Fined S'pore Firms A Record $1.29M For Data Breaches'
ZDNet (2019), 'Employees sacked, CEO fined in SingHealth security breach'

3: TechCrunch (2019), 'Your mass consumer data collection is destroying consumer trust'
McKinsey & Company (2020),'The consumer-data opportunity and the privacy imperative'
Los Angeles Times (2020), 'Muslims reel over a prayer app that sold user data: 'A betrayal from within our own community''

4: VentureBeat (2018), 'McAfee: 26% of companies have suffered cloud data theft'
The Washington Post (2020), 'How the cloud has opened new doors for hackers'
Forbes (2020), '5 Key Security Lessons From The Cloud Hopper Mega Hack'
Data Center Knowledge (2020), 'Hackers Use Java to Hide Malware on the Data Center Network'

5: Security Magazine (2015), 'The Consequences of Neglecting Access Management'
Computer Weekly (2016), 'Security Think Tank: Many breaches down to poor access controls'

6: The Straits Times (2020), 'Parliament: Proposed changes to PDPA include stiffer fines for data breaches, mandatory notification when they occur'
PDPC Singapore (2021), 'Most recent 25 decisions'

7: Channel NewsAsia (2020), 'Lazada suffers data breach; personal information from 1.1 million RedMart accounts for sale online'
The Straits Times (2020), 'Personal data from 2.8 million Eatigo accounts stolen, put up for sale online'