UTeM
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MCMC

DSRG
DIGITAL SOCIETY RESEARCH GRANT

Security And Privacy Challenges Of Big Data Adoption: A Case Study In The Telecommunication Industry

Syarulnaziah Anawar, Nur Fadzilah Othman, Siti Rahayu Selamat,
Zakiah Ayop, Norharyati Harum

Research Symposium 2022:
"Towards an Inclusive Malaysia: Research Insights on the Implications of Digital Communications on Society"

Research Objectives

MCMC DSRG DIGITAL SOCIETY RESEARCH GRANT

Investigate perspectives of telecommunications data users in addressing privacy and security issues. Perspectives sought shall include perceived risks and mitigation, industry and/or internal standards being applied process and modes of redress for data subjects, and compliance requirements.

Investigate perspectives of data subjects (telecommunication users and subscribers) on issues pertaining to privacy and security issues and correlation with take up and continued use of applications and services utilising Data Analytics

Comparative review of codes of practices and standards being used by local and international telecommunications providers and recommend potential areas for improvement and/or adoption.

Methodologies

MCMC DSRG DIGITAL SOCIETY RESEARCH GRANT

Research Phase	Research Activities	Research Objective	Research Deliverable
Phase 1: Qualitative Study	• Literature review • Interview instrument design • Data collection (Focus Group) • Data reduction • Data display • Conclusion drawing	Objective 1	Deliverable 1 Big data adoption assessment for Data Users
Phase 2: Quantitative Study	• Survey instrument design • Content validation. • Forward-backward translation. • Pilot study. • Perform data collection using proportional quota sampling • Construct validation • Descriptive analysis • Path analysis	Objective 2	Deliverable 2 Big Data adoption assessment for Data Subjects
Phase 3: Systematic Review	• Region and telco providers identification • Data collection: Code of practice and rivacy notice collection • Review principles and features determination • Feature extraction: content • Features classification	Objective 3	Deliverable 3 Privacy Notice Assessment for local and international telecommunication provider

RO1-Sub RQ1: What are the perceived security and privacy risks and mitigation strategies by the telecommunication provider for big data adoption?

MCMC

DSRG
DIGITAL SOCIETY RESEARCH GRANT

Context	Themes	Dimension	Explication
Technological	**Integrity and reactive security (7)**	Advanced security analytic (3)	Real-time threat detection tool with enhanced network-based security analytics and forensic.
		Reactive Security (1)	A measure was taken based on detected threats from real-time monitoring.
		Security automation (3)	Security tools and technology that monitor, detect, troubleshoot, and remediate cyberthreats without human intervention.
	Data Management (16)	Data over-collection (1)	Collection of users' data more than its original function while within the permission scope.
		High volume (3)	A large number and diverse set of data from multiple sources.
		Data discrimination (1)	A bias occurs when predefined data types or data sources are intentionally or unintentionally treated differently than others.
		Data integration (2)	Process of bringing data from disparate sources together to provide users with a unified view.
		Data quality and usability (6)	The ability of data users to derive useful information from data.
	Data Privacy (14)	Data anonymisation (3)	Process of masking personally identifiable information with an irreversible value from data sets.
		Data encryption (2)	Process of encoding data from plaintext (unencrypted) to ciphertext (encrypted) to protect data confidentiality.
		Granular access control (8)	The practice of granting different levels of access to a particular resource to a particular user.
	Data Compliance (13)	Comp-Data collection (6)	The practice of ensuring the process of data collection is following legal requirements.
		Comp-Data injection (3)	The practice of ensuring the process of data injection is following legal requirements.
		Comp-Secondary use (4)	The practice of ensuring the use of personal information is following legal requirements and within what has been authorised.

RO1-Sub RQ1: What are the perceived security and privacy risks and mitigation strategies by the telecommunication provider for big data adoption?

Context	Themes	Dimension	Explication
Organisational Challenge	**Data governance (9)**	Data Stewardship (5)	Responsibilities on assuring that the right data gets to the right processes/parties in the proper format, and is compliant with the regulations.
		Data transposition (2)	Process of restructuring values or shape of data set.
	Subject Matter Expert (1)		Professionals who have advanced and specialised knowledge in the field.
Environmental Challenge	**Competition intensity and market structure (1)**	Competition intensity (1)	The degree of rivalry between providers within the telecommunication industry.
		Market Structure (2)	The number of providers and their market share.
	Relevant law and regulation (6)	Regulatory Change (1)	Any regulatory changes at a national and regional level that substantially affect the industry.
		Regulatory Orchestration (5)	A form of regulatory actors' engagement with industry players at different levels to address a target in the pursuit of public goals.
	Technological support (2)	Vendor Support (1)	The availability and ability of vendors to fulfil the implementation and use of a given technology.
		Open Source (1)	Open and publicly available tools and software.
		Leadership support	The organisation attitudes and behaviours of the top management in providing support and required direction to employees.

RO1-Sub RQ1: What are the perceived security and privacy risks and mitigation strategies by the telecommunication provider for big data adoption?

Context	Themes	Dimension	Explication
Mitigation Strategies	**Advanced Security Tools**		Real-time threat detection tool with enhanced network-based security analytics and forensic.
	Security Talent Development		The development of an employee's human capital as a resource for improving professional skills and quality in the security domain.
	Continuous Security Assessment	Security Assessment	Process of comprehensively analysing and evaluating the security attributes of the business operation.
		Audit	Examination of the practices, procedures, technical controls, personnel, and other resources that are leveraged to manage companies' security risks and assure that they adhere to best practices.
	Security Plan	Key performance indicator (KPI)	A set of quantifiable measures to evaluate organisational success in meeting the strategic goal.
		Strategic roadmap	a plan that defines the organisation's objectives, strategies, and pathways for the future.
	Security Culture Promotion	Awareness program	Activities that are designed to influence employees' secure behaviour by promoting understanding of endpoint security.
		Awareness training	Activities that are designed to influence employees' secure behaviour by introducing knowledge, skills, and competence of endpoint security.
		Leadership support	The organisation attitudes and behaviours of the top management in providing support and required direction to employees.

RO1-Sub RQ2: What are the industry and/or internal standards being applied for the mitigation strategies?

Risk/Concern	Industry and/or internal standards
Data Privacy	• Data protection impact assessments (DPIA) • ISO 27701- Privacy Information Management System (PIMS) • Personal Data Protection Act (PDPA) • General Data Protection Regulation (GDPR)
Data management	• Data protection impact assessments (DPIA) • ISO 27701- Privacy Information Management System (PIMS) • Personal Data Protection Act (PDPA) • ISO27001 – Information Security Management • Payment Card Industry Data Security Standard (PCI DSS)
Data Compliance	• Information Security Readiness Assessment • Cloud Security Alliance (CSA) practices • ISO27001 – Information Security Management • ISO 27701- Privacy Information Management System (PIMS) • Personal Data Protection Act (PDPA) • General Data Protection Regulation (GDPR) • Information Security Framework (ISF)
Advanced security technology	• Critical Security (CIS) control

RO1-Sub RQ3: What is the compliance requirement (external and internal) applied in the organisation?

MCMC

DSRG
DIGITAL SOCIETY RESEARCH GRANT

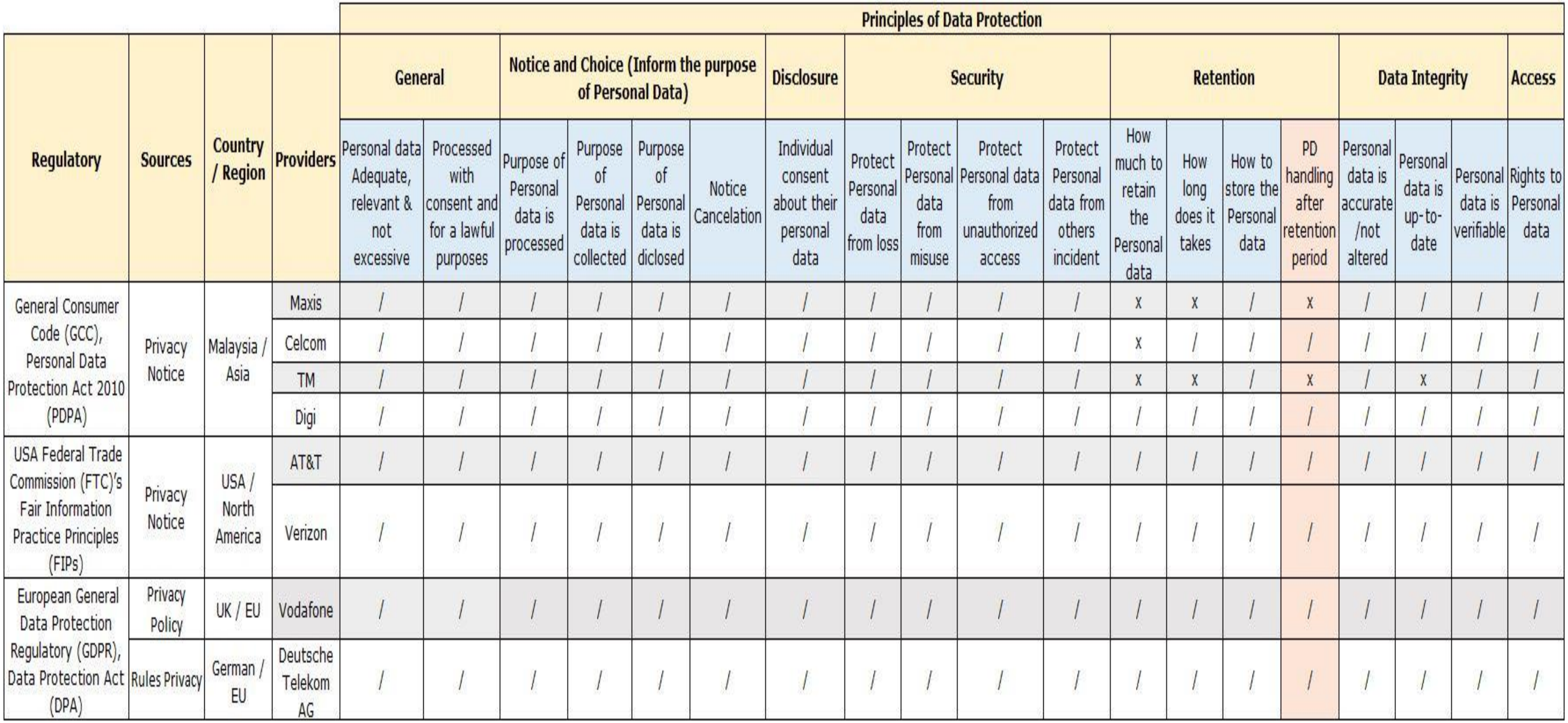
Type	Compliance Requirement	Description
Internal	Data protection impact assessments (DPIA)	A process that is designed to identify and minimise risks associated with the processing of personal data.
	Information Security Readiness Assessment	Assessment mechanism that enables organisations to determine their current cybersecurity capabilities, set individual goals for a target state, and establish a plan for improving and maintaining information security readiness.
	Critical Security (CIS) control	Recommended set of actions for cyber defense that provide specific and actionable ways to stop pervasive and dangerous attacks.
	Cloud Security Alliance (CSA) practices	Best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.
	ISO27001 – Information Security Management	The framework that helps organisations establish, implement, operate, monitor, review, maintain, and continually improve an Information Security Management System.
	ISO 27701- Privacy Information Management System (PIMS)	Procedures and organisational structures that are designed to protect personal data from unauthorised access, processing, or use for purposes other than those originally given as well as to ensure privacy data security.
	Payment Card Industry Data Security Standard (PCI DSS)	Set of security standards designed to ensure that ALL companies that accept, process, store, or transmit credit card information maintain a secure environment.
	Information Security Framework (ISF)	Documented processes that define policies and procedures around the implementation and ongoing management of information security controls.
	IT Audit	IT audit determines whether IT controls protect corporate assets, ensure data integrity, and are aligned with the business' overall goals.
	Security Audit	Security audit measures information system's security against an audit checklist of industry best practices, externally established standards, or federal regulations.
External	Personal Data Protection Act (PDPA)	The act that regulates the processing of personal data in regards to commercial transactions.
	General Data Protection Regulation (GDPR)	The legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

Research Objective 2:
The influence of data subjects' security and privacy concern on big data adoption

Hypotheses	From → To	Path Coefficient			Mediation	Result
		PT	PR	UA		
H1a	COL	-0.119*		0.006	Full	Accepted
H1b	IA	-0.604*		0.068	Full	Accepted
H1c	ERR	0.148*		0.246*	Partial	Accepted
H1d	SU	-0.014		-0.008	No	Rejected
H2a	COL		0.369*	0.006	Full	Accepted
H2b	IA		0.008	0.068	No	Rejected
H2c	ERR		0.201*	0.246*	Partial	Accepted
H2d	SU		0.220*	-0.008	Full	Accepted
H3	SA		0.072	0.024	No	Rejected
H4	PA		0.130*	0.296*	Partial	Accepted
H5	PT		0.018		NA	Rejected
H6	PT			0.136*	NA	Accepted
H7	PR			0.068*	NA	Accepted
Notes: Overall Model F= 48.334; *p<0.05; R^2 = 0.657; adjusted R^2 = 0.66						

DIGITAL SOCIETY RESEARCH GRANT

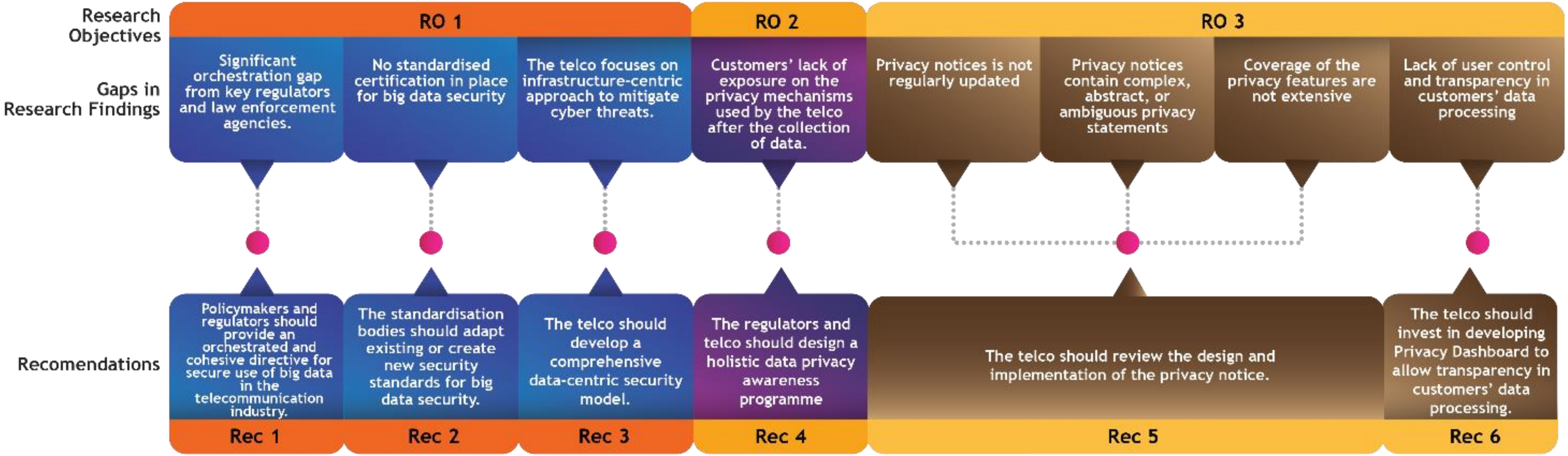
Research Objective 3:
Comparative review of codes of practices



Regulatory	Sources	Country / Region	Providers	Principles of Data Protection																		
				General		Notice and Choice (Inform the purpose of Personal Data)				Disclosure	Security				Retention				Data Integrity			Access
				Personal data Adequate, relevant & not excessive	Processed with consent and for a lawful purposes	Purpose of Personal data is processed	Purpose of Personal data is collected	Purpose of Personal data is diclosed	Notice Cancelation	Individual consent about their personal data	Protect Personal data from loss	Protect Personal data from misuse	Protect Personal data from unauthorized access	Protect Personal data from others incident	How much to retain the Personal data	How long does it takes	How to store the Personal data	PD handling after retention period	Personal data is accurate /not altered	Personal data is up-to-date	Personal data is verifiable	Rights to Personal data
General Consumer Code (GCC), Personal Data Protection Act 2010 (PDPA)	Privacy Notice	Malaysia / Asia	Maxis	/	/	/	/	/	/	/	/	/	/	/	x	x	/	x	/	/	/	/
			Celcom	/	/	/	/	/	/	/	/	/	/	/	x	/	/	/	/	/	/	/
			TM	/	/	/	/	/	/	/	/	/	/	/	x	x	/	x	/	x	/	/
			Digi	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
USA Federal Trade Commission (FTC)'s Fair Information Practice Principles (FIPs)	Privacy Notice	USA / North America	AT&T	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
			Verizon	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
European General Data Protection Regulatory (GDPR), Data Protection Act (DPA)	Privacy Policy	UK / EU	Vodafone	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
	Rules Privacy	German / EU	Deutsche Telekom AG	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/

Recommendations

DSRG
DIGITAL SOCIETY RESEARCH GRANT



Research Objectives	RO 1			RO 2	RO 3			
Gaps in Research Findings	Significant orchestration gap from key regulators and law enforcement agencies.	No standardised certification in place for big data security	The telco focuses on infrastructure-centric approach to mitigate cyber threats.	Customers' lack of exposure on the privacy mechanisms used by the telco after the collection of data.	Privacy notices is not regularly updated	Privacy notices contain complex, abstract, or ambiguous privacy statements	Coverage of the privacy features are not extensive	Lack of user control and transparency in customers' data processing
Recomendations	Policymakers and regulators should provide an orchestrated and cohesive directive for secure use of big data in the telecommunication industry.	The standardisation bodies should adapt existing or create new security standards for big data security.	The telco should develop a comprehensive data-centric security model.	The regulators and telco should design a holistic data privacy awareness programme	The telco should review the design and implementation of the privacy notice.			The telco should invest in developing Privacy Dashboard to allow transparency in customers' data processing.
	Rec 1	Rec 2	Rec 3	Rec 4	Rec 5			Rec 6