

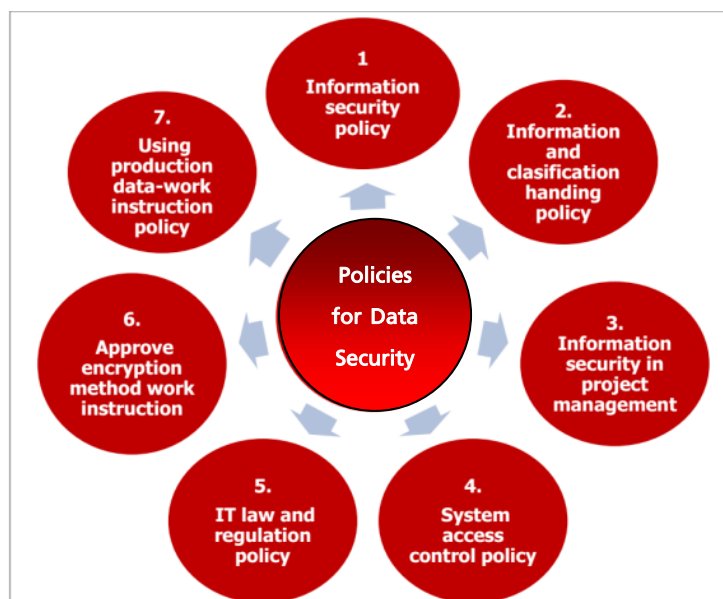
DATA PRIVACY & SECURITY

True has always paid great attention to personal data protection and cybersecurity as we have declared these issues in our corporate agenda. As a telecommunications and digital service provider, we collect large amount of personal customer information. While we see an unprecedented increase in internet data usage as a result of the recent COVID-19 pandemic, a rise in cyber threats and privacy breaches inevitably follows.

We managed both issues in accordance with the Cybersecurity Act B.E. 2562 and Personal Data Protection Act B.E. 2562 of Thailand and other global standards:

1. The CIA Triad encompassing confidentiality, integrity, and availability,
2. ISMS Information Security Management System
3. The US National Institute of Standards and Technology (NIST) Cybersecurity Framework,
4. ISO27001 Information Security Management Standard, and
5. The EU General Data Protection Regulation (GDPR)

POLICIES FOR DATA SECURITY



PERSONAL DATA PROTECTION PROCESS



CUSTOMER REQUEST TO USE, EDIT, DELETE, OR TRANSFER PERSONAL DATA

Customers, as data subjects, have rights to their personal data pursuant to the Personal Data Protection Act B.E. 2562. They can exercise these rights at any True Shop or by contacting our Call Center 1242.



COMPLAINT REPORTING AND HANDLING

True has set in place various channels to receive complaints and suggestions about cybersecurity and personal data protection from customers and stakeholders through email, call center, and True Shop as shown below. When we receive a question or concern from a stakeholder, we will contact the stakeholder within a reasonable time to answer their question or concern.

Any violation of true privacy policy will result in legal action. If True's employees violate the policy, they shall be punished as stated in the Company's Code of conduct and related laws.

PRIVACY POLICY COMPLIANCE AUDIT

The Company assesses and reviews its personal data sharing processes and practices with internal entities and third parties annually, conducted by both internal and external auditors to ensure privacy policy compliance.



Stage 1& 2 Verification

Report for:

True Corporation Public Company Limited

LRQA reference:	BGK61971381476562
Verification dates:	10-26 July 2023
Verification location:	Bangkok, Thailand
Verification criteria:	LRQA's Report Verification
Verification team:	Nit Tanasuthiseri
LRQA Client Facing Office:	LRQA Bangkok

LRQA, its affiliates and subsidiaries, and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'LRQA'. LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

LRQA UK, 71 Fenchurch Street, London, EC3M 4BS, United Kingdom



Contents

01. Executive report3

02. Verification summary4

03. Findings Log.....6

04. Verification schedule 7

Attachments

N/A

This report was presented to and accepted by:

Name: Khun Rachaya Kulnapongse

Job Title: Sustainability, True Corp.



1. Executive report

Verification outcome:

The verification was successfully completed at True Corporation Public Company Limited (referred to hereafter in this report as TRUE).

The verification of status of implementation of Privacy Policy 2022.

LRQA wishes to thank all those involved at TRUE for their preparation and willing participation in the verification process.

The report is the outcome of the verification with detailed finding was documented at each area being visited.

Areas for senior management attention:

Further observations and findings, made during the verification engagement, are

- PDPA framework has been established to drive subsidiary company to comply in full and it is noted that Privacy policy has been introduced to the public via groups' web page.
- High rate of training to employee was succeed in 2022
- Given the number of subsidiary company and resource available it is becoming a concern how and whether the deployment of policy to be cascade down to each subsidiary to ensure the full compliance.
- Lack of data and information upon request at the time of engagement to verify how the relevant function has managed PP for compliance. It is therefore unable to provide the opinion the state of management of compliance.



2. Verification summary

Visit objective

The objective is to review, assess and verify the data and information against the agreed criteria , standard in accordance with Terms of Engagement and to provide the independent verification report

Introduction

LRQA was commissioned by True Corporation Public Company Limited (TRUE) to verify the degree of implementation of Privacy Policy within the group for the year between 1st January and 31st December 2022.

Thank you Khun Rachaya Kulnapongse – Sustainability office performing as our guide and facilitating our work.

Our verification approach was risk-based and undertaken as a sampling exercise of the data and information being provided by TRUE. It covered the following activities:

Reviewing TRUE's process for identifying and determining PDPA framework on how to implement PDPA at TRUE's subsidiary company

Auditing TRUE's data and information to confirm that PDPA has been managed by relevant function We did this by reviewing the PDPA framework, policy procedures, instructions and systems, including those for internal verification. We also spoke with those key people responsible for managing the PDPA

Grading of Findings

The following definitions apply to the grading of findings in this report:

Misstatement (MIS)	A misstatement (omissions, misrepresentations and errors) in an assertion, data or information that, in the professional judgment of the verifier, is unlikely to affect the decision of the intended user. If such a finding is outstanding at the end of the verification, a positive Assurance Statement will be possible, although qualifications, limitations, and/or recommendations may be included in the Assurance Statement.
Material Misstatement (MMIS)	A misstatement, (omissions, misrepresentations and errors) in an assertion, data, or information that, in the professional judgment of the verifier, could affect the decision of the intended user. If such a finding is left outstanding at the end of the verification then the misstatement must be corrected or a positive Assurance Statement will not be possible.
Non-conformity (NCN)	A nonconformity with the requirements of the assurance criteria (including the terms of engagement) that, in the professional judgment of the verifier, is unlikely to affect the decision of the intended user. If such a finding is outstanding at the end of the verification, a positive Assurance



	Statement will be possible, although qualifications, limitations, and/or recommendations may be included in the Assurance Statement.
Material Non-conformity (MNCN)	A nonconformity with the requirements of the assurance criteria (including the terms of engagement) that, in the professional judgment of the verifier, could affect the decision of the intended user. If such a finding is left outstanding at the end of the verification then the nonconformity must be corrected or a positive Assurance Statement with regard to the assurance criteria will not be possible.
Opportunity for Improvement (OFI)	An opportunity for improvement is a suggestion from the verifier to improve the operator's performance in monitoring and reporting.
LRQA	A 'follow up' item for the LRQA Verifier to track ongoing issues within the Findings Log where required.



3. Findings Log

1. Grading of the finding *	2. New, Open, Closed	3. Description of the LRQA finding	4. Review by LRQA	5. Process, aspect, department or theme
6. Date of the finding	7. YYYY<Initials>seq.#	8. Clause of the applicable standard		
* MIS = Misstatement	MMIS = Material Misstatement	NCN = Nonconformity	MNCN = Material Nonconformity	OFI = Opportunity for Improvement
				xLRQA = LRQA Follow Up

Grade 1	Status 2	Finding 3	Correction, root cause & corrective action review 4	Process / aspect 5	Date 6	Reference 7	Clause 8
Not Applicable on this visit							



Verifier: Nit Tanasuthiseri

Verification of:

Terms of Engagement -
Contract Conditions
Confirmation

Auditee(s):

Rachaya Kulnpongse

Audit trails and sources of evidence:

Contract signed dd 5/7/2023
Kick off meeting 10 July 2023

Evaluation and conclusions:

Scope: To conduct the audit how relevant function managed compliance of the Personnel Data Privacy policy 2022 and period of verification would be from 1 Jan-31 Dec 2022

Objectives: To support the DJSI's requirement

Criteria: LRQA's Report Verification Procedure

Materiality: Professional judgement of LRQA verifier

Changes to Terms of Engagement: None

In completing this report, the LRQA verifiers confirm their independence from the client and that there was no known conflict of interest during the engagement.



Verification of:	Strategic Analysis and Risk Analysis (SARA)	Auditee(s):	Rachaya Kulnapongse, Wimonrat Rattanakamut, Kanyanuch Eksook, Suchin Saeng-la-or, Montri Stapornkul
-------------------------	---	--------------------	--

Strategic Analysis:

Through the interview and meeting via IT platform the following data and information the PDPA framework could be summarised :-

The boundary of implementation of PDPA compliance has been designed to apply to the entity where the TRUE has stakeholder more than 50%. In this context, total 45 companies have been identified to meet this criteria.

True Group has set up PDPA Readiness Steering Committee #1/2021 on April 2021 to address the PDPA requirement and plan for the full compliance. The responsibility of committee is to ensure the deployment and implementation of the Privacy Policy and procedure and guidelines.

Personal Data Protection Policy has been established and applied within the group as list of companies could be referred by <https://www.true.th/true-corporation/site/assets/truecorp/pdf/en/true-ar2022-en.pdf> PDPA policy is designed to be top down approach and centralized managed and aim for all subsidiaries to comply in full.

This PDPA would not only apply to employee but also personal data of natural persons such as customers, service users, suppliers, business partners, and other third parties collected by True Corporation Public Company Limited, True Move H Universal Communication Co., Ltd., True Internet Corporation Co., Ltd., True Visions Group Co., Ltd., and True Distribution and Sales Co., Ltd, for example.

According to the abovementioned framework Data Protection Office (DPO) would be appointed to be responsible to implement PDPA policy and cascade down into operation level to each of qualified subsidiaries company.

PDPA has comprise of Processing Personal Data (collect, use, disclose) , Security and Data subject Right. Those three subjects were under responsibility by Data Privacy Center Team.

The following procedure and guidelines has been established as a primary control to implement at business units and subsidiaries

PPD-PC-02 DATA SUBJECT RIGHTS POLICY

PDP-PC-03 DATA BREACH HANDLING POLICY

PPD-PC-01 Data Subject Right Procedure TRUE V3.0

PPD-PC-02 Guideline for Lawful Basis (TH) V1.0

PPD-PC-03 Guideline for Customer Consent Enforcement (TH) V1.0

Regular training and consultation session regarding the PDPA policy and procedures provided from center team are regularly delivered to subsidiaries and staff with a measurement of success.

Monitoring and measurement of compliance is established through the regular testing and review, and audit on a periodical basis.

Through the Strategic Analysis, the Verifier determined the significance of the items of information and data to be verified. This judgement of significance is based on the nature and scale of the information and data as they relate to the scheme requirements.

Verification Planning:

As a result of the completion of the Strategic Analysis and Risk Analysis, a Verification Plan was developed. The Verification Plan defines the key elements of the verification and when those elements will be covered. The Verification Plan is supported by a Data / Information Sampling Plan which defines all the specific items of data and information which the Verification Team has identified as relevant and the depth to which relevant data is to be verified.



Verification of:	Privacy Policy Deployment	Auditee(s):	Rachaya Kulnpongse, Wimonrat Rattanakamut, Kanyanuch Eksook,
Audit trails and sources of evidence: Privacy Notice to Customers: https://www.true.th/true-corporation/site/privacy-policy?ln=en Privacy Notice to Employees: https://hr.truecorp.co.th/service/app/employee-pdpa/ApplicantPrivacy Privacy Notice for Outsourced Parties and Suppliers is the same as the one for Customers: https://www.true.th/true-corporation/site/privacy-policy?ln=en https://www.true.th/true-corporation/site/group-privacy-policy			
Evaluation and conclusions: Privacy Policy was observed to be implemented in public domain and accessible without disruption. However, it was noted as follows <ol style="list-style-type: none">1. Privacy Policy established by True Digital Group is not 100% as TRUE group despite the fact TDG has been incorporated to comply in full with the TRUE Group's policy2. TDG's PP has been last updated on 29/11/2021 whilst TRUE Group's PP has been updated on 30/9/2022.3. Privacy Policy clause 16 addressing the list of TRUE group companies with whom the company may share personal data with, it is worth noting those company as listed in this policy , many of them was not listed as subsidiary whose ownership is more than 50%. It is unclear whether those companies have themselves implemented PDPA on their own. Otherwise, personal data being engaged with TRUE group would be exposed.			

Verification of:	Data Protection Officer (DPO)	Auditee(s):	Rachaya Kulnpongse, Wimonrat Rattanakamut, Kanyanuch Eksook,
Audit trails and sources of evidence: List of appointed DPO. Data Centre Team responsibility			
Evaluation and conclusions: Three DPO have been officially appointed to drive PP into each of subsidiary company. However, it is skeptical on the fact total 45 subsidiary companies to be driven by DPO to enable to establish, implement and maintain privacy policy in full compliance. It is substantiated by the fact that 3 DPO has been officially assigned to set up at approx 8% of all subsidiaries.			



Verification of:	Awareness and Training	Auditee(s):	Rachaya Kulnpongse, Wimonrat Rattanakamut, Kanyanuch Eksook,
Audit trails and sources of evidence: Page 41 – SD report 2022, stating that 12,395 employee was trained on PDPA act.			
Evaluation and conclusions: It was found that only subsidiary company and employee within the group has been trained to raise awareness of PDPA however the contractor and supplier has yet to be made.			

Verification of:	Deployment of Privacy Policy into company level	Auditee(s):	Rachaya Kulnpongse, Wimonrat Rattanakamut, Kanyanuch Eksook,
Audit trails and sources of evidence: Business Unit sample :- Customer service, Network Engineering and Operation, Product Service Group commercial			
Evaluation and conclusions: Based on the framework established and given the 3 samples taken of business unit , the company has been unable to provide data and information for verification whether the procedure and guideline has been deployed into subsidiary company.			

Verification of:	Monitoring and measurement	Auditee(s):	Rachaya Kulnpongse, Wimonrat Rattanakamut, Kanyanuch Eksook,
Audit trails and sources of evidence: Business Unit sample :- Customer service, Network Engineering and Operation, Product Service Group commercial IA report Oct 2022			
Evaluation and conclusions: Based on the framework established, it is a mandatory to have a system audited and assured either from DPO team or corporate team, however, the company has been unable to provide data and information for verification whether the audit has been done to evaluate the compliance. Similar to the reporting of progress of level of implementation was also not evident to be available by sampled business unit. It was noted corporate team has conducted one full audit to regional shop, regional sales and TDS			

Evidence list:
Final-IA-Rpt - Personal data protection_TRUE&TDG(Final - 20221017) Overall_Progress



PDPA Readiness Steering_1st_05APR2021_v02
PDP-PC-01 PERSONAL DATA PROTECTION POLICY
PPD-PC-02 DATA SUBJECT RIGHTS POLICY
PDP-PC-03 DATA BREACH HANDLING POLICY
PPD-PC-01 Data Subject Right Procedure_TRUE V3.0
PPD-PC-02 Guideline for Lawful Basis (TH) V1.0
PPD-PC-03 Guideline for Customer Consent Enforcement (TH) V1.0.
DPC 2022
example DIM

4. Verification schedule

	SARA	Stage 2	TR/AS	Project closing and present recommendation to				
Visit type >								
Due date >								
Start date >	20/7/23	26/7/23						
End date >								
Verifier days >	1	1.5						
Process / aspect								
On-Site								
Stakeholder relevant / material CSR issues								
Strategic Analysis	X							
Risk Analysis	X							
Preparation of Verification Plan	X							
Preparation of Data / Information Sampling Plan	X							
Data / Information Verification		x						
Criteria Conformance Assessment		x						
Review of organisation's inventory assertion, report, etc.								
LRQA Reporting		x						
Preparation of External Verification Report / Assurance Statement, etc.								
Technical Review								