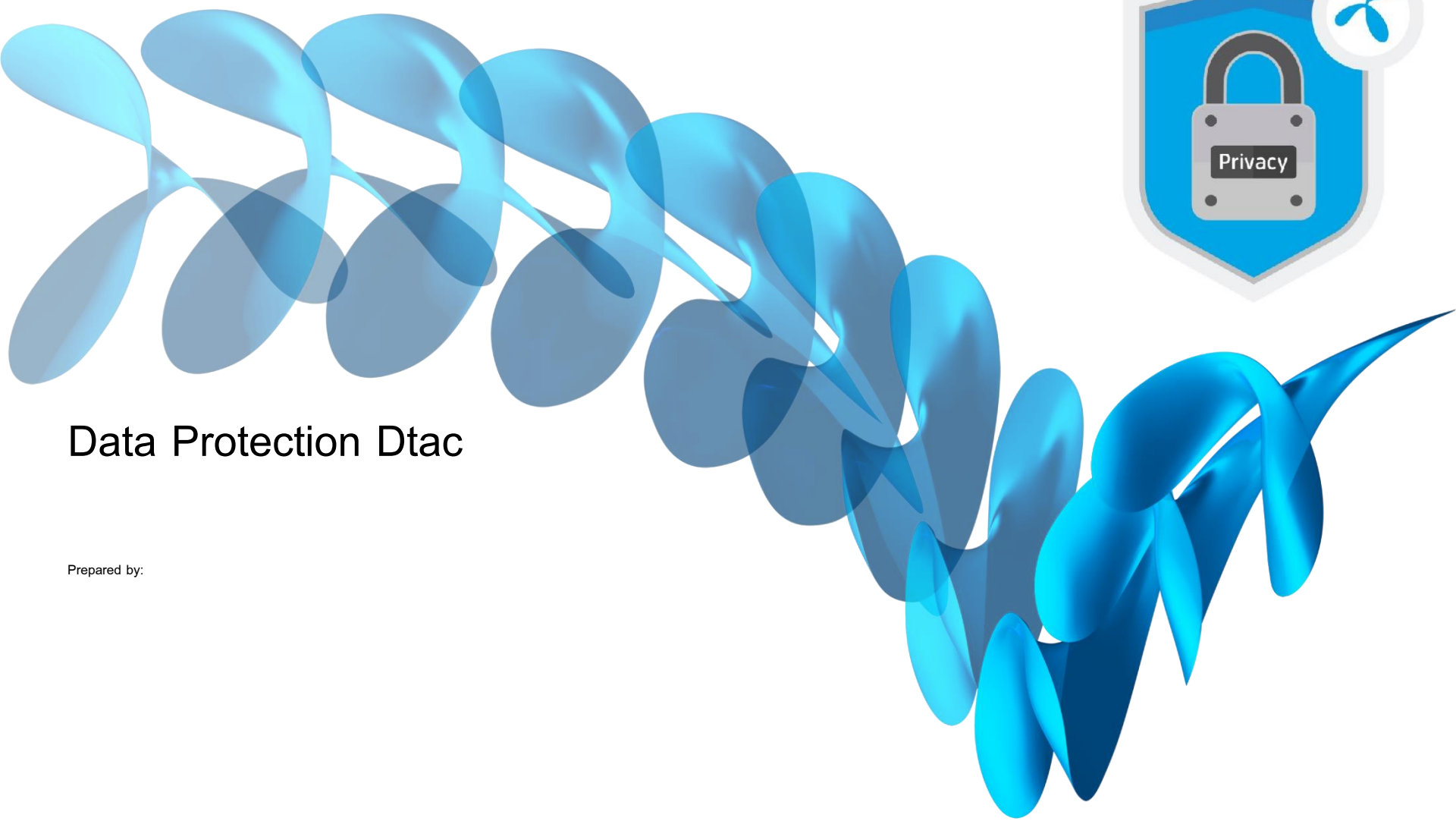


Data Protection Dtac

Prepared by:

Turn what's on paper into actions

(Principles to implementation)

GDPR

NBTC

Corporate policies

Other applicable laws

What's Data Protection?

Cyber Threats

Data Protection

=

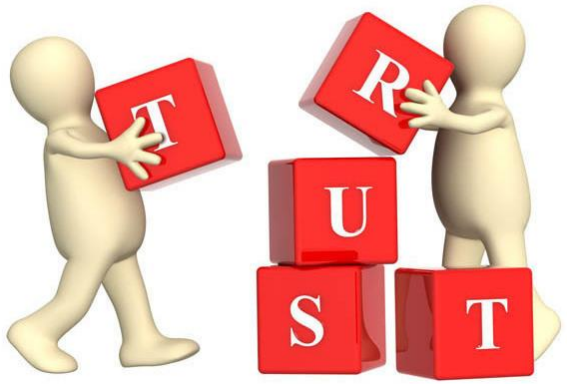
Data Security	+	**Data Privacy**
"Data Accessing (Safeguarding)" • User Access Control • Infrastructure & Network Security • Cyber Security		**"Data Processing"** • Data Transfer • Data Usage Determination • Data Storing • Data Destruction

"Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues may arise in response to information" Reference: Wikipedia on data privacy.

dtac

Our Mission

23 +/- million subscribers



How do we gain trust

Openness

(Data Subject Right)

Consents

Data Protection

Privacy by Design (DPIA, DPA, DPO, Awareness)

Data Accessing

Data Processing

Process Controls

Controls Set

- Reconciliation
- SOD

Technology

Operations

Self assessment

Retention

As Necessary/Governed by law

Breach Handling

Detection/Contain/

Evaluate/Notification/

Preventive actions

Governed by: NBTC Data Protection Act 2549 and other applicable laws, GDPR, Corporate Policies

dtac

Samples

D. ข้อกำหนดสำหรับความเป็นส่วนตัวตั้งแต่การออกแบบ (สำหรับทีมโครงการเพื่อเพิ่มเข้าไปในข้อกำหนดพื้นฐานด้านล่าง)		
ดิชนี	ถ้อยแถลงข้อกำหนด	เกณฑ์
D-1	**การบริหารจัดการความยินยอมทั่วไป**	
D-1-1	ระบบจะต้องมีกล่องทำเครื่องหมายถูกสำรับการยอมรับข้อตกลงและเงื่อนไข (T&C) ของผลิตภัณฑ์ของลูกค้า	**Mandatory**
D-1-2	ระบบจะต้องสามารถบันทึกและดึงข้อมูลความยินยอมทั้งหมดเพื่ออ้างอิงและตรวจสอบในอนาคตได้ทั้งหมด กล่าวคือ การบันทึกเวลาสำหรับบัญชีผู้ใช้งานที่มีการใช้งานอยู่ในปัจจุบัน	**Mandatory**
D-1-3	ระบบไม่ควรเข้าถึงหรือเก็บภาพตำแหน่งสถานที่ของเจ้าของข้อมูลไว้นอกจากจะเป็นผลิตภัณฑ์/แอพพลิเคชันที่ต้องใช้ตำแหน่งสถานที่	**Mandatory**
D-1-4	ระบบจะต้องรองรับการร้องขอของเจ้าของข้อมูลเพื่อลบหรือบล็อกข้อมูลส่วนบุคคลไม่ให้มีการประมวลผลในอนาคตโดยผู้ใช้งานข้อมูล (มูลฐานทางกฎหมายที่ถูกต้องสำหรับการใช้ข้อมูลไม่มีผลบังคับใช้อีกต่อไป)	**Mandatory**
D-2	**การประกาศและการบริหารจัดการตัวเลือก**	
D-2-1	ฝ่ายบริการลูกค้า/ระบบรับมือลูกค้าต้องเก็บภาพหลังจากไปยังข้อตกลงและเงื่อนไขของผลิตภัณฑ์ ถ้อยแถลงเกี่ยวกับความเป็นส่วนตัว และหน้าที่ในการคุ้มครองข้อมูล และทำให้สามารถเข้าถึงบนหน้าแลนดิงของเว็บไซต์ได้	**Mandatory**
D-2-2	ระบบควรรองรับการจัดการกับความยินยอมของผู้ใช้งาน/เจ้าของข้อมูลและความสามารถในการเชื่อมต่อกับระบบ opt-in/opt-out ภายนอกได้	**Mandatory**
D-3	**การบริหารจัดการความปลอดภัยของข้อมูล**	
D-3-1	ระบบจะต้องปฏิบัติตามและจัดทำข้อมูลอ้างอิงถึงข้อกำหนดด้านความปลอดภัยของข้อมูลในด้านต่าง ๆ ที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและเกี่ยวข้องกับการนิยามการบรรลุและการรักษาความลับ ความพร้อม ความถูกต้อง และความน่าเชื่อถือของข้อมูลหรือสถานที่ประมวลผลข้อมูล	บังคับ
D-3-2	ระบบจะต้องรับรองว่าในการรับส่งทางอิเล็กทรอนิก หรือระหว่างการขนส่งหรือการบันทึกผู้ขนส่งข้อมูล ข้อมูลส่วนตัวไม่สามารถอ่าน คัดลอก ดัดแปลง หรือลบโดยผู้ที่ไม่ได้รับอนุญาตได้ และต้องสามารถตรวจสอบและกำหนดว่าจะต้องส่งข้อมูลส่วนบุคคลไปที่ไหนโดยอุปกรณ์รับส่งข้อมูล (การควบคุมการรับส่งข้อมูล)	บังคับ
D-4	**การบริหารจัดการความสมบูรณ์ของข้อมูล**	
D-4-1	ระบบจะต้องรับรองว่าข้อมูลส่วนบุคคลที่รวบรวมไว้ถูกต้อง สมบูรณ์ ไม่ทำให้เข้าใจผิด และได้รับการปรับปรุงล่าสุดเสมอ ตรวจสอบตัวตนของเจ้าของข้อมูลในกรณีที่สามารถกระทำได้โดยใช้วิธีการตรวจสอบตัวตนที่เหมาะสมกับความเสี่ยง สามารถดำเนินการได้โดยการทดสอบเชิงตรรกะหรือการจัดทำพจนานุกรม: 1) เพื่อหลีกเลี่ยงข้อมูลหลอกและตัวเลขสำหรับชื่อของลูกค้า 2) เพื่อรับรองว่าหมายเลขประจำตัวมี 13 หลัก และไม่มีตัวอักษรผสมอยู่	บังคับ
D-5	**การบริหารจัดการการเข้าถึงข้อมูล**	
D-5-1	ฝ่ายบริการลูกค้า/ระบบรับมือลูกค้าจะต้องรองรับและทำให้เจ้าของข้อมูลสามารถเข้าถึงข้อมูลส่วนบุคคลของตนที่ผู้ใช้งานข้อมูลถืออยู่ได้	บังคับ
D-5-2	ระบบจะต้องรองรับการร้องขอของเจ้าของข้อมูลเพื่อแก้ไขข้อมูลส่วนบุคคลหากข้อมูลไม่สมบูรณ์หรือไม่ถูกต้อง (สิทธิในการแก้ไขข้อมูล)	บังคับ
D-5-3	ระบบจะต้องสร้างข้อมูลประวัติการแก้ไข/บันทึกเวลาโดยอัตโนมัติสำหรับการเข้าถึง การแก้ไขหรือการลบข้อมูลของผู้ใช้งาน	บังคับ
D-6	**การบริหารจัดการปัญหาและการดำเนินการ**	
D-6-1	ระบบจะต้องสามารถรองรับการเข้ารหัส/การไม่ระบุชื่อ/การลบข้อมูลระบุตัวตนออกของข้อมูลส่วนบุคคลเมื่อโอนข้อมูลส่วนบุคคลนอกประเทศไทยที่เป็นข้อมูลที่มีข้อมูล CRM (ส่วนบุคคล) / เพื่อการจัดเก็บข้อมูลส่วนบุคคลหลังจากการบรรลุจุดประสงค์ของการรวบรวมและระยะเวลาจัดเก็บที่จำเป็นของระบบและอื่น ๆ	บังคับ
D-7	**การบริหารจัดการการจัดเก็บข้อมูล**	
D-7-1	ระบบจะต้องรองรับการจัดเก็บข้อมูลส่วนบุคคลที่หมดประสิทธิภาพแล้วเป็นระยะเวลาที่ระบุโดยข้อบังคับ	บังคับ
D-7-2	ระบบควรสามารถสถานะต่อไปนี้ได้โดยอัตโนมัติ: 1)สถานะ "จัดเก็บน้อยเกินไป" ทันทีหลังจากลูกค้าบอกเลิกการเป็นสมาชิก (หมดประสิทธิภาพ (EOE)) 2) สถานะ "จัดเก็บนานเกินไป" หลังจากการกำกับดูแลการจัดเก็บโดยมีสัญญาณกระตุ้น และสามารถดึงรายงานตามระยะเวลาไปยังเจ้าของข้อมูลได้ ไม่สามารถลบแบบอัตโนมัติได้ยกเว้นจะได้รับการอนุมัติจากเจ้าของข้อมูล	ไม่บังคับ
D-7-3	ระบบจะต้องรองรับการเข้ารหัสข้อมูลของผู้ใช้งานโดยไม่ระบุชื่อระหว่างที่อยู่ในระยะเวลาการจัดเก็บ	บังคับ
D-8	**การบริหารจัดการการทำลายข้อมูล**	
D-8-1	ระบบจะต้องรองรับการลบข้อมูลในลักษณะที่เหมาะสมกับเนื้อหาของข้อมูลทันทีที่จุดประสงค์เดิมไม่มีผลอีกต่อไป หรือเมื่อไม่มีจุดประสงค์ทางธุรกิจที่จะต้องเก็บข้อมูล	บังคับ
D-9	**การแชร์/การโอนข้อมูล**	
D-9-1	การแชร์/การโอนข้อมูลส่วนบุคคลเป็นไปตามจุดประสงค์ทางธุรกิจที่ถูกต้องตามกฎหมาย	บังคับ
D-9-2	ผู้ประมวลผลข้อมูลจะต้องได้รับการสอบทานธุรกิจก่อนทำสัญญาตามกระบวนการเลือกผู้ขายของดีแทคเพื่อรับรองว่าข้อมูลส่วนบุคคลได้รับการบริหารจัดการอย่างปลอดภัย	บังคับ
D-9-3	ประเทศที่ข้อมูลส่วนบุคคลจะต้องถูกโอนให้การคุ้มครองข้อมูลในระดับที่เพียงพอ	บังคับ
D-9-4	สัญญาการประมวลผลข้อมูลจะมีผลกับผู้ประมวลผลข้อมูลตามเจตนารมณ์ของสัญญาก่อนการแชร์/การโอนข้อมูลส่วนบุคคล	บังคับ
D-9-5	เฉพาะข้อมูลขั้นต่ำที่จำเป็นเพื่อบรรลุวัตถุประสงค์เท่านั้นที่จะถูกแชร์/โอน	บังคับ
D-9-6	ข้อมูลส่วนบุคคลที่ถูกแชร์/โอนไปยังบุคคลหรือกลุ่มบุคคลต้องเป็นไปตามความจำเป็นที่ต้องรู้ข้อมูลเท่านั้น	บังคับ

Data Processing Agreement (DPA)

- Purpose of Processing
- Location of Processing
- Obligations to Subcontractors
- Right to Audit
- Data destruction

Data Privacy Impact Assessment

- Information Security Framework
- Data processing risk identification and mitigation

Privacy Awareness to

- Technology (In house & Vendors)
- Operation (In house & Vendors)
- Staffs in General

dtac

Potential Impact from Privacy Failure

- Loss of Trust
- Brand Name (Reputation)
- Loss of revenue and new business
- Litigation from consumers, privacy advocates, business partners

ดีแทคคุ้มครองข้อมูลลูกค้าอย่างไร?