

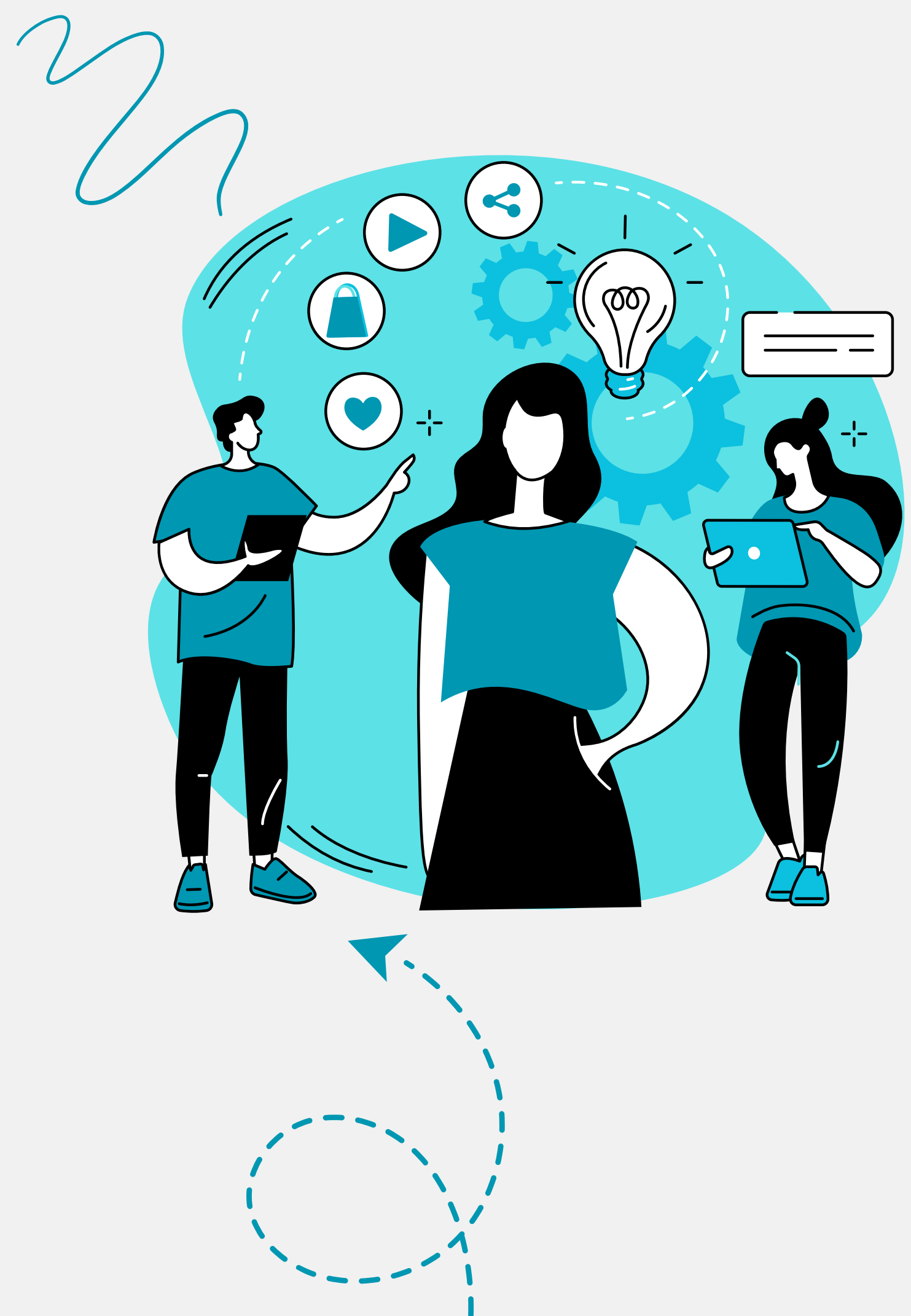


PERSONAL DATA PROTECTION ACT

ดร.กิตติ์ เรียร์โนปจัย
ผู้ช่วยอธิการบดีฝ่ายดิจิทัล
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
มหาวิทยาลัยขอนแก่น

กฎหมายเกี่ยวกับระบบสารสนเทศ ในประเทศไทย

- ลิขสิทธิ์
- ธุรกรรมทางอิเล็กทรอนิกส์
- การกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- ความมั่นคงปลอดภัยไซเบอร์
- คุ้มครองข้อมูลส่วนบุคคล



EU GDPR

AMAZON/ADS ~ €746M

WHATSAPP/TRANSPARENCY ~ €225M

GOOGLE/ADS ~ €50M

INSTAGRAM/CHILD'S PII ~ €405M

FACEBOOK/LEAK ~ €265M

...



แต่ .. เกี่ยวอะไรกับ
เรา?

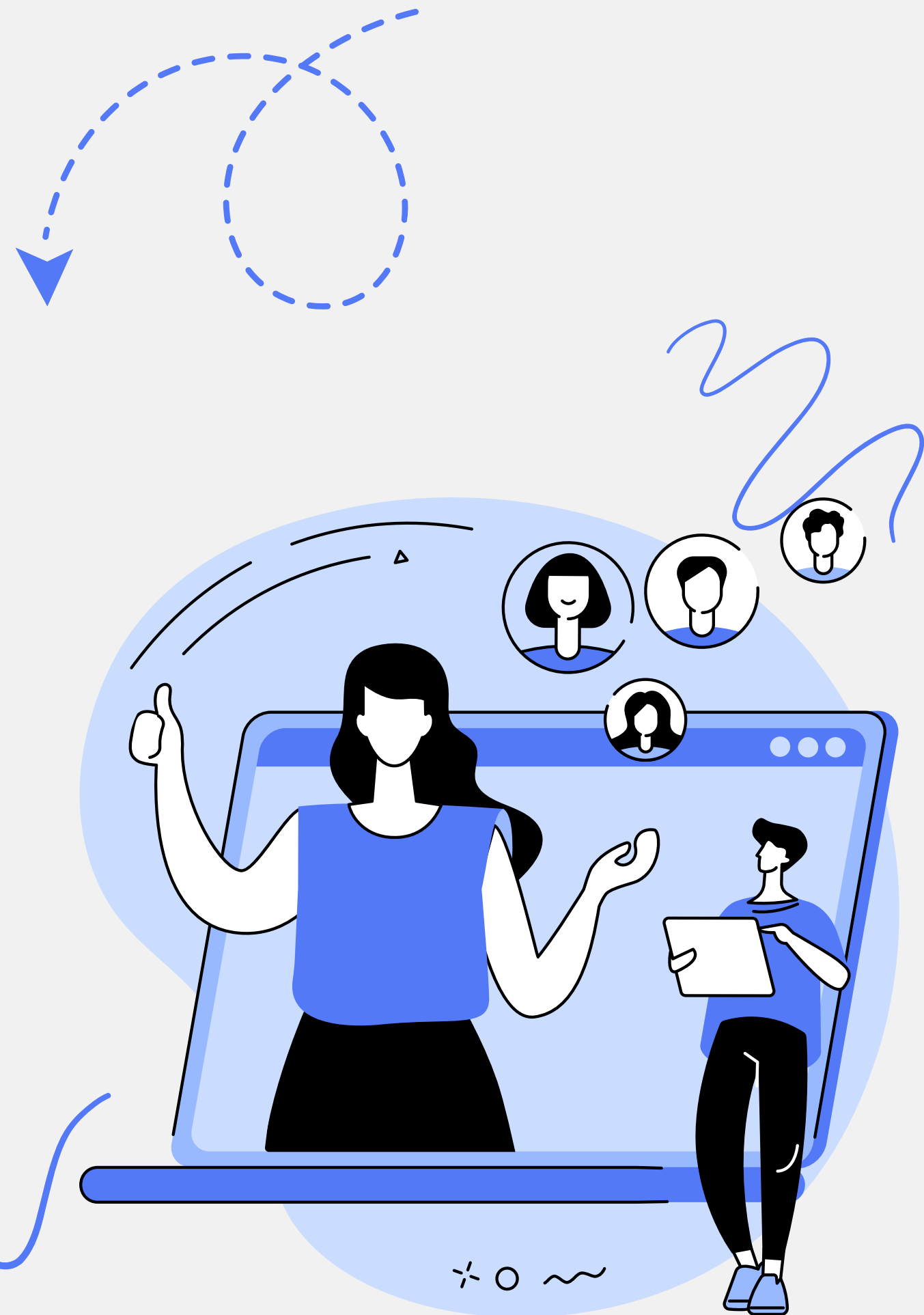




<https://kku.digital/pwned>

WHY PDPA

- ปกป้องสิทธิขั้นพื้นฐาน
- ป้องกันการใช้ข้อมูลส่วนตัวในทางที่ผิด
- ป้องกันการจัดการข้อมูลส่วนตัวผิด
- มีมาตรฐาน/แนวปฏิบัติที่เหมาะสม
- รับมือกับภัยคุกคามต่อข้อมูลได้ถูกต้อง
- ความเชื่อมั่นในระบบเศรษฐกิจดิจิทัล
- สอดคล้อง/เทียบเท่าสากล



NOT APPLY TO

- ประโยชน์ส่วนตัวหรือครอบครัว
- การรักษาความมั่นคงของรัฐ
- สื่อมวลชน ตามจริยธรรมวิชาชีพ
- สภาผู้แทนฯ วุฒิสภา รัฐสภา กรรมการการฯ
- กระบวนการยุติธรรม
- ข้อมูลเครดิต
- ...
- **แต่** ต้องมีการรักษาความมั่นคงปลอดภัยฯ



UNDERSTAND

PERSONAL IDENTIFIABLE INFORMATION

สามารถระบุตัวบุคคลนั้นได้
ไม่ว่าทางตรงหรือทางอ้อม
ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม



UNDERSTAND

SENSITIVE PERSONAL INFORMATION

เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง
ความเชื่อในลัทธิศาสนาหรือปรัชญา
พฤติกรรมทางเพศ ประวัติอาชญากรรม
ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน
ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรืออื่นใดในทำนองเดียวกัน



PERSONAL DATA

PROCESSING



ยินยอม



ปฏิบัติตาม



DATA SUBJECT
เจ้าของข้อมูลส่วนบุคคล

DATA CONTROLLER
อำนาจหน้าที่ตัดสินใจเก็บ
รวบรวม ใช้ เปิดเผย

DATA PROCESSOR
ดำเนินการตามคำสั่งหรือ
ในนามผู้ควบคุมฯ

DATA SUBJECT

RIGHTS

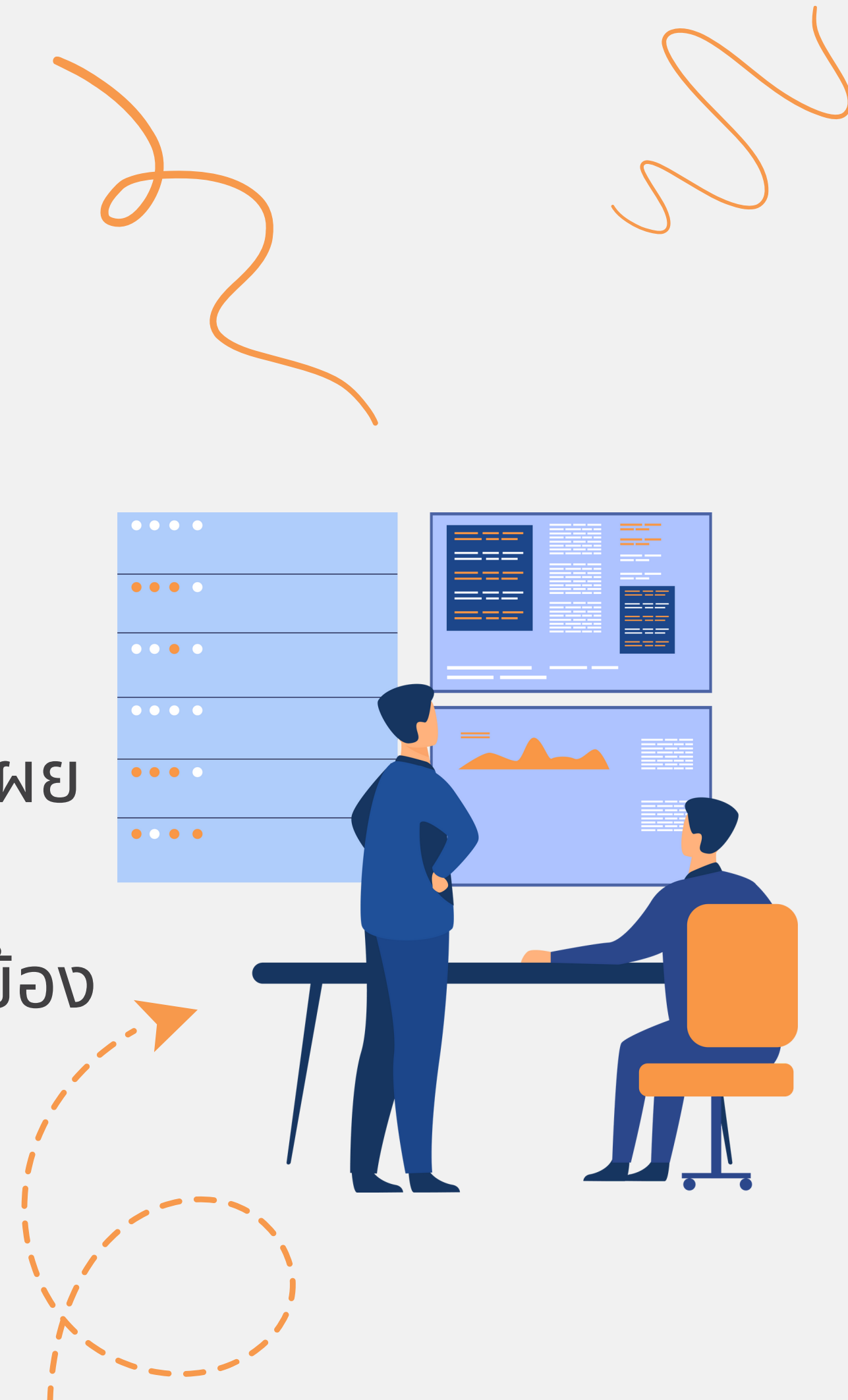
- ขอเข้าถึงและรับสำเนา
- ขอให้เปิดเผยการได้มาโดยไม่ได้รับความยินยอม
- คัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผย
- ขอให้ลบ หรือทำลาย
- ขอระงับการใช้
- ขอให้ปรับปรุงข้อมูล



DUTY OF DATA

CONTROLLER

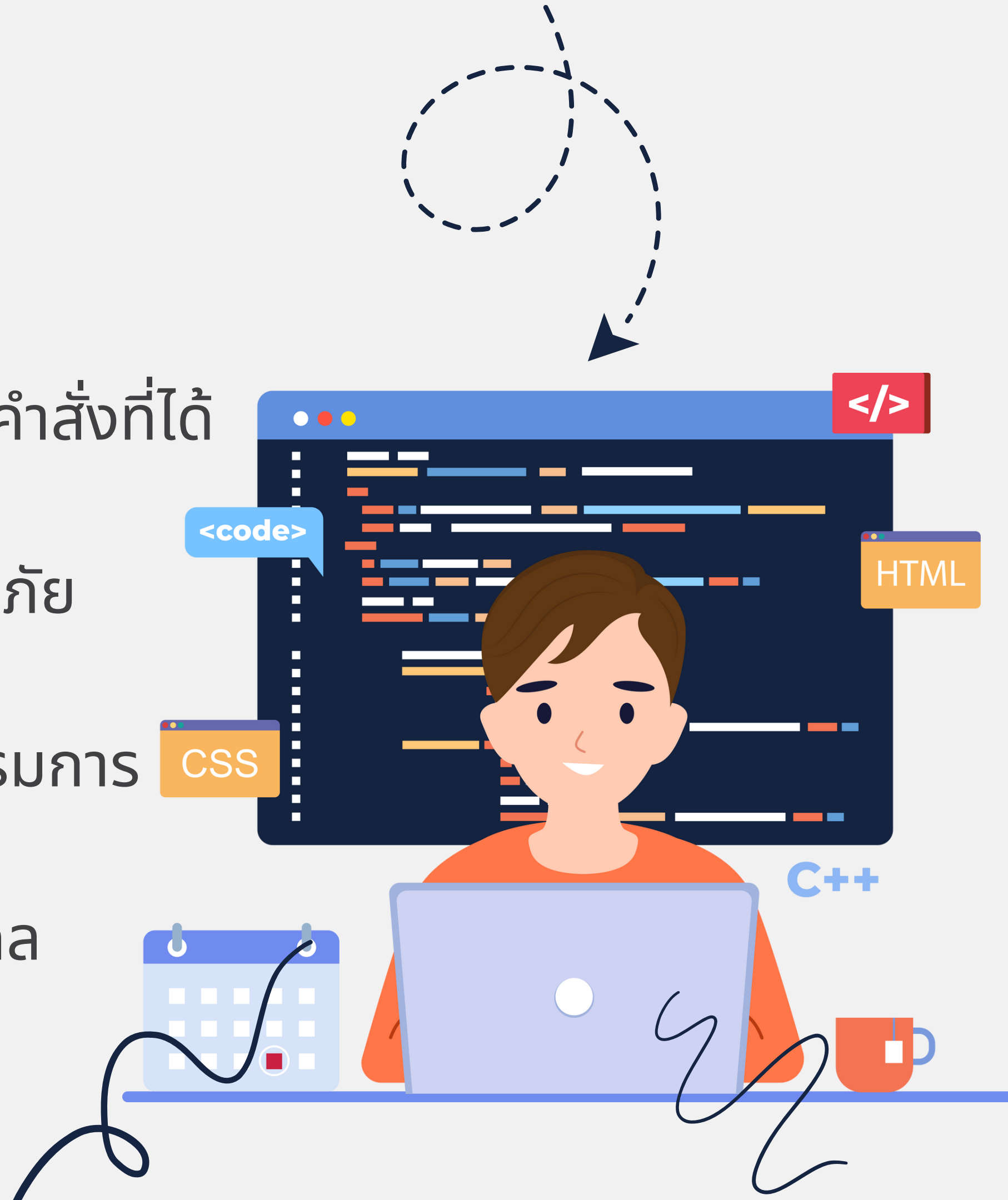
- แจ้งวัตถุประสงค์การเก็บรวบรวม ใช้ เปิดเผย
- ขอความยินยอม
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผย
- จัดทำ ROPA
- ลบหรือทำลายเมื่อพ้นกำหนดการเก็บรักษา ไม่เกี่ยวข้องเกินจำเป็น หรือได้รับการร้องขอ
- แจ้งเหตุการณ์ละเมิดแก่สำนักงานโดยไม่ชักช้า
- จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)



DUTY OF DATA

PROCESSOR

- ดำเนินการเก็บรวบรวม ใช้ เผยแพร่ ตามคำสั่งที่ได้
รับจากผู้ควบคุมฯ
- จัดให้มีมาตรการรักษาความมั่นคงปลอดภัย
- แจ้งเหตุละเมิดให้ผู้ควบคุมฯ ทราบ
- จัดทำและเก็บรักษาบันทึกการกิจกรรมการ
ประมวลผล
- จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



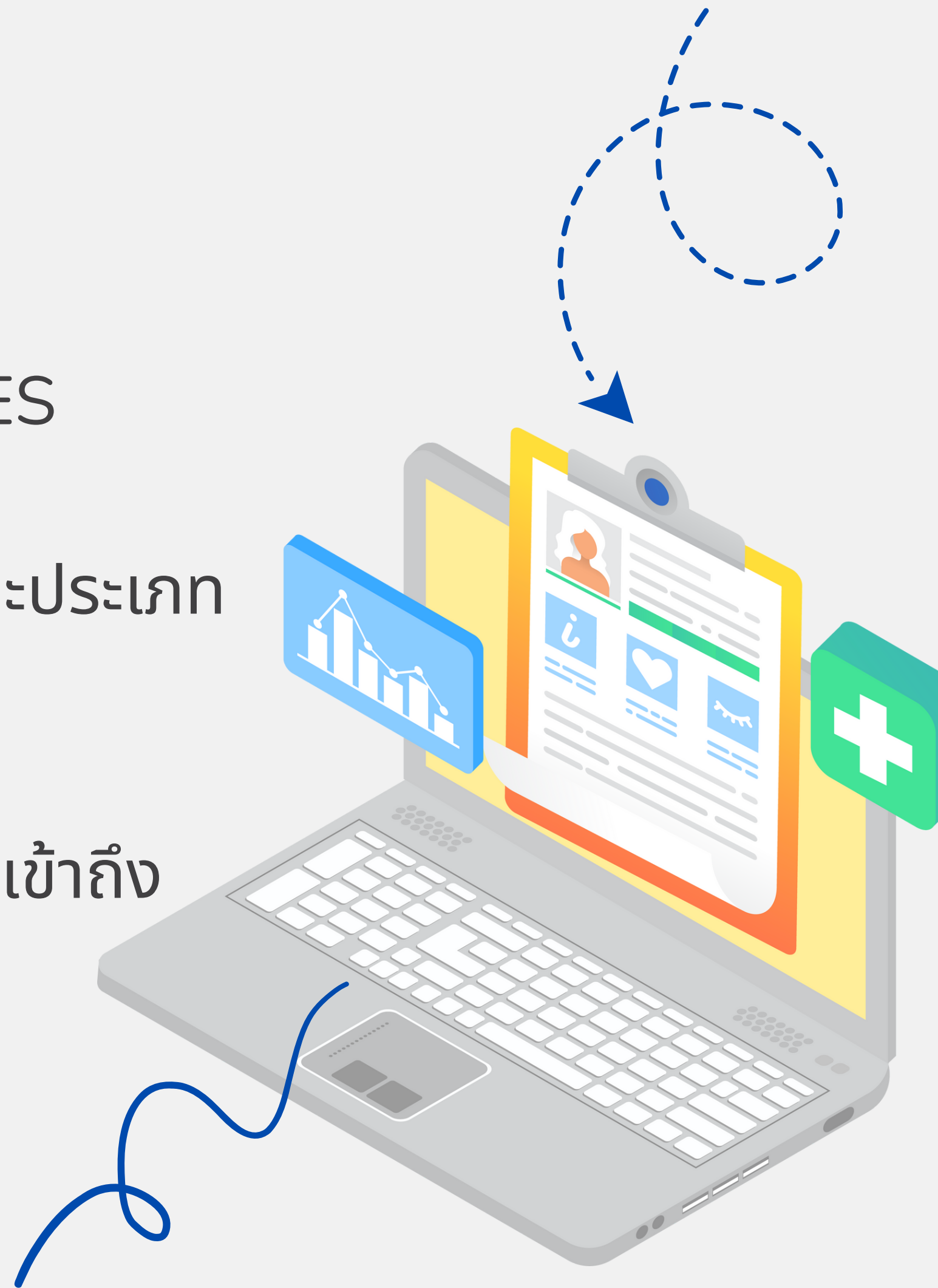
DUTY OF DPO

- ให้คำแนะนำเกี่ยวกับการปฏิบัติตาม พรบ.
- ตรวจสอบการดำเนินงานเพื่อให้เป็นไปตาม พรบ.
- ประสานความร่วมมือกับสำนักงานกรณีมีปัญหา
- รักษาความลับที่ตนล่วงรู้



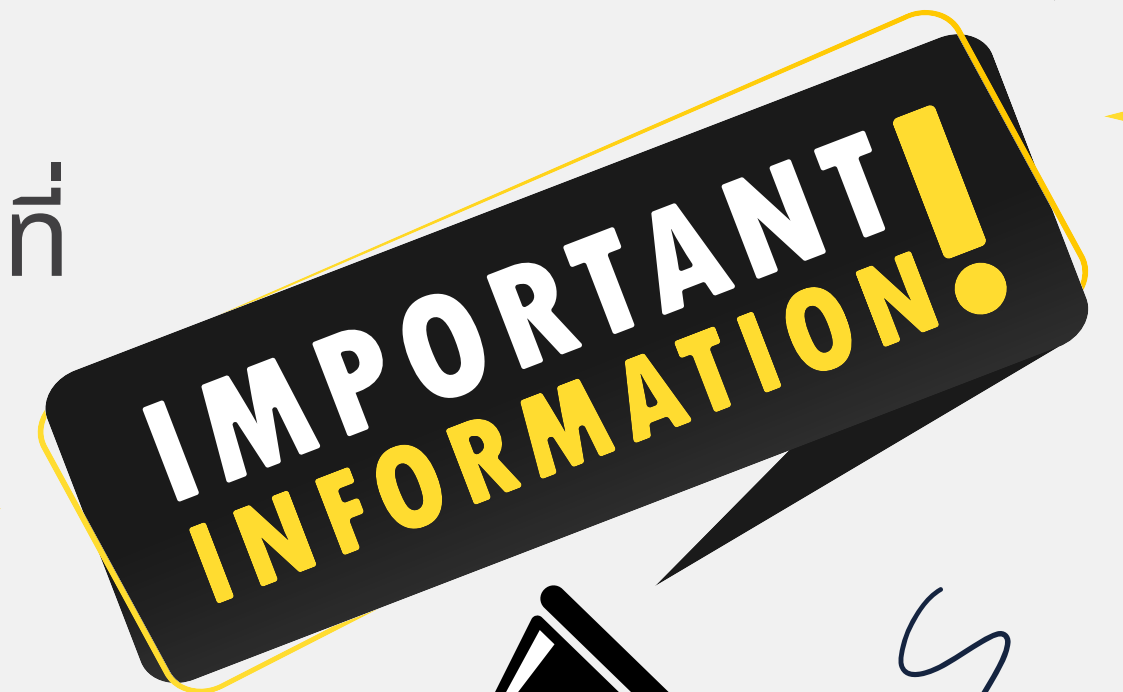
ROPA

- RECORDS OF PROCESSING ACTIVITIES
- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม
- วัตถุประสงค์ของการเก็บรวบรวมข้อมูลฯ แต่ละประเภท
- ข้อมูลเกี่ยวกับผู้ควบคุมฯ
- ระยะเวลาในการเก็บรักษาข้อมูลฯ
- สิทธิและวิธีการเข้าถึงของบุคคลที่มีสิทธิในการเข้าถึง
- การใช้หรือเปิดเผย
- การปฏิเสธคำขอ คัดค้าน
- คำอธิบายมาตรการรักษาความมั่นคงปลอดภัย



PRIVACY NOTICE

- แจ้งวัตถุประสงค์การเก็บรวบรวมเพื่อนำไปใช้หรือเปิดเผย
- แจ้งกรณีที่เจ้าของข้อมูลต้องให้เพื่อปฏิบัติตามกฎหมาย และผลกระทบที่เป็นไปได้หากไม่ให้ข้อมูล
- ระยะเวลาการเก็บรวบรวม
- ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย
- ข้อมูลเกี่ยวกับผู้ควบคุม สถานที่ วิธีติดต่อ DPO
- สิทธิของเจ้าของข้อมูล



CONSENT

- ผู้ควบคุมฯ ต้องได้รับความยินยอมจากเจ้าของข้อมูลฯ PII
- ผู้ควบคุมฯ ต้องได้รับความยินยอมจากเจ้าของข้อมูลฯ SPI โดยชัดเจน
 - แยกส่วนจาก PII
 - รายละเอียดจำเพาะเจาะจง
 - รูปแบบจำเพาะเจาะจง
- เจ้าของข้อมูลฯ ถอนความยินยอมได้
- เว้นแต่ ...



EXCEPTIONS

PERSONAL IDENTIFIABLE INFORMATION

- ประวัติศาสตร์ จดหมายเหตุ
- ป้องกัน/ระงับอันตรายต่อชีวิต ร่างกาย สุขภาพ
- จำเป็นเพื่อปฏิบัติตามสัญญา
- จำเป็นในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมฯ
- จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมฯ เว้นแต่ความสำคัญน้อยกว่าสิทธิขั้นพื้นฐาน
- ปฏิบัติตามกฎหมายของผู้ควบคุม



EXCEPTIONS

SENSITIVE PERSONAL INFORMATION

- ป้องกัน ระวังอันตรายต่อชีวิต ร่างกาย สุขภาพ ซึ่งเจ้าของข้อมูลฯ ไม่สามารถให้ความยินยอมได้
- กิจกรรมโดยชอบด้วยกฎหมายของมูลนิธิ สมาคม NGO ที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา ฯ
- เปิดเผยต่อสาธารณะโดยได้รับความยินยอมโดยชัดแจ้ง
- จำเป็นต่อสิทธิเรียกร้องตามกฎหมาย

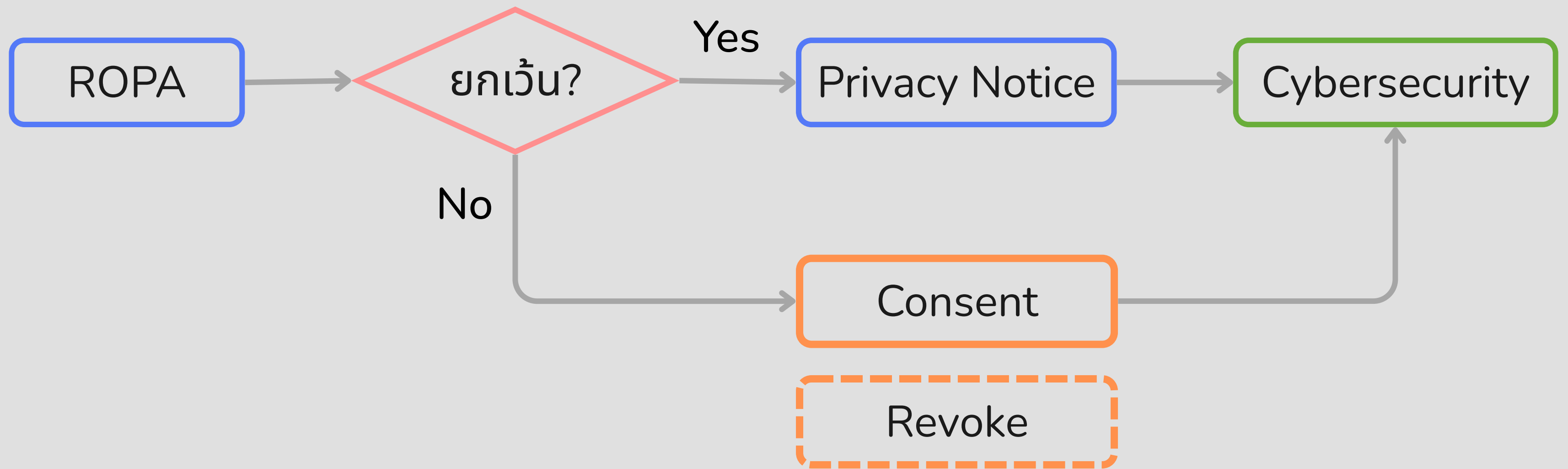


EXCEPTIONS

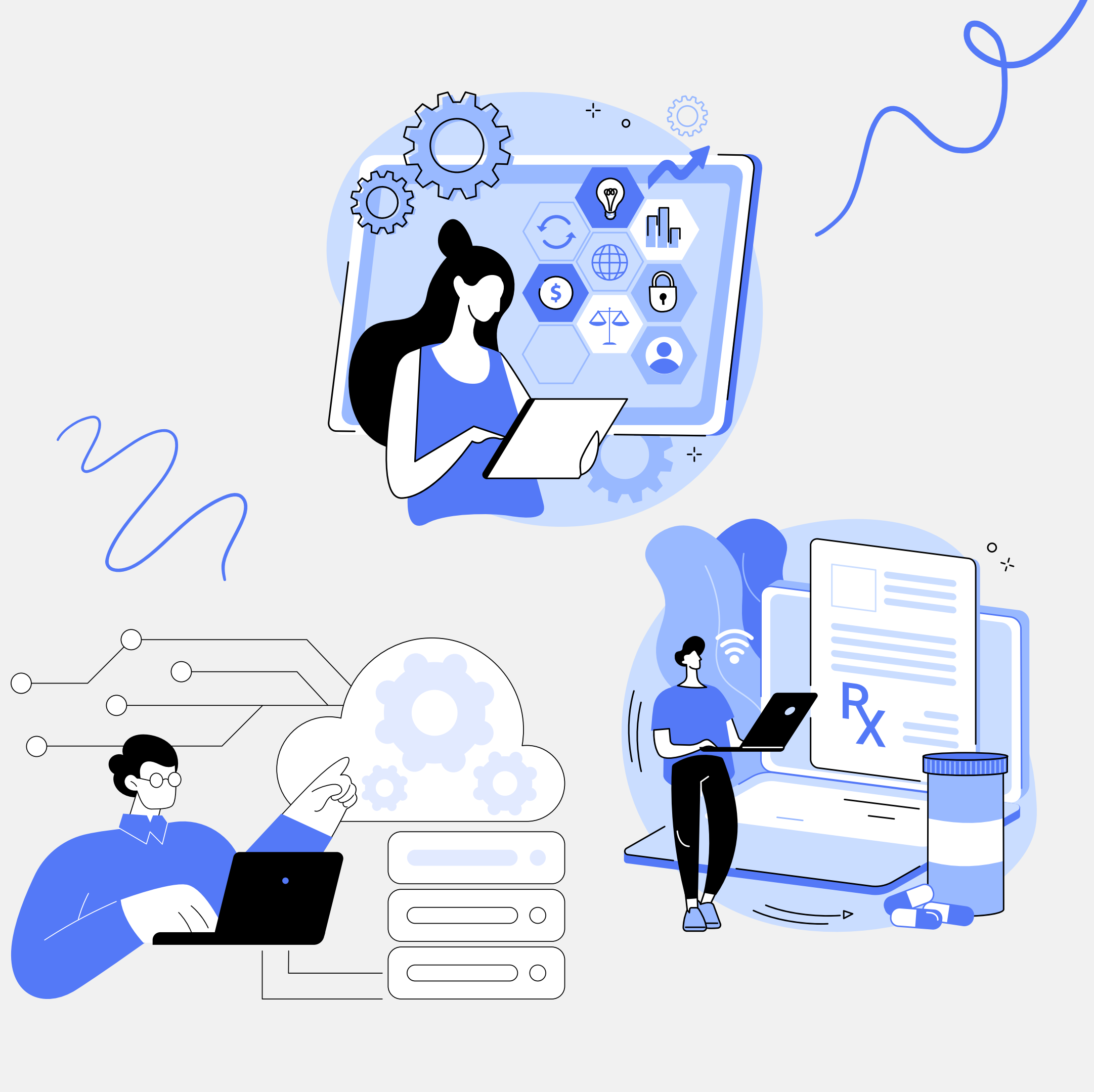
SENSITIVE PERSONAL INFORMATION

- ปฏิบัติตามกฎหมายเพื่อวัตถุประสงค์ประสงค์เกี่ยวกับ
 - เวชศาสตร์ป้องกัน วินิจฉัยโรค บริการสุขภาพ การรักษาทางการแพทย์ สังคมสงเคราะห์ ฯ
 - ประโยชน์ด้านการสาธารณสุข ฯ
 - การคุ้มครองแรงงาน ประกันสังคมสวัสดิการ รักษาพยาบาล ฯ
 - วิจัยทางการแพทย์ ประวัติศาสตร์ สลิตี ฯ
 - ประโยชน์สาธารณะที่สำคัญ ฯ





CYBER SECURITY MEASURES





ป้องกันการเข้าถึง

HARDWARE

COMPUTER

MOBILE PHONE

NETWORK

FIREWALL

IOT DEVICES

LAB PCS

SHARED PCS/DEVICES



PHYSICAL SECURITY

DATA CENTER DESIGN
DISASTER RECOVERY SITE
PHYSICAL ACCESS CONTROL
USER-DEVICE ACCESS CONTROL
BRING-YOUR-OWN-DEVICE



ตรวจสอบ-แก้ไข

VULNERABILITIES

อย่างสม่ำเสมอ

NETWORK SCAN

WEB APPLICATION SCAN

ENDPOINT SCAN

CLOUD SCAN

ZERO TRUST

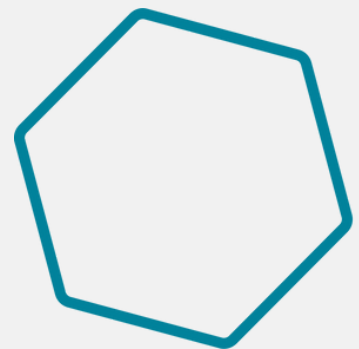
SECURE CODING





OpenVAS

Open Vulnerability Assessment Scanner



nessus[®]

Professional



Burp Suite



OWASP

Zed Attack Proxy

Flawfinder

Valgrind



อัปเดต

SOFTWARE

อย่างสม่ำเสมอ

OPERATING SYSTEMS
APPLICATIONS
BROWSERS
ANTI-MALWARE
ANTI-SCAM/FRAUD
VULN. SCANNERS

Google Workspace

 Microsoft 365

foxit



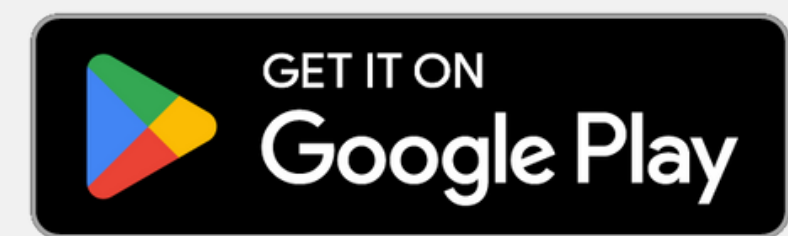
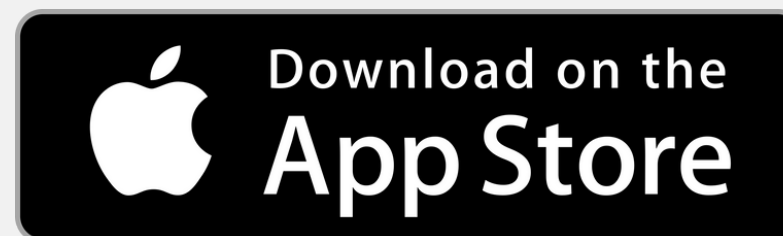
 Windows

 zoom

STATA

Canva

KASPERSKY 



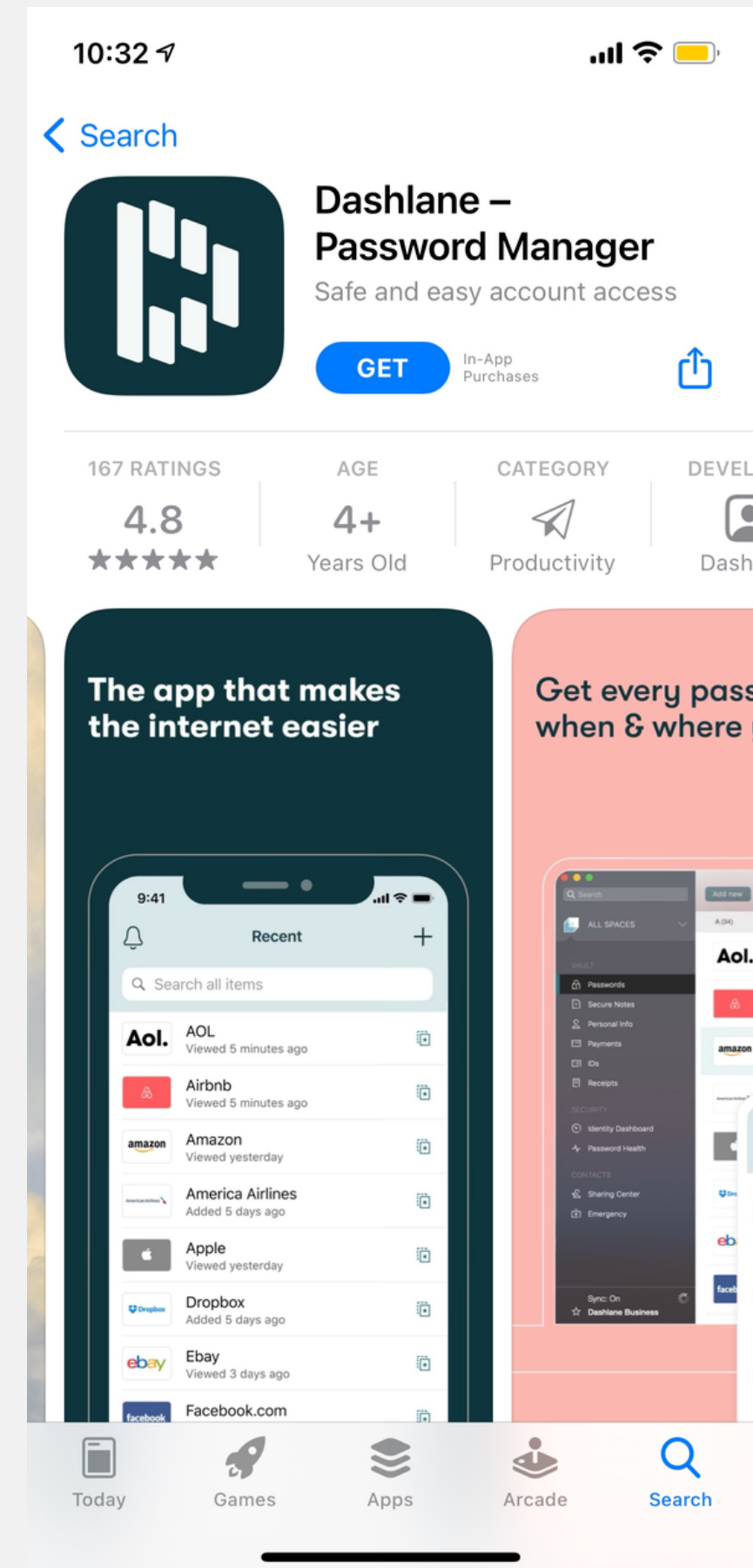
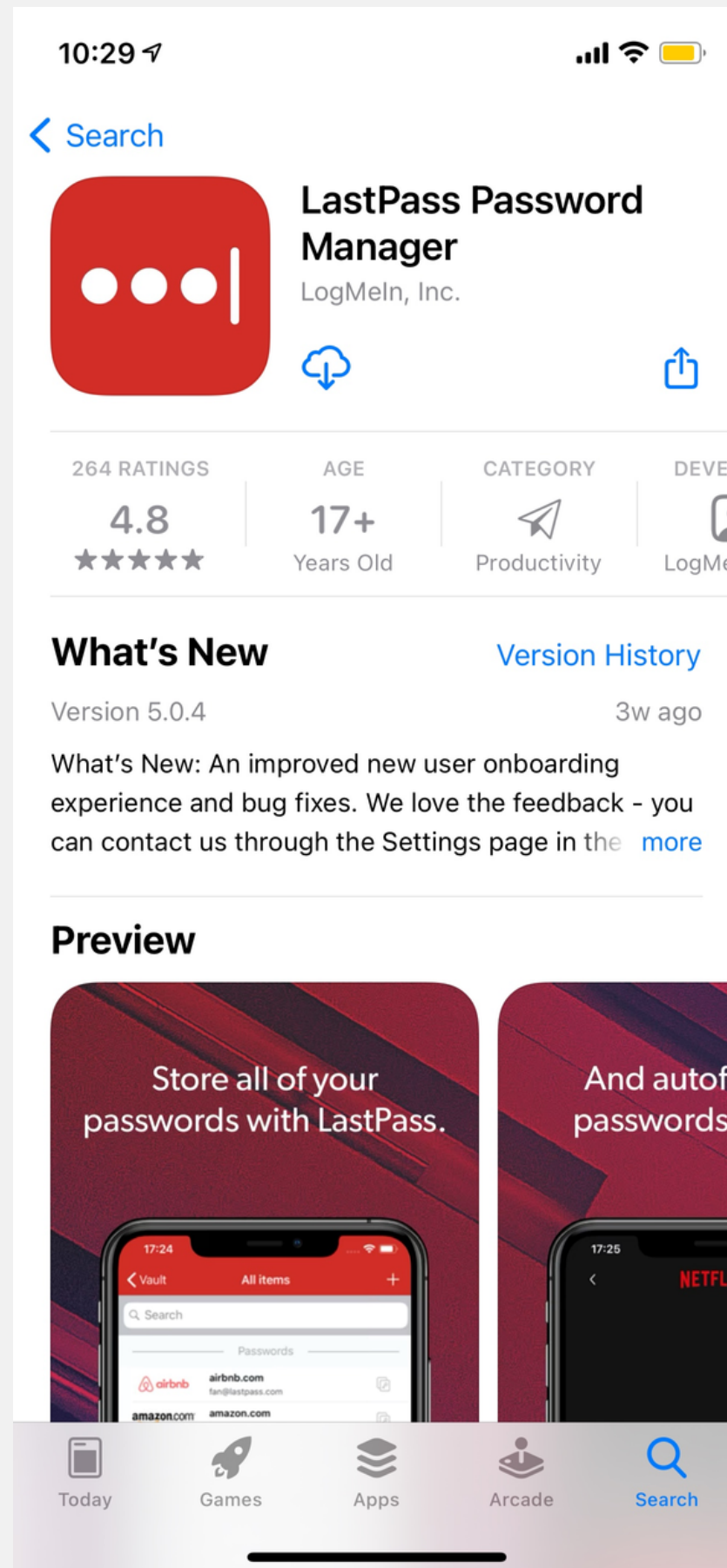
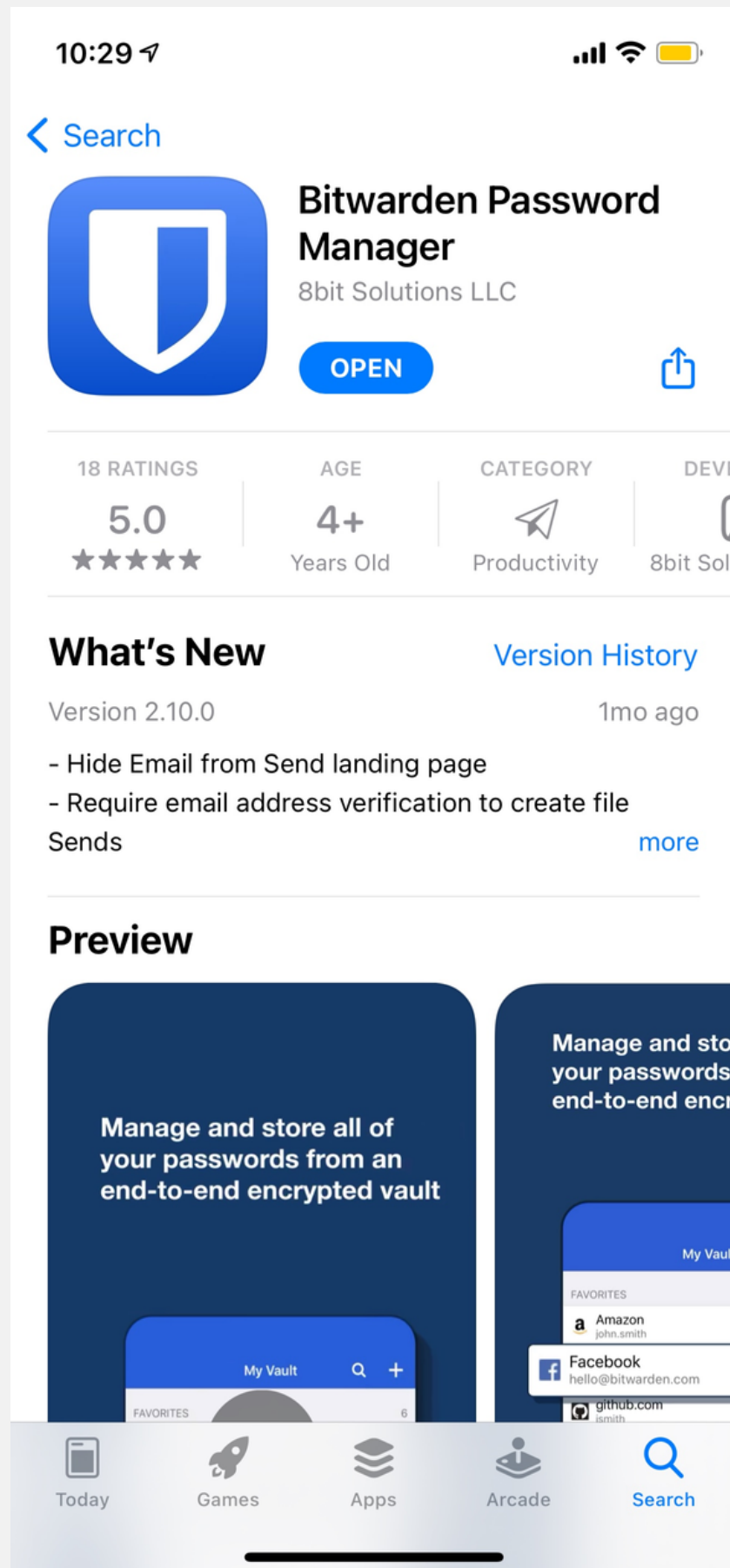
PASSWORDS

PROTECT YOUR IDENTITY
DATA ENCRYPTION
ACCESS TO DEVICES



123456
Aa123456
admin
12345678
123456789
password
Ar123455
aa123456
12345
123456Za

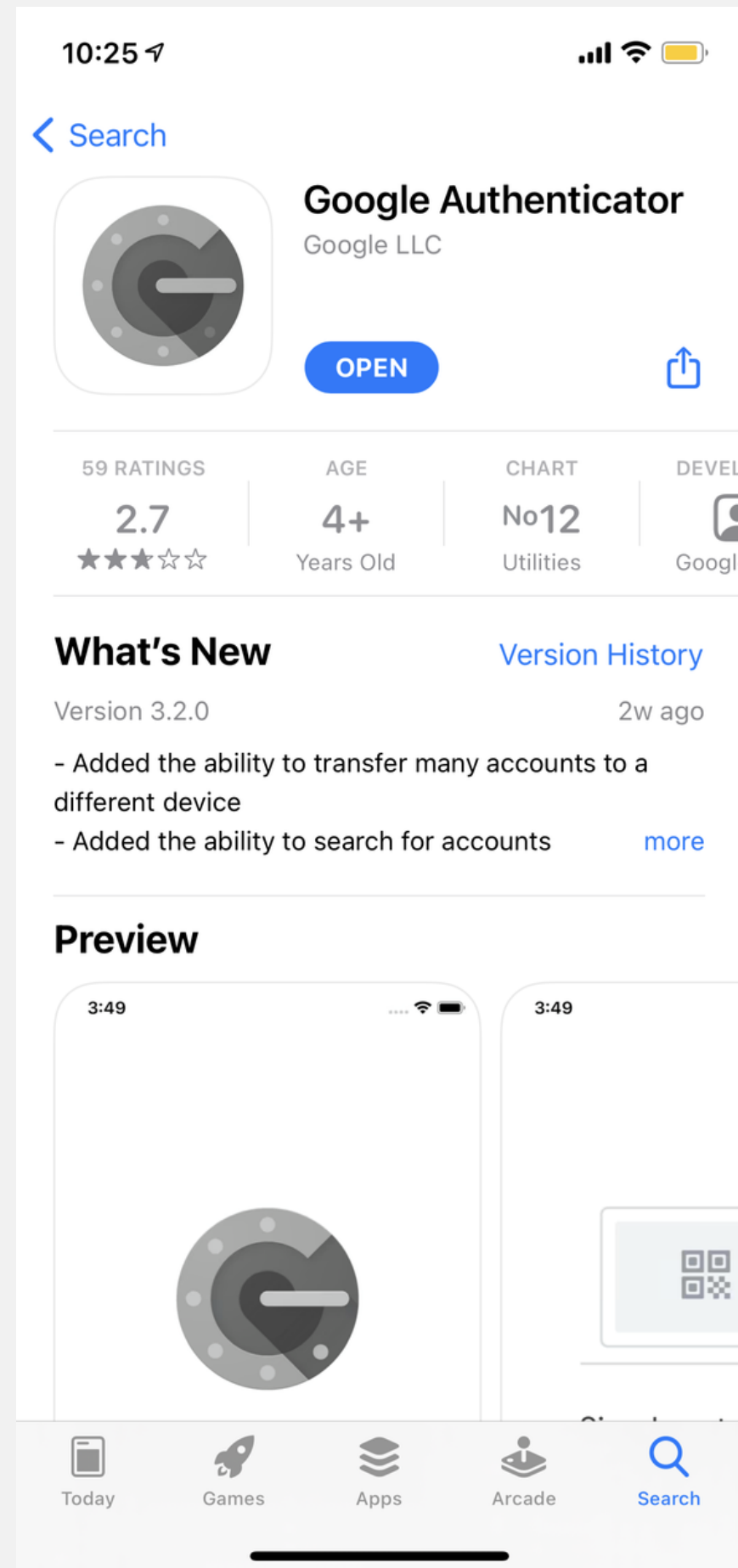
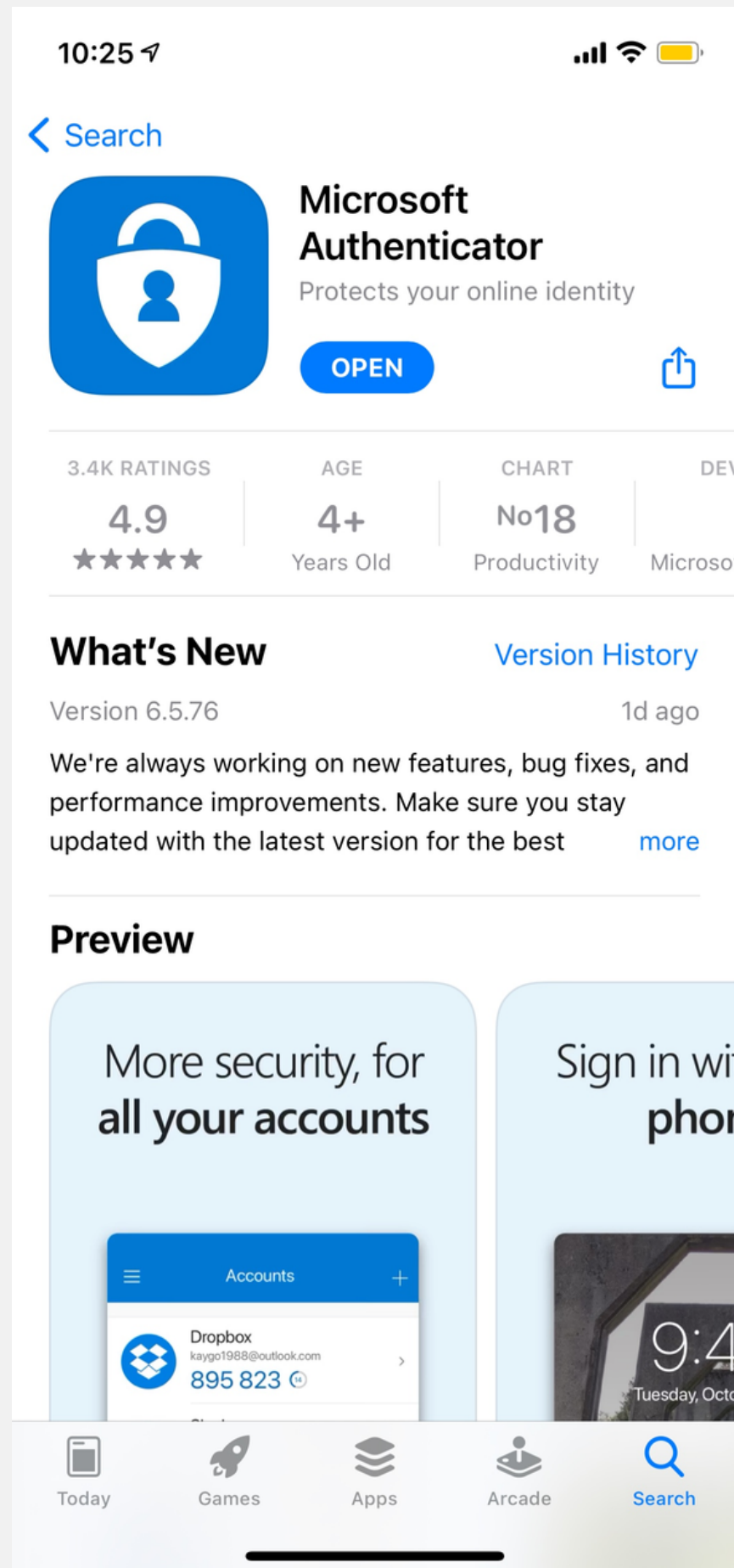
123456789Za
Aa112233
P@ssw0rd
1234567890
123456za
1212312121
111111
12345678910
Mm1234567
aisadmin





USE MULTI-FACTOR AUTHENTICATION

2-FACTOR AUTHENTICATION
2-STEP VERIFICATION
ONE-TIME PASSWORD
SECURITY TOKEN
FINGERPRINT
FACE



LEARN ABOUT

PHISHING & SCAM

SOCIAL ENGINEERING
EMAIL FRAUD
PHONE CALL
SMS/MESSAGING
DEEPFAKE



USE AND ALWAYS CHECK

ENCRYPTION

CONFIDENTIALITY

DATA-AT-REST

DATA-IN-TRANSIT

HTTPS EVERYWHERE



BACKUP

ข้อมูล

DATA CLASSIFICATION

3 REPLICAS

2 DIFFERENT TECHNOLOGIES

1 OFFSITE/OFFLINE

BACKUP ENCRYPTION

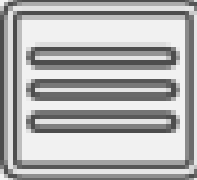
RESTORE TEST



QNAP

Synology®

 TrueNAS
CORE

 OpenMediaVault
The open network attached storage solution



pCloud

เก็บบันทึก

ACTIVITY LOGS

CONFIDENTIALITY
INTEGRITY
NO-REPUDIATION



CASE #1

บริษัททำข้อมูลลูกค้าเร็วไหน

- ลูกค้า = เจ้าของข้อมูลส่วนบุคคล
- บริษัท = ผู้ควบคุมข้อมูลส่วนบุคคล



CASE #2

ผู้รับจ้างพัฒนาซอฟต์แวร์ทำข้อมูลรั่วไหล

- ลูกค้า = เจ้าของข้อมูลส่วนบุคคล
- องค์กร = ผู้ควบคุมข้อมูลส่วนบุคคล
- ผู้รับจ้าง = ผู้ประมวลผลข้อมูลส่วนบุคคล



CASE #3

ที่ปรึกษา รับงานพัฒนาระบบ ทำข้อมูลลูกค้ารัวไหล

- ลูกค้า = เจ้าของข้อมูลส่วนบุคคล
- องค์กร = ผู้ควบคุมข้อมูลส่วนบุคคล
- ที่ปรึกษา = ผู้ประมวลผลข้อมูลส่วนบุคคล



CASE #4

บริษัททัวร์ ทำข้อมูลลูกค้าเร็วไหน

- ลูกค้า = เจ้าของข้อมูลส่วนบุคคล
- องค์กร = ผู้ควบคุมข้อมูลส่วนบุคคล
- บริษัททัวร์ = ผู้ประมวลผลข้อมูลส่วนบุคคล

