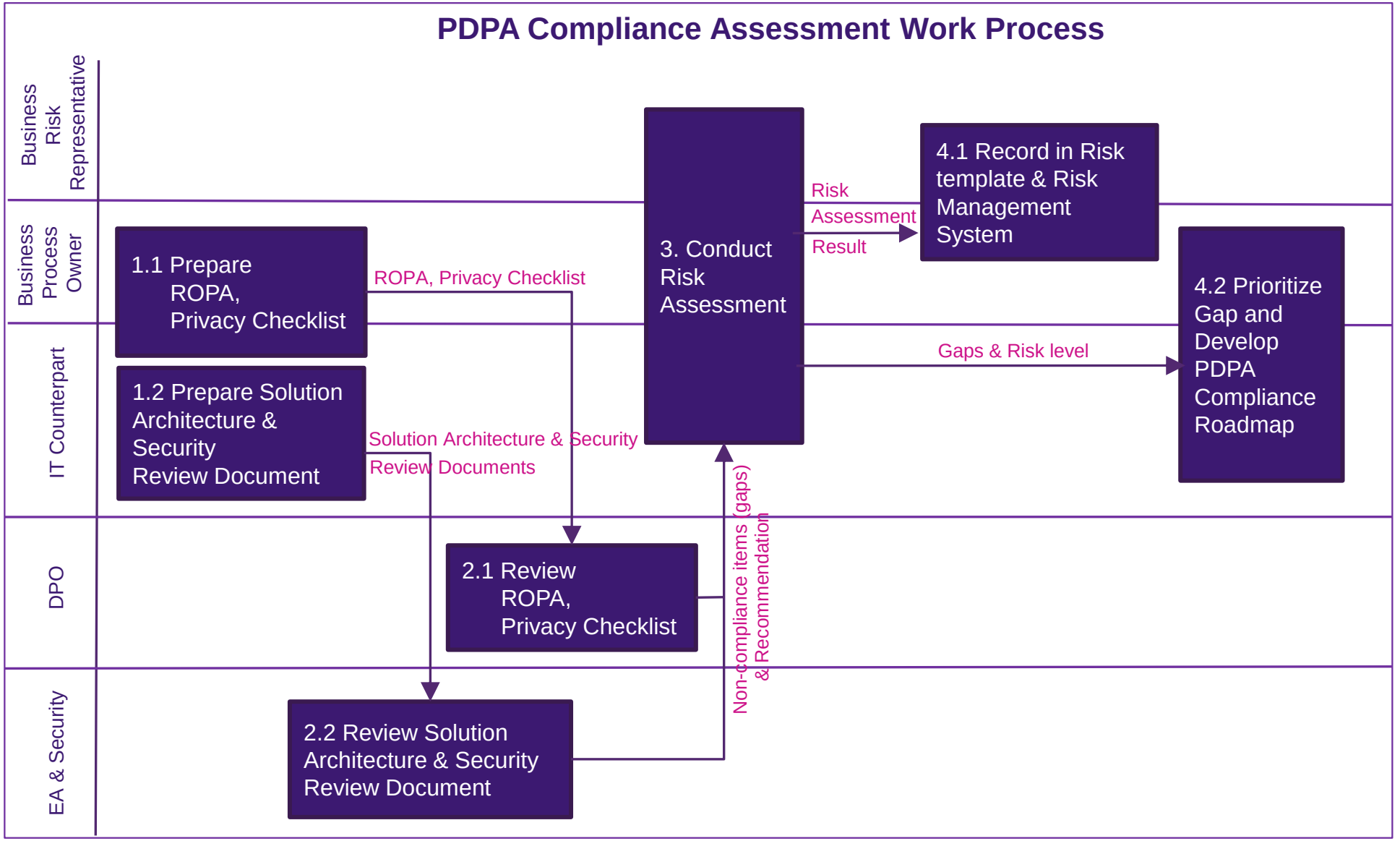
# Data Flow/RoPA/Privacy Checklist

# PDPA Compliance Assessment Work Process



# Records of Processing Activities (ROPA)

มาตรา ๓๙ ให้ผู้ควบคุมข้อมูลส่วนบุคคลบันทึกรายการ อย่างน้อยดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานสามารถตรวจสอบได้ โดยจะบันทึกเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้

(๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

(๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท



(๓) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล

(๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

(๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

(๖) การใช้หรือเปิดเผยตามมาตรา ๒๗ วรรคสาม

(๗) การปฏิเสธคำขอหรือการคัดค้านตามมาตรา ๓๐ วรรคสาม มาตรา ๓๑ วรรคสาม มาตรา ๓๒ วรรคสาม และมาตรา ๓๖ วรรคหนึ่ง

(๘) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัยตามมาตรา ๓๗ (๑)

ความในวรรคหนึ่งให้นำมาใช้บังคับกับตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง โดยอนุโลม

ความใน (๑) (๒) (๓) (๔) (๕) (๖) และ (๘) อาจยกเว้นมิให้นำมาใช้บังคับกับผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด เว้นแต่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมิใช่กิจการที่เก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเป็นครั้งคราว หรือมีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๖

# Records of Processing Activities (ROPA)

## For Controllers (GDPR vs PDPA)

| Description (At least) | GDPR | PDPA |
|---|---|---|
| Name and contact details of the Controller, Joint Controller | 30 (a) | ๓๙ (๓) |
| Purposes of the processing | 30 (b) | ๓๙ (๒) |
| Categories of data subjects and categories of personal data | 30 (c) | ๓๙ (๑) |
| Categories of recipients including recipients in third countries or international Organisations | 30 (d) | |
| Transfers of personal data to a third country , and suitable Safeguards | 30 (e) | |
| Time limits for Erasure | 30 (f) | ๓๙ (๔) |
| The technical and organisational security measures | 30 (g) | ๓๙ (๘) |
| สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล | | ๓๙ (๕) |
| การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอม | | ๓๙ (๖) |
| การปฏิเสธคำขอหรือการคัดค้าน[1] | | ๓๙ (๗) |

[1] บันทึกรายการดังกล่าวน่าจะไปปรากฏในบันทึกการปฏิบัติงานในแต่ละฝ่ายงานหรือกิจกรรมประมวลผลข้อมูลย่อยๆ ที่เกี่ยวข้องมากกว่าที่จะมาปรากฏในบันทึกที่เป็นภาพรวมขององค์กร (TDPG 3.0, 2563: 124) และตามร่างกฎหมายลำดับรอง กลุ่มที่ 1 หน้า 28 - 29 การบันทึกกิจกรรมการประมวลผลต้องบันทึกเป็นรายกิจกรรม และรายการในมาตรา 39(7) ให้นำไปบันทึกแยกต่างหาก

# ROPA
## For Controllers (PDPA)



**1.5 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล**
**เรื่อง การจัดให้มีบันทึกรายการกิจกรรมประมวลผล การจัดมาตรการเกี่ยวกับการขอใช้สิทธิในการเข้าถึงข้อมูล ข้อมูลส่วนบุคคล และการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล**

**สรุปสาระสำคัญของร่างประกาศฯ**

(2.1) กำหนดนิยามคำว่า

"การประมวลผลข้อมูลส่วนบุคคล" หมายถึง การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"เหตุละเมิดข้อมูลส่วนบุคคล" หมายความว่า การรั่วไหลหรือละเมิดมาตรการความมั่นคงปลอดภัยต่อข้อมูลส่วนบุคคลซึ่งทำให้เกิดความเสียหาย สูญหาย เปลี่ยนแปลง ไม่ว่าจะโดยอุบัติเหตุหรือโดยมิชอบด้วยกฎหมาย รวมถึงการเปิดเผย หรือเข้าถึงข้อมูลส่วนบุคคลที่ใช้งาน เก็บรวบรวม หรือประมวลผลข้อมูลส่วนบุคคลใด ๆ โดยไม่ได้รับอนุญาต

(2.2) ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกรายการกิจกรรมประมวลผลข้อมูลของแต่ละประเภทกิจกรรมไว้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม โดยให้มีคำอธิบายประเภทเจ้าของข้อมูลส่วนบุคคลและประเภทของข้อมูลส่วนบุคคลด้วย
- วัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลแต่ละประเภท
- ชื่อและข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล ตัวแทน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) รวมถึงช่องทางการติดต่อ
- ระยะเวลาในการเก็บรักษาและการลบข้อมูลส่วนบุคคลประเภทต่าง ๆ
- สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับการขอใช้สิทธิเข้าถึงข้อมูลส่วนบุคคลนั้น
- การใช้หรือเปิดเผยข้อมูลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามมาตรา 24 หรือมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประเภทของผู้ที่อาจได้รับการเปิดเผยข้อมูลและข้อมูลเกี่ยวกับการโอนข้อมูลส่วนบุคคลออกไปยังประเทศที่สามหรือองค์การระหว่างประเทศ (ถ้ามี)
- คำอธิบายทั่วไปเกี่ยวกับมาตรการในการรักษาความมั่นคงปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล





บันทึกรายการดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษรอาจจัดให้อยู่ในรูปแบบหนังสือหรือระบบอิเล็กทรอนิกส์ก็ได้ โดยต้องทำให้สามารถเข้าถึงได้ง่าย และเมื่อมีการร้องขอ ผู้ควบคุมข้อมูลส่วนบุคคลต้องสามารถแสดงให้สำนักงานตรวจสอบได้อย่างรวดเร็ว

(2.3) ผู้ควบคุมข้อมูลส่วนบุคคลซึ่งเป็นกิจการขนาดเล็กอาจได้รับยกเว้นให้ไม่บันทึกรายการตามมาตรา 39 (1) (2) (3) (4) (5) (6) และ (8) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เว้นแต่มีการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือการประมวลผลข้อมูลส่วนบุคคลนั้นมิได้กระทำเป็นครั้งคราว หรือมีการประมวลผลข้อมูลส่วนบุคคลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กิจการขนาดเล็ก หมายความถึง กิจการที่มีลักษณะเป็นวิสาหกิจขนาดย่อมตามหลักเกณฑ์ที่กำหนดไว้ในกฎกระทรวงที่ออกตามกฎหมายว่าด้วยการส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม พ.ศ. 2543 และที่แก้ไขเพิ่มเติม และกิจการขนาดเล็กนั้นต้องมีการประมวลผลข้อมูลส่วนบุคคลน้อยกว่า 1,000 ราย

(2.4) การทำบันทึกการปฏิเสธการใช้สิทธิตามมาตรา 39 (7) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดทำและเก็บรักษาบันทึกการปฏิเสธคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลแยกต่างหากจากบันทึกรายการกิจกรรมประมวลผลข้อมูล โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

- คำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล
- คำอธิบายพร้อมทั้งเหตุผลในการปฏิเสธการขอใช้สิทธินั้น
- กิจกรรมประมวลผลข้อมูลที่ปฏิเสธการขอใช้สิทธิ

บันทึกการปฏิเสธการใช้สิทธิดังกล่าวต้องจัดทำเป็นลายลักษณ์อักษรซึ่งอาจจัดให้อยู่ในรูปแบบหนังสือหรืออิเล็กทรอนิกส์ก็ได้ โดยต้องทำให้บันทึกสามารถเข้าถึงได้ง่าย และสามารถแสดงให้สำนักงานตรวจสอบได้อย่างรวดเร็ว

(2.5) ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีข้อมูลดังต่อไปนี้ เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลได้

- วัตถุประสงค์ในการประมวลผล
- ประเภทของข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- ผู้รับหรือประเภทของผู้รับที่ข้อมูลนั้นจะถูกส่งต่อหรือถูกเปิดเผย โดยเฉพาะอย่างยิ่งผู้รับในประเทศที่สามหรือองค์การระหว่างประเทศ

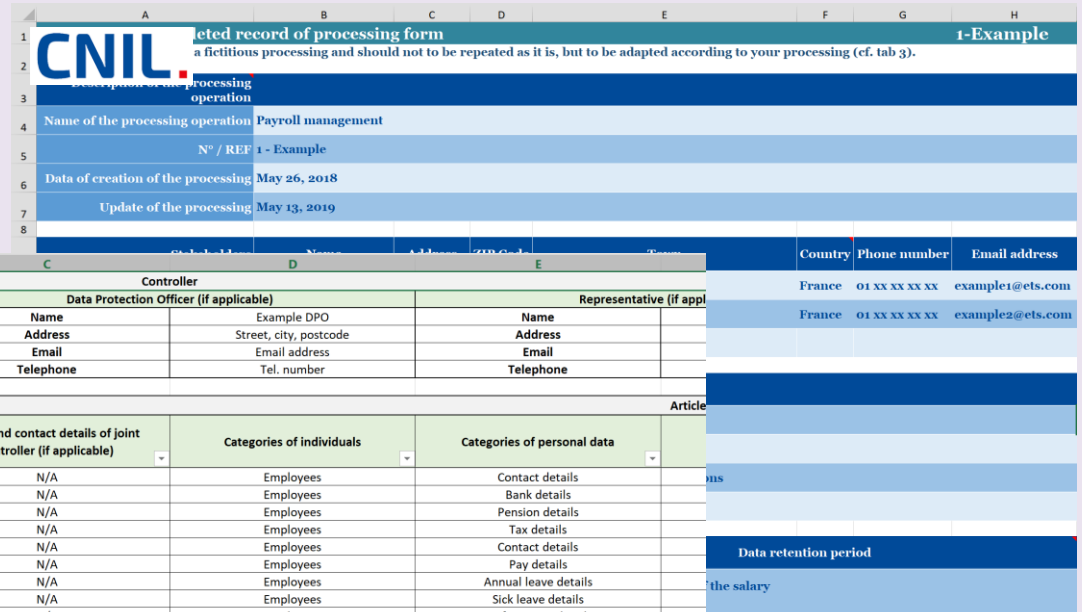


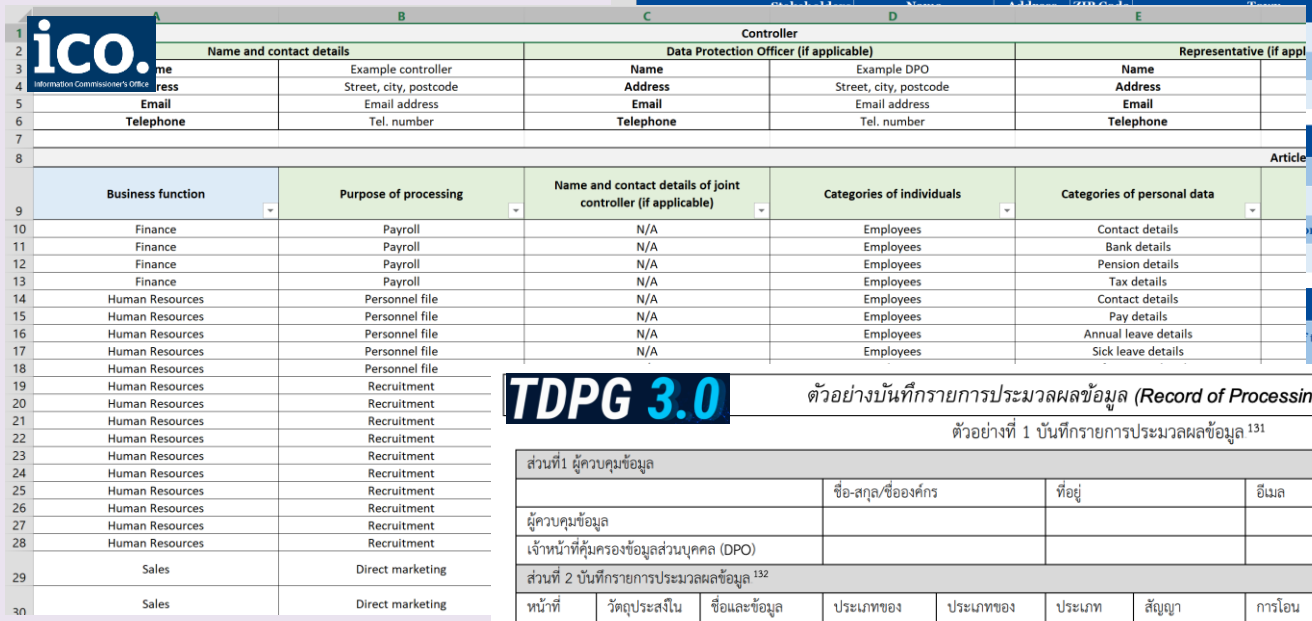
https://www.mdes.go.th/mission/detail/2315-%E0%B8%9C%E0%B8%A5%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%A8%E0%B8%B6%E0%B8%81%E0%B8%A9%E0%B8%B2%E0%B8%A0%E0%B8%B2%E0%B8%A2%E0%B9%83%E0%B8%95%E0%B9%89%E0%B9%82%E0%B8%84%E0%B8%A3%E0%B8%87%E0%B8%81%E0%B8%B2%E0%B8%A3%E0%B8%82%E0%B8%AD%E0%B8%87%E0%B8%AA%E0%B8%B3%E0%B8%99%E0%B8%B1%E0%B8%81%E0%B8%87%E0%B8%B2%E0%B8%99 เข้าถึงเมื่อ 4 เมษายน 2565

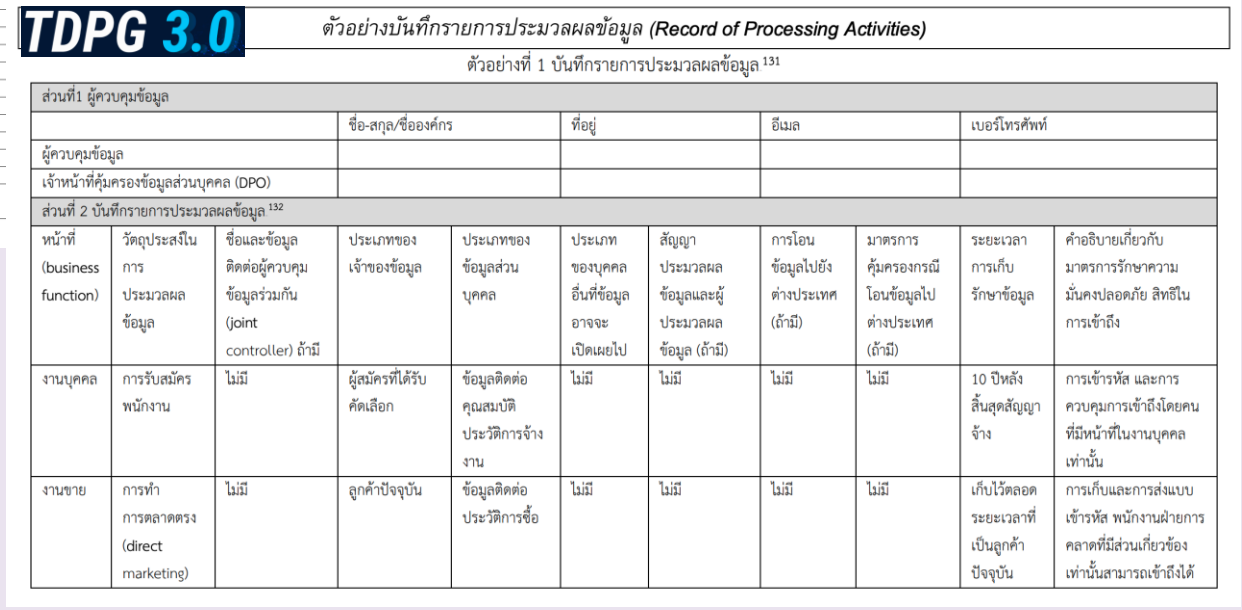
# ROPA

วิธีการ:

- เริ่มจากการเขียน Data mapping
- จัดเตรียมข้อคำถาม
- พบหน่วยงานหลัก
- ตรวจสอบ ทบทวน แบบฟอร์มต่าง ๆ ที่ใช้อยู่ ตลอดจน กระบวนการ สัญญา และข้อตกลงต่าง ๆ




ICO > https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/
CNIL > https://www.cnil.fr/en/record-processing-activities

THAI

CNIL.

# f a completed record of processing form — 1-Example

This example is based on a fictitious processing and should not to be repeated as it is, but to be adapted according to your processing (cf. tab 3).

| Description of the processing operation | |
|---|---|
| Name of the processing operation | Payroll management |
| N° / REF | 1 - Example |
| Data of creation of the processing | May 26, 2018 |
| Update of the processing | May 13, 2019 |

| Stakeholders | Name | Address | ZIP Code | Town | Country | Phone number | Email address |
|---|---|---|---|---|---|---|---|
| Controller | Louise DUPONT | 1 rue Rivoli | 75001 | Paris | France | 01 xx xx xx xx | example1@ets.com |
| Data protection officer | Martin HENRI | 1 rue Rivoli | 75001 | Paris | France | 01 xx xx xx xx | example2@ets.com |
| DPO's Organisation (if external DPO) | N/A | | | | | | |

| Purpose(s) of the data processing | |
|---|---|
| Main purpose | Payroll management |
| Sub-purpose 1 | Calculation of remuneration |
| Sub-purpose 2 | Calculation of the amount of payments made to social security organisations |
| Sub-purpose 3 | Transfer orders to the bank |

| Categories of personal data | Description | Data retention period |
|---|---|---|
| Marital status, ID, identification data, images... | Last names, names and addresses | 5 years from the payment of the salary |

| | A | B | C | D | E | |
|---|---|---|---|---|---|---|
| | | | Controller | | | |
| | Name and contact details | | Data Protection Officer (if applicable) | | Representative (if appl | |
| 3 | **Name** | Example controller | **Name** | Example DPO | **Name** | |
| 4 | **Address** | Street, city, postcode | **Address** | Street, city, postcode | **Address** | |
| 5 | **Email** | Email address | **Email** | Email address | **Email** | |
| 6 | **Telephone** | Tel. number | **Telephone** | Tel. number | **Telephone** | |
| 7 | | | | | | |
| 8 | | | | | | Article |
| 9 | **Business function** | **Purpose of processing** | **Name and contact details of joint controller (if applicable)** | **Categories of individuals** | **Categories of personal data** | |
| 10 | Finance | Payroll | N/A | Employees | Contact details | |
| 11 | Finance | Payroll | N/A | Employees | Bank details | |
| 12 | Finance | Payroll | N/A | Employees | Pension details | |
| 13 | Finance | Payroll | N/A | Employees | Tax details | |
| 14 | Human Resources | Personnel file | N/A | Employees | Contact details | |
| 15 | Human Resources | Personnel file | N/A | Employees | Pay details | |
| 16 | Human Resources | Personnel file | N/A | Employees | Annual leave details | |
| 17 | Human Resources | Personnel file | N/A | Employees | Sick leave details | |
| 18 | Human Resources | Personnel file | N/A | Employees | Performance details | |
| 19 | Human Resources | Recruitment | N/A | Successful candidates | Contact details | |
| 20 | Human Resources | Recruitment | N/A | Successful candidates | Qualifications | |
| 21 | Human Resources | Recruitment | N/A | Successful candidates | Employment history | |
| 22 | Human Resources | Recruitment | N/A | Successful candidates | Ethnicity | |
| 23 | Human Resources | Recruitment | N/A | Successful candidates | Disability details | |
| 24 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Contact details | |
| 25 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Qualifications | |
| 26 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Employment history | |
| 27 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Ethnicity | |
| 28 | Human Resources | Recruitment | N/A | Unsuccessful candidates | Disability details | |
| 29 | Sales | Direct marketing | N/A | Existing customers | Contact details | |
| 30 | Sales | Direct marketing | N/A | Existing customers | Purchase history | |

# ตัวอย่างบันทึกรายการประมวลผลข้อมูล (Record of Processing Activities)

## ตัวอย่างที่ 1 บันทึกรายการประมวลผลข้อมูล[131]

| ส่วนที่1 ผู้ควบคุมข้อมูล | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | ชื่อ-สกุล/ชื่อองค์กร | | ที่อยู่ | | อีเมล | | เบอร์โทรศัพท์ | | |
| ผู้ควบคุมข้อมูล | | | | | | | | | | |
| เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) | | | | | | | | | | |
| **ส่วนที่ 2 บันทึกรายการประมวลผลข้อมูล[132]** | | | | | | | | | | |
| หน้าที่ (business function) | วัตถุประสงค์ในการประมวลผลข้อมูล | ชื่อและข้อมูลติดต่อผู้ควบคุมข้อมูลร่วมกัน (joint controller) ถ้ามี | ประเภทของเจ้าของข้อมูล | ประเภทของข้อมูลส่วนบุคคล | ประเภทของบุคคลอื่นที่ข้อมูลอาจจะเปิดเผยไป | สัญญาประมวลผลข้อมูลและผู้ประมวลผลข้อมูล (ถ้ามี) | การโอนข้อมูลไปยังต่างประเทศ (ถ้ามี) | มาตรการคุ้มครองกรณีโอนข้อมูลไปต่างประเทศ (ถ้ามี) | ระยะเวลาการเก็บรักษาข้อมูล | คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย สิทธิในการเข้าถึง |
| งานบุคคล | การรับสมัครพนักงาน | ไม่มี | ผู้สมัครที่ได้รับคัดเลือก | ข้อมูลติดต่อ คุณสมบัติ ประวัติการจ้างงาน | ไม่มี | ไม่มี | ไม่มี | ไม่มี | 10 ปีหลังสิ้นสุดสัญญาจ้าง | การเข้ารหัส และการควบคุมการเข้าถึงโดยคนที่มีหน้าที่ในงานบุคคลเท่านั้น |
| งานขาย | การทำการตลาดตรง (direct marketing) | ไม่มี | ลูกค้าปัจจุบัน | ข้อมูลติดต่อ ประวัติการซื้อ | ไม่มี | ไม่มี | ไม่มี | ไม่มี | เก็บไว้ตลอดระยะเวลาที่เป็นลูกค้าปัจจุบัน | การเก็บและการส่งแบบเข้ารหัส พนักงานฝ่ายการตลาดที่มีส่วนเกี่ยวข้องเท่านั้นสามารถเข้าถึงได้ |


# KEEP CALM AND GET READY FOR PDPA