

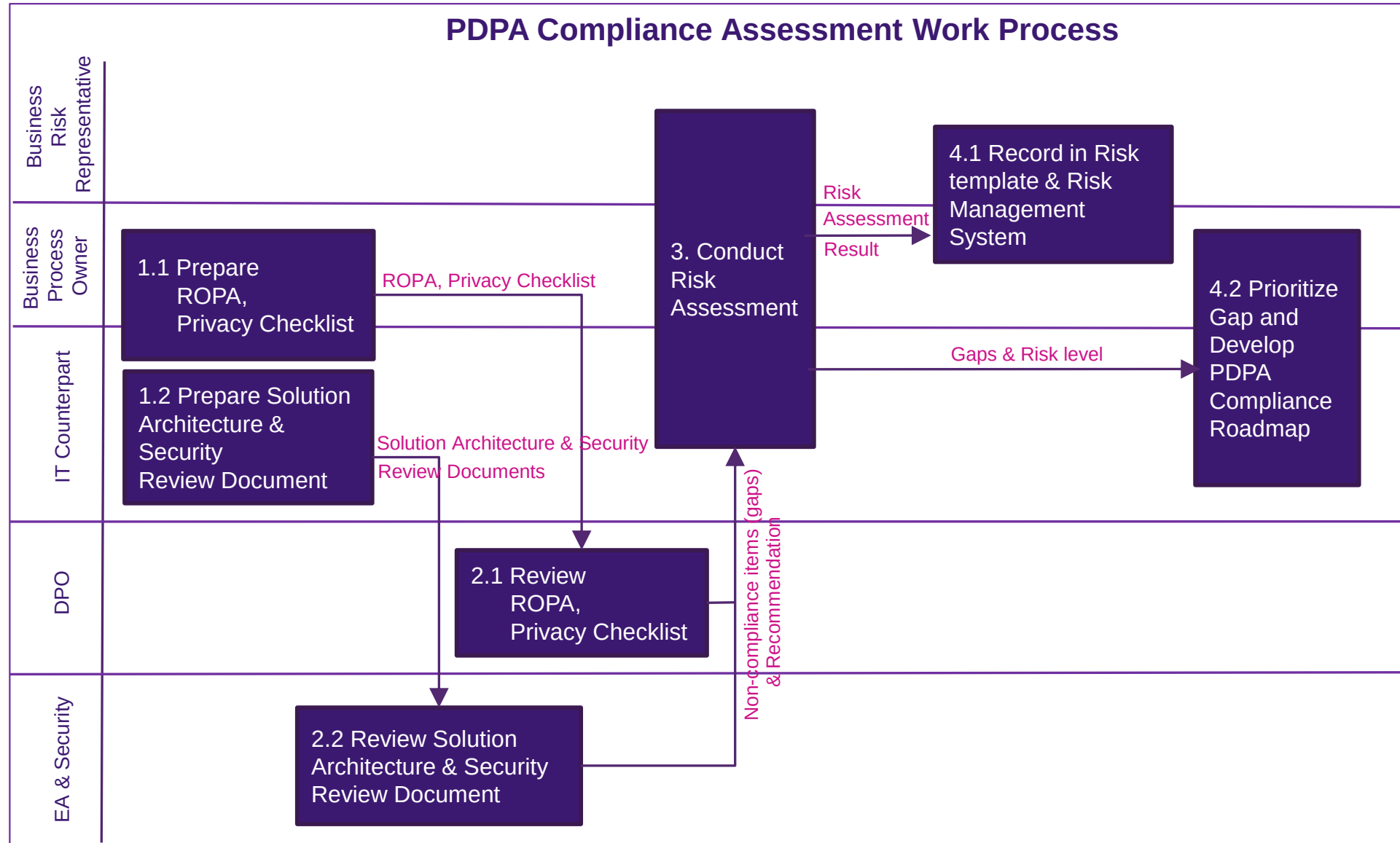
Data Protection Impact Assessment

How to?

ดร.สิทธิชัย จันทรานนท์

20 May 2022





Data Protection Impact Assessment (DPIA)

Section 3

Data protection impact assessment and prior consultation

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
 - (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
 - (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
 - (c) a systematic monitoring of a publicly accessible area on a large scale.
4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.
5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.
6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

DPIA

For Controllers (GDPR)

L 119/54

EN

Official Journal of the European Union

4.5.2016

7. The assessment shall contain at least:

- (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

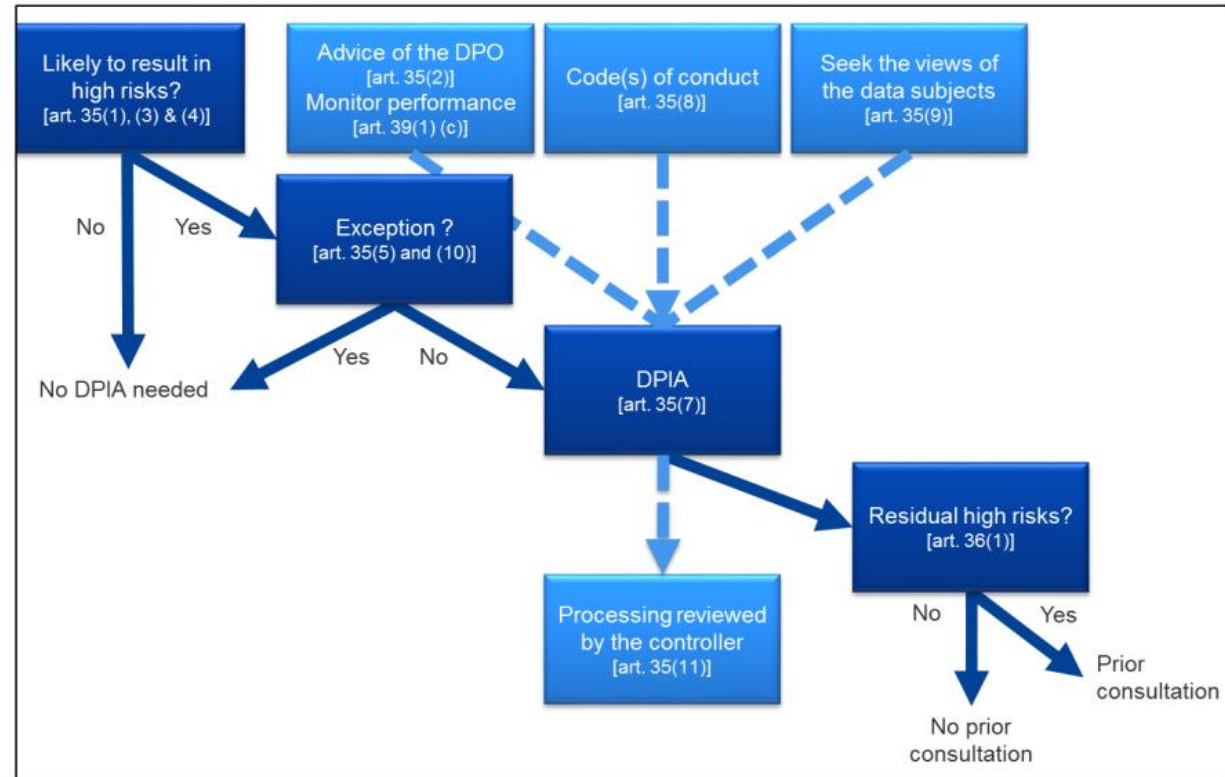
10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

DPIA

For Controllers (GDPR vs PDPA)

The following figure illustrates the basic principles related to the DPIA in the GDPR:



DPIA

For Controllers (GDPR vs PDPA)

In order to provide a more concrete set of processing operations that require a DPIA due to their inherent high risk, taking into account the particular elements of Articles 35(1) and 35(3)(a) to (c), the list to be adopted at the national level under article 35(4) and recitals 71, 75 and 91, and other GDPR references to “*likely to result in a high risk*” processing operations¹⁴, the following nine criteria should be considered.

1. Evaluation or scoring, including profiling and predicting, especially from “*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements*” (recitals 71 and 91). Examples of this could include a financial institution that screens its customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.
2. Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects producing “*legal effects concerning the natural person*” or which “*similarly significantly affects the natural person*” (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion. Further explanations on these notions will be provided in the upcoming WP29 Guidelines on Profiling.
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or “*a systematic monitoring of a publicly accessible area*” (Article 35(3)(c))¹⁵. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in public (or publicly accessible) space(s).
4. Sensitive data or data of a highly personal nature: this includes special categories of personal data as defined in Article 9 (for example information about individuals’ political opinions), as well as personal data relating to criminal convictions or offences as defined in Article 10. An example would be a general hospital keeping patients’ medical records or a private investigator keeping offenders’ details. Beyond these provisions of the GDPR, some categories of data can be considered as increasing the possible risk to the rights and freedoms

¹⁴ See e.g. recitals 75, 76, 92, 116.

¹⁵ The WP29 interprets “*systematic*” as meaning one or more of the following (see the WP29 Guidelines on Data Protection Officer 16/EN WP 243):

- occurring according to a system;
- pre-arranged, organised or methodical;

DPIA

For Controllers (GDPR vs PDPA)

5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale¹⁶:
 - a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
 - b. the volume of data and/or the range of different data items being processed;
 - c. the duration, or permanence, of the data processing activity;
 - d. the geographical extent of the processing activity.
6. Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject¹⁷.
7. Data concerning vulnerable data subjects (recital 75): the processing of this type of data is a criterion because of the increased power imbalance between the data subjects and the data controller, meaning the individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data), employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, *etc.*), and in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
8. Innovative use or applying new technological or organisational solutions, like combining use of finger print and face recognition for improved physical access control, *etc.* The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology, defined in “*accordance with the achieved state of technological knowledge*” (recital 91), can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals’ rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain “Internet of Things” applications could have a significant impact on individuals’ daily lives and privacy; and therefore require a DPIA.

¹⁶ See the WP29 Guidelines on Data Protection Officer 16/EN WP 243.

¹⁷ See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24.

DPIA

For Controllers (GDPR vs PDPA)

9. When the processing in itself “*prevents data subjects from exercising a right or using a service or a contract*” (Article 22 and recital 91). This includes processing operations that aims at allowing, modifying or refusing data subjects’ access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller envisages to adopt.

However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

The following examples illustrate how the criteria should be used to assess whether a particular processing operation requires a DPIA:

Examples of processing	Possible Relevant criteria	DPIA likely to be required?
A hospital processing its patients’ genetic and health data (hospital information system).	- Sensitive data or data of a highly personal nature. - Data concerning vulnerable data subjects. - Data processed on a large-scale.	
The use of a camera system to monitor driving behavior on highways. The controller envisages to use an intelligent video analysis system to single out cars and automatically recognize license plates.	- Systematic monitoring. - Innovative use or applying technological or organisational solutions.	
A company systematically monitoring its employees’ activities, including the monitoring of the employees’ work station, internet activity, etc.	- Systematic monitoring. - Data concerning vulnerable data subjects.	
The gathering of public social media data for generating profiles.	- Evaluation or scoring. - Data processed on a large scale. - Matching or combining of datasets. - Sensitive data or data of a highly personal	Yes

1.2 ร่างประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

เรื่อง การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลและหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล
ที่จะให้เจ้าของข้อมูลส่วนบุคคลปฏิเสธการถูกตัดสินใจโดยใช้กระบวนการอัตโนมัติเพียงอย่างเดียว

สรุปสาระสำคัญของร่างประกาศฯ

(2.1) กำหนดคำนิยาม

“ผู้เปราะบาง” หมายถึง บุคคลที่ภายใต้วัตถุประสงค์ของการประมวลผลข้อมูลส่วนบุคคลนั้น มีความจำกัดของความสามารถในการให้ความยินยอมโดยอิสระ หรือคัดค้านการประมวลผลข้อมูลส่วนบุคคลได้โดยอิสระ หรือเข้าใจผลกระทบที่อาจเกิดจากการประมวลผลข้อมูลส่วนบุคคลนั้น

“โปรไฟล์ลิง” หมายถึง รูปแบบการประมวลผลข้อมูลส่วนบุคคลใดๆ ซึ่งมีการใช้ข้อมูลส่วนบุคคลในการประเมินแง่มุมเกี่ยวกับบุคคล โดยเฉพาะอย่างยิ่งเพื่อวิเคราะห์หรือคาดการณ์เกี่ยวกับบุคคลธรรมดาในเรื่องประสิทธิภาพในการทำงาน สถานะทางเศรษฐกิจ สุขภาพของบุคคล ความชื่นชอบส่วนบุคคล ประโยชน์ของบุคคล พฤติกรรมของบุคคล ความน่าเชื่อถือของบุคคล ตำแหน่งทางภูมิศาสตร์ หรือความเคลื่อนไหวของบุคคล

“การตัดสินใจโดยใช้กระบวนการอัตโนมัติเพียงอย่างเดียว” หมายถึง กระบวนการตัดสินใจโดยใช้วิธีอัตโนมัติ และปราศจากการมีส่วนร่วมของมนุษย์ ซึ่งเป็นการตัดสินใจโดยอาศัยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลทั้งที่เป็นข้อมูลที่ได้รับมา และเป็นข้อมูลที่ถูกสร้างขึ้น

For Controllers (GDPR vs PDPA)

โดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลเอง

(2.2) การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

- การประมวลผลอันจะส่งผลให้สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลต้องเสื่อมเสียไปหรือทำให้ไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ ถือเป็นการประมวลผลข้อมูลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- คณะกรรมการอาจกำหนดให้กิจกรรมการประมวลผลบางประเภทเป็นการประมวลผลข้อมูลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลตามรายชื่อแนบท้ายประกาศ หรือตามที่กำหนดไว้ในข้อปฏิบัติที่ได้รับการรับรองจากคณะกรรมการ
- ในกรณีที่การประมวลผลมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (DPIA) และให้สันนิษฐานว่าผู้ควบคุมข้อมูลส่วนบุคคลได้ดำเนินการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลและจัดให้มีมาตรการที่เหมาะสมแล้วตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

DPIA

For Controllers (GDPR vs PDPA)

โครงการศึกษาและเตรียมการเพื่อจัดทำร่างกฎหมายลำดับรองภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

- ในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล จะต้องประเมินความเสี่ยงของการประมวลผลข้อมูลส่วนบุคคลก่อนหรือในขณะที่มี การประมวลผลข้อมูลส่วนบุคคล รวมถึงการประมวลผลข้อมูลส่วนบุคคลที่มีอยู่แล้ว
- นอกเหนือจากกรณีที่กำหนดในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือ ที่กำหนดในประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลว่าด้วยรูปแบบ วิธีการ และ มาตรฐานขั้นต่ำที่กำหนดร่วมกัน การประมวลผลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิ เสรีภาพของบุคคลให้รวมถึงกิจกรรมการประมวลผลที่มีลักษณะดังต่อไปนี้
 - กรณีที่มีการประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ รวมถึง การโปรไฟล์ ซึ่งการประมวลผลดังกล่าวส่งผลเป็นการตัดสินใจที่ส่งผลทางกฎหมาย หรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล
 - กรณีที่มีการประมวลผลข้อมูลจำนวนมากที่เป็นข้อมูลส่วนบุคคลตาม มาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยพิจารณาจากจำนวน บุคคลที่เกี่ยวข้อง ปริมาณข้อมูลที่เกี่ยวข้อง ความหลากหลายของข้อมูลที่เกี่ยวข้อง ระยะเวลาการประมวลผลข้อมูลที่เกี่ยวข้อง และขนาดพื้นที่ทางภูมิศาสตร์ของ การประมวลผลข้อมูลที่เกี่ยวข้อง
 - กรณีที่เป็นการตรวจตราและเฝ้าดูพื้นที่สาธารณะจำนวนมากอย่างเป็นระบบ

DPIA

For Controllers (GDPR vs PDPA)

- กรณีที่เป็นการตรวจตราและเฝ้าดูพื้นที่สาธารณะจำนวนมากอย่างเป็นระบบ
- ในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลประมวลผลข้อมูลส่วนบุคคลตามหน้าที่ที่กฎหมายกำหนด ทั้งโดยฐานภายใต้มาตรา 24 (4) หรือ (6) ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อาจหรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเพื่อกำหนดกิจกรรมที่มีความเสี่ยงสูงซึ่งอาจไม่จำเป็นต้องจัดให้มีการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลก็ได้ ทั้งนี้ขั้นตอนและรายละเอียดให้เป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้อง
- การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลอาจมีขึ้นเพื่อรองรับการประมวลผลข้อมูลหลายกรณีที่มีลักษณะเดียวกันทั้งโดยสภาพ วัตถุประสงค์ หรือความเสี่ยง กรณีเช่นนี้พึงเปิดเผยข้อมูลอ้างอิงของการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลสู่สาธารณะ รวมถึงมาตรการที่กำหนดและเหตุผลที่จัดทำ การประเมินร่วมกัน
- กรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลร่วมกัน การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล พึงระบุหน้าที่ความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคลแต่ละรายและมาตรการที่แต่ละฝ่ายรับผิดชอบไว้เป็นลายลักษณ์อักษร โดยระบุถึงเหตุผลความจำเป็นและข้อมูลของแต่ละฝ่าย แต่ทั้งนี้เท่าที่ไม่กระทบถึงความปลอดภัยหรือจุดอ่อนทางธุรกิจของผู้ควบคุมข้อมูลส่วนบุคคล

(2.3) การจัดทำ การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล

DPIA

For Controllers (GDPR vs PDPA)

โครงการศึกษาและเตรียมการเพื่อจัดทำร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

- ในกรณีที่จำเป็นผู้ควบคุมข้อมูลส่วนบุคคลอาจมอบหมายให้ผู้ประมวลผลข้อมูลส่วนบุคคล
จัดการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลในกิจกรรมที่อยู่ภายใต้
ความรับผิดชอบของผู้ประมวลผลข้อมูลส่วนบุคคลแทนก็ได้
- การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล อาจแสดงให้เห็นขั้นตอนอย่างน้อย
ดังต่อไปนี้
 - ระบุความจำเป็นในการทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
 - อธิบายรายละเอียดการประมวลผลข้อมูลส่วนบุคคล
 - การรับฟังความคิดเห็นผู้มีส่วนได้เสีย
 - แสดงให้เห็นความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูลส่วนบุคคล
 - การประเมินความเสี่ยง ทั้งในเชิงร่างกาย จิตใจ และทรัพย์สิน
 - ระบุมาตรการลดความเสี่ยง
 - บันทึกรายละเอียดของแต่ละขั้นตอน
 - การติดตามตรวจสอบและทบทวนการดำเนินการตามแผนและมาตรการที่ได้จาก
การทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล
- หากได้ดำเนินการตามข้อปฏิบัติที่ได้รับการรับรองจากคณะกรรมการแล้ว ให้ถือว่า
ได้ดำเนินการจัดทำ DPIA แล้ว
- ผู้ควบคุมข้อมูลส่วนบุคคลต้องเผยแพร่เอกสารการบันทึกผลการจัดการประเมินผลกระทบ
ด้านการคุ้มครองข้อมูลส่วนบุคคลให้สามารถเข้าถึงได้โดยสาธารณะด้วยวิธีการตามสมควร
และแจ้งช่องทางเผยแพร่ที่สำนักงาน โดยอาจปกปิดหรือตัดเฉพาะส่วนที่เป็นข้อมูลลับ

DPIA

For Controllers (GDPR vs PDPA)

รายชื่อกิจกรรมการประมวลผลข้อมูลที่มีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลส่วนบุคคลที่คณะกรรมการกำหนด

กิจกรรมใดที่มีลักษณะดังต่อไปนี้รวมกันตั้งแต่ 2 ประการขึ้นไป ให้ถือเป็นกิจกรรมที่มีความเสี่ยงสูง

1. การประมวลผลข้อมูลส่วนบุคคลที่มีการใช้เทคโนโลยีใหม่ เช่น ปัญญาประดิษฐ์ (artificial intelligence)
2. การใช้โปรไฟล์หรือข้อมูลที่อ่อนไหวในการปฏิเสธไม่ให้เข้าถึงบริการ
3. การทำโปรไฟล์ของบุคคลในปริมาณมาก
4. การประมวลผลข้อมูลชีวภาพ
5. การประมวลผลข้อมูลพันธุกรรม
6. การจับคู่หรือเชื่อมโยงข้อมูลหรือชุดข้อมูลจากแหล่งข้อมูลหลายแหล่ง
7. การเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงโดยไม่มีการแจ้งเตือนเกี่ยวกับความเป็นส่วนตัว
8. การติดตามตำแหน่งที่อยู่หรือพฤติกรรมของบุคคล
9. การทำโปรไฟล์หรือทำการตลาดแบบระบุเป้าหมาย (target marketing) หรือบริการออนไลน์ที่มุ่งโดยตรงแก่ผู้เยาว์หรือผู้เปราะบาง
10. การประมวลผลข้อมูลที่น่าจะเป็นอันตรายต่อสุขภาพหรือความปลอดภัยของบุคคลในกรณีที่มีการรั่วไหล

13. แนวปฏิบัติเกี่ยวกับการจัดทำประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA)

การประมวลผลข้อมูลส่วนบุคคลผู้ควบคุมข้อมูลส่วนบุคคลจะต้องคำนึงถึงความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล และจะต้องจัดให้มีมาตรการในการรักษาความมั่นคงและปลอดภัยที่เหมาะสมกับความเสี่ยง ดังนั้นการจัดทำประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลหรือ Data Protection Impact Assessment (DPIA) นั้นเป็นหนึ่งในกระบวนการที่ธนาคารต้องจัดให้มีสำหรับการประมวลผลที่มีความเสี่ยงสูง เพื่อเป็นการปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งสอดคล้องกับ GDPR

การจัดทำ DPIA ที่มีประสิทธิภาพนั้นจะช่วยให้ธนาคารสามารถกำกับการปฏิบัติตามกฎหมายในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลได้ดียิ่งขึ้น อีกทั้งยังเป็นการสร้างความเชื่อมั่นและความไว้วางใจให้กับเจ้าของข้อมูลส่วนบุคคลและส่วนรวมมากขึ้น ช่วยลดความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลที่ไม่เหมาะสม ลดความเสี่ยงที่จะเกิดผลกระทบต่อชื่อเสียงของธนาคาร ซึ่งจะเป็นผลดีแก่ธนาคารเอง

13.1 ความแตกต่างระหว่าง Data Protection Impact Assessment (DPIA) กับ Privacy Impact Assessment (PIA)

- **Data Protection Impact Assessment (DPIA)** เป็นกระบวนการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล สำหรับกิจกรรมประมวลผลข้อมูลส่วนบุคคลต่าง ๆ ซึ่งตามกฎหมายกำหนดให้ทำเฉพาะกับความเสี่ยงสูง นั่นก็คือมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ซึ่งธนาคารสามารถขอคำปรึกษาจาก DPO ในขั้นตอนการออกแบบและการจัดทำ DPIA กระบวนการในจัดทำ DPIA ได้แก่ การระบุความเสี่ยงและผลกระทบที่อาจเกิดขึ้น (สำหรับการระบุความเสี่ยงและประเมินผลกระทบที่อาจเกิดขึ้น โปรดดูรายละเอียดในหัวข้อ 3.2 แนวปฏิบัติเกี่ยวกับการจำแนกข้อมูล) รวมถึงแนวทางการลดความเสี่ยงที่อาจเกิดขึ้นจากกิจกรรมการประมวลผลนั้น การทำ DPIA ไม่ใช่กระบวนการที่ทำเพียงครั้งเดียวแต่

จะต้องมีการทบทวนความเหมาะสมอยู่เสมอ เนื่องจากความเสี่ยงอาจเปลี่ยนแปลงได้จากปัจจัยหลายอย่าง เช่น การเปลี่ยนแปลงของเทคโนโลยีอย่างรวดเร็วอาจทำให้ความเสี่ยงที่จะเกิดผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลสูงขึ้น เป็นต้น

- **Privacy Impact Assessment (PIA)** เป็นกระบวนการที่เกี่ยวข้องกับการวิเคราะห์ การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลว่าจะทำอะไร โดยที่ PIA เป็นกระบวนการที่ใช้ในการป้องกันในเรื่องของการจัดทำ Privacy by Design นั่นก็คือ การที่ธนาคารจะต้องคำนึงถึงสิทธิความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลตั้งแต่ขั้นตอนการออกแบบ ซึ่งมักทำเมื่อมีการเริ่มหรือเข้าควบคุมกิจการอื่น มีการใช้กระบวนการใหม่ หรือออกผลิตภัณฑ์ใหม่

ธนาคารอาจทำ DPIA เพียงอย่างเดียวก็ได้หรืออาจจัดทำ PIA เข้ากับ DPIA ก็ได้เนื่องจากแนวทางในการจัดทำนั้นมีความคล้ายคลึงกัน อย่างไรก็ตาม ธนาคารอาจพิจารณาการทำ PIA เพิ่มเติมเมื่อเห็นว่ามีความจำเป็น

13.2 แนวปฏิบัติเกี่ยวกับการจัดทำ DPIA

แนวปฏิบัติฉบับนี้ได้ อ้างอิงหลักการจาก GDPR ในการจัดทำ DPIA ซึ่งกำหนดให้กระบวนการจัดทำจะต้องปฏิบัติตาม 4 ขั้นตอนต่อไปนี้เป็นอย่างน้อย

1. ธนาคารจะต้องทำการระบุรายละเอียดของกิจกรรมการประมวลผลอย่างเป็นระบบ อันได้แก่ กระบวนการหรือวิธีการประมวลผลข้อมูล วัตถุประสงค์ในการประมวลผลข้อมูล และประโยชน์อันชอบด้วยกฎหมายของธนาคาร
2. การประเมินความจำเป็นและสัดส่วนในการใช้ข้อมูลอย่างเหมาะสม ที่เกี่ยวข้องกับการประมวลผลตามวัตถุประสงค์
3. การประเมินความเสี่ยงที่อาจเกิดผลกระทบกับความเป็นส่วนตัว สิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
4. แนวทางในการจัดการกับความเสี่ยงที่อาจเกิดขึ้น รวมถึงมาตรการในการรักษาความปลอดภัยของข้อมูลที่เหมาะสมเพื่อให้แน่ใจว่าธนาคารมีการคุ้มครองสิทธิเสรีภาพและประโยชน์อันชอบธรรมของเจ้าของข้อมูลส่วนบุคคลหรือบุคคลอื่นที่มีความเสี่ยงที่จะได้รับผลกระทบ หากธนาคารพิจารณาแล้วว่าระดับของความเสี่ยงนั้นสูงเกินกว่าที่ธนาคารสามารถจัดให้มีมาตรการในการลดความเสี่ยงนั้นได้ ธนาคารควรพิจารณาไม่กระทำการประมวลผลข้อมูลส่วนบุคคลหรือปรึกษาคณะกรรมคุ้มครองข้อมูลส่วนบุคคลก่อน

การจัดทำ DPIA เป็นกระบวนการที่ธนาคารควรเริ่มจัดทำก่อนการทำการประมวลผลข้อมูล ละดำเนินการควบคู่ไปกับกระบวนการวางแผนและพัฒนา และทำอย่างต่อเนื่อง หากขั้นตอนในการจัดทำ DPIA มีความละเอียดและชัดเจน ก็จะเป็นการเพิ่มประสิทธิภาพและประสิทธิผลในการประมวลผลข้อมูลอย่างเหมาะสม ธนาคารอาจพิจารณาขั้นตอนในการจัดทำ DPIA เพิ่มเติมตามดังภาพด้านล่าง เพื่อใช้ในการจัดทำ DPIA ได้อย่างครอบคลุมยิ่งขึ้น

ในการพิจารณาการจัดทำ DPIA นั้นได้กำหนดให้จำเป็นต้องทำเมื่อมีกิจกรรมการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ซึ่งธนาคารสามารถพิจารณากิจกรรมการประมวลผลที่เข้าข่ายเป็นกิจกรรมที่มีความเสี่ยงสูงได้ ตามหลักการของ GDPR ดังต่อไปนี้

- Systematic and Extensive Profiling with Significant Effects การประมวลผลข้อมูลด้วยระบบอัตโนมัติ หรือ การทำ Profiling ที่อาจมีผลกระทบอย่างมีนัยสำคัญ
- Process Special Category or Criminal Offence Data on a Large Scale การประมวลผลข้อมูลที่มีความอ่อนไหว เช่น ข้อมูลประวัติอาชญากรรม ข้อมูลพฤติกรรมทางเพศ เป็นจำนวนมาก
- Systematically Monitor Publicly Accessible Places on a Large Scale ระบบการตรวจตราที่ใช้เฝ้าดูพื้นที่สาธารณะเป็นจำนวนมาก เช่น ศูนย์การค้า ห้องสมุด

กรอบในการพิจารณาที่จะช่วยในการตัดสินใจของธนาคารว่าในกรณีใดธนาคารมีความจำเป็นต้องทำ DPIA สามารถทำตามมาตรฐานสากลของ GDPR กำหนดให้หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลเข้าข่ายตามเกณฑ์ที่ระบุตั้งแต่ 2 ข้อขึ้นไป

s (GDPR vs PDPA) : Guidelines of the Bank of Thailand

1. (Evaluation or Scoring) เป็นกระบวนการทำโปรไฟล์หรือการประเมินผลหรือให้คะแนน โดยระบบอัตโนมัติ และการใช้ข้อมูลส่วนบุคคลเพื่อการคาดการณ์ (prediction) โดยเฉพาะเมื่อการประมวลผลนั้นมีความเกี่ยวข้องกับข้อมูลส่วนบุคคลเชิงลึก เช่น พฤติกรรม, ความชอบ, สุขภาพ, หรือ ตำแหน่งที่ตั้ง เป็นต้น
2. (Automated-Decision Making with Legal or Similar Significant Effect) หากกิจกรรมการประมวลผลข้อมูลส่วนบุคคลมีการใช้เทคโนโลยีเพื่อทำการตัดสินใจอัตโนมัติ ในเรื่องที่ส่งผลกระทบต่อกฎหมายหรือในเรื่องที่ส่งผลกระทบต่อบุคคลอย่างมีนัยสำคัญ เช่น อาจทำให้ถูกเลือกปฏิบัติ
3. (Systematic Monitoring) ระบบการประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้องกับ การติดตาม การสังเกต สอดส่อง หรือควบคุมบุคคล โดยเฉพาะในพื้นที่ที่บุคคลสาธารณะสามารถเข้าถึงได้ (Public Accessible Area) เช่น ระบบเฝ้าระวังหรือตรวจตราในพื้นที่สาธารณะ โดยที่บุคคลไม่อาจทราบถึงหรือไม่รู้ล่วงหน้าว่ามีกิจกรรมการประมวลผลนี้ หรือไม่ทราบว่ามีความควบคุมข้อมูลส่วนบุคคลเป็นใครและกำลังทำอะไรอยู่ ส่งผลให้เป็นการยากที่เจ้าของข้อมูลส่วนบุคคลจะสามารถหลีกเลี่ยง หรือ ปฏิเสธการมีส่วนร่วมได้
4. (Sensitive Data) เมื่อกิจกรรมการประมวลผลข้อมูลส่วนบุคคลนั้นเกี่ยวข้องกับข้อมูลอ่อนไหว เช่น เชื้อชาติ, เผ่าพันธุ์, ประวัติอาชญากรรม, ความเห็นทางการเมือง เป็นต้น (โปรดดูรายละเอียดเพิ่มเติมในหัวข้อ 5.4 ข้อมูลอ่อนไหว) เนื่องจากการประมวลผลข้อมูลดังกล่าว
5. (Data Processed on a Large Scale) หากการประมวลผลข้อมูลส่วนบุคคลนั้นเป็นการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก โดยพิจารณาจากจำนวนเจ้าของข้อมูลส่วนบุคคลที่เกี่ยวข้อง, ปริมาณข้อมูลหรือเนื้อหาของข้อมูลส่วนบุคคล, ระยะเวลาของกิจกรรมประมวลผล, และ ขอบเขตทางภูมิศาสตร์ของกิจกรรมการประมวลผล

6. (Datasets That Have Been Matched or Combined) ชุดข้อมูลที่เกิดเปรียบเทียบข้อมูลส่วนบุคคลที่มาจากแหล่งข้อมูลหลายแหล่ง ที่ประมวลผลข้อมูลต่างกัน ข้อมูลที่ถูกนำมารวมหรือเปรียบเทียบไม่จำเป็นต้องประมวลผลแล้ว และไม่จำกัดว่าแหล่งข้อมูลมาจากรธนาคารเองแต่อาจอื่นก็ได้ ซึ่งการทำเช่นนี้อาจทำให้การประมวลผลข้อมูลส่วนบุคคลนั้นได้มีการแจ้งเจ้าของข้อมูลส่วนบุคคลไว้ในตอนแรก อีกทั้งอาจไม่เป็นไปอย่างสมเหตุสมผลของเจ้าของข้อมูลส่วนบุคคลได้
7. (Data Concerning Vulnerable Data Subjects) หากองค์กรมีการบุคคลเกี่ยวกับผู้เปราะบาง (Vulnerable Person) เช่น ผู้เยาว์ ผู้ฉ้อพ ผู้สูงวัย GDPR ให้จัดว่ากิจกรรมการประมวลผลนั้นมีความเสี่ยงที่จะ

เจ้าของข้อมูลส่วนบุคคล เนื่องจากผู้เปราะบางอาจไม่อยู่ในสภาพที่สามารถให้ความยินยอมหรือปฏิเสธการประมวลผลข้อมูลส่วนบุคคลได้ รวมถึงการทำโปรไฟล์ข้อมูลของผู้เยาว์หรือการให้บริการออนไลน์แก่ผู้เยาว์โดยเฉพาะเพื่อวัตถุประสงค์การทำการตลาดแบบตรง

8. (Innovative Use or Applying Technological or Organizational Solutions) เมื่อมีการประมวลผลข้อมูลส่วนบุคคลซึ่งเกิดจากเทคโนโลยีใหม่ที่มีการใช้อย่างกว้างขวางในชีวิตประจำวันของเจ้าของข้อมูลส่วนบุคคล เช่น การ สแกนลายนิ้วมือ และใบหน้า ซึ่งอาจจะนำไปสู่ความเสี่ยงที่นอกเหนือความคาดหมายได้ เนื่องด้วยเทคโนโลยีดังกล่าวยังไม่เคยปรากฏหรือใช้มาก่อน ธนาคารจึงอาจไม่มีข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นได้ต่อเจ้าของข้อมูลส่วนบุคคล
9. (Data Transfer Across Borders) หากมีการโอนข้อมูลไปยังต่างประเทศ สามารถดูรายละเอียดเพิ่มเติมได้ที่หัวข้อ “6.2 การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศหรือองค์การระหว่างประเทศ” นอกจากธนาคารจะต้องพิจารณากฎหมายและมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางแล้ว ยังต้องพิจารณาถึงความเป็นไปได้ที่ข้อมูลนั้นอาจถูกส่งต่อด้วย
10. (Prevents Data Subjects from Exercising a Right or Using a Service or a Contract) หากกิจกรรมการประมวลผลนั้นอาจส่งผลให้เกิดการเปลี่ยนแปลงหรืออาจถูกปฏิเสธสิทธิของเจ้าของข้อมูล หรืออาจถูกปฏิเสธการได้รับบริการหรือการเข้าทำสัญญาของเจ้าของข้อมูล เช่น ธนาคารมีกระบวนการคัดกรองลูกค้า จากการประมวลผลข้อมูลของลูกค้ากับฐานข้อมูลของธนาคาร เพื่อตรวจสอบข้อมูลเครดิตและตัดสินใจว่าจะให้ลูกค้าเข้าทำสัญญาเงินกู้กับธนาคารหรือไม่

อย่างไรก็ตามในกรณีที่กิจกรรมประมวลผลข้อมูลนั้นเข้าข่ายตามเกณฑ์ที่ได้ระบุไว้มากกว่าสองข้อ ธนาคารสามารถเลือกที่จะไม่ทำ DPIA ได้ หากพิจารณาแล้วว่าการประมวลผลข้อมูลส่วนบุคคลนั้นจะไม่ส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงต่อเจ้าของข้อมูลส่วนบุคคล โดยธนาคารควรที่จะทำการปรึกษากับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลก่อนเพื่อพิจารณาถึงความเหมาะสม รวมถึงทำการจดบันทึกถึงเหตุผลที่ธนาคารใช้ในการตัดสินใจไม่ทำ DPIA หรือกรณีที่แม้เข้าข่ายเพียงหนึ่งข้อแต่อาจส่งผลกระทบที่ทำให้เกิดความเสี่ยงสูงกับเจ้าของข้อมูลส่วนบุคคล ธนาคารก็จำเป็นต้องจัดทำ DPIA

8. DPIA Quick Scan

8.1 Criteria-based test

8.1.1 Do you process personal data in order to evaluate individual persons, including the creation of "score values", "personal profiles" and predictions of the future behavior of that person? คุณได้มีการประมวลผลข้อมูลเพื่อประเมินบุคคล โดยเฉพาะรวมถึงการให้คะแนน หรือการทำ personal profile	This concerns in particular aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements.	<Select>	
8.1.2 Are there automated decisions made about individual persons that have a legal or similarly significant effect for these persons? มีการประมวลผลข้อมูลโดยใช้หุ่นยนต์หรือทำการตัดสินใจแบบautomateหรือไม่ และมีผลตามกฎหมาย	This is processing that aims at taking decisions on data subjects producing hat has "legal effects concerning a natural person" or which "similarly significantly affects" such a person. For example, if the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.	<Select>	
8.1.3 Are persons systematically monitored? คุณติดตามพฤติกรรมของบุคคลอย่างเป็นระบบ	This would be the case if there is personal data processed in order to observe, monitor or control data subjects, including data collected through networks or CCTV of a publicly accessible area.	<Select>	
8.1.4 Is there large-scale processing of sensitive data or data of a highly personal nature? ประมวลผลข้อมูล sensitive ขนาดใหญ่ ?	This includes special categories of personal data (health data, genetic and biometric data, data on racial or ethnic origin, data indicating religious or political beliefs and data on trade union membership) and data relating to criminal convictions or offences. Answer "yes" only if such data is processed	<Select>	

For Controllers (GDPR vs PDPA) : Quick Scan Tool

8.1.4 Is there large-scale processing of sensitive data or data of a highly personal nature? ประมวลผลข้อมูล sensitive ขนาดใหญ่ ?	This includes special categories of personal data (health data, genetic and biometric data, data on racial or ethnic origin, data indicating religious or political beliefs and data on trade union membership) and data relating to criminal convictions or offences. Answer "yes" only if such data is processed frequently and/or in relation to a large number of persons.	<Select>
8.1.5 Do you match or combine datasets about individual persons that were originally collected for other purposes? คุณเอาข้อมูลส่วนบุคคลที่เอามาจากระบบอื่น เอามาวิเคราะห์ประมวลผลเพื่อวัตถุประสงค์อย่างอื่นหรือไม่	This may be the case if you collect data from different sources in order to create personal profiles, or if you use "big data" about individual persons.	<Select>
8.1.6 Does the data processing relate to data subjects that need special protection? การประมวลผลข้อมูลเกี่ยวข้องกับเจ้าของข้อมูลที่ต้องการการคุ้มครองเป็นพิเศษหรือไม่	This is the case if there is a strong power imbalance between the data subjects and the data controller. Answer "yes" in particular if the data subjects may be intimidated and may therefore refrain from using their individual rights. Data subjects requiring protection may include children, employees, mentally ill persons, asylum seekers, elderly persons, patients, etc.	<Select>
8.1.7 Does the data processing use a new technology or an innovative organizational solution that may have additional implications for the privacy of individual persons? ใช้เทคโนโลยีหรือนวัตกรรมใหม่ ซึ่งอาจจะมีผลกระทบต่อความเป็นส่วนตัวของข้อมูล	Answer "yes" if the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Example: Combining use of a fingerprint and face recognition for improved physical access	<Select>

8.2 The blacklist test	8.1.7 Does the data processing use a new technology or an innovative organizational solution that may have additional implications for the privacy of individual persons? ใช้เทคโนโลยีหรือนวัตกรรมใหม่ ซึ่งอาจจะมีผลกระทบต่อความเป็นส่วนตัวของข้อมูล	Answer "yes" if the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Example: Combining use of a fingerprint and face recognition for improved physical access control.	<Select>	
	8.1.8 Is the data processing intended to prevent individual persons from exercising a right or using a service or a contract? การประมวลผลข้อมูลมีเจตนาที่จะป้องกันมิให้บุคคลใช้สิทธิ์หรือบริการหรือสัญญา หรือไม่	This includes processing operations that aim at allowing, modifying or refusing data subjects' access to a service or entry into a contract.	<Select>	
	8.2.1 Is there, on a large scale, processing of personal data that is subject to a professional or official secrecy obligation? มีอาชีพเป็นหมอนายความ หรือไม่	Professional secrecy obligations pertain to, inter alia, physicians, lawyers, therapists and persons belonging to the cleric if the receive secrets. Answer "yes" only if such data is processed either frequently and/or in relation to a large number of persons.	<Select>	
	8.2.2 Is there processing, on a large scale, of information on the behaviour of employees which can be used to assess their work in such a way as to have legal or other significant consequences for them? มีการประมวลผลข้อมูลขนาดใหญ่เกี่ยวกับพฤติกรรมของลูกจ้าง	This includes the use of large scale data loss prevention systems that monitor network activity or other activity of the employees.	<Select>	
	8.2.3 Is there a consolidation of personal data from various sources and further processing of the data thus consolidated, provided that the aggregation or processing is carried out on a large scale? มีการเก็บรวบรวมจากหลายแหล่งและเอามารวมกันหรือไม่	This is the case if the data is processed for purposes for which not all of the data was originally collected, if the data processing includes the use of algorithms that are incomprehensible to the persons concerned, and the data processing is intended to discover previously unknown connections between the data	<Select>	

	8.2.2 Is there processing, on a large scale, of information on the behaviour of employees which can be used to assess their work in such a way as to have legal or other significant consequences for them? มีการประมวลผลข้อมูลขนาดใหญ่เกี่ยวกับพฤติกรรมของลูกจ้าง	This includes the use of large scale data loss prevention systems that monitor network activity or other activity of the employees.	<Select>	
	8.2.3 Is there a consolidation of personal data from various sources and further processing of the data thus consolidated, provided that the aggregation or processing is carried out on a large scale? มีการเก็บรวบรวมจากหลายแหล่งและเอามารวมกันหรือ?	This is the case if the data is processed for purposes for which not all of the data was originally collected, if the data processing includes the use of algorithms that are incomprehensible to the persons concerned, and the data processing is intended to discover previously unknown connections between the data for purposes that are not predetermined This may include big data analysis of customer data enriched with information from third parties, or fraud prevention systems.	<Select>	
	8.2.4 Is there a collection of personal data via interfaces of personal electronic devices, which are not protected against unauthorised readout, which the persons concerned cannot recognise? มีการเก็บข้อมูลส่วนบุคคลจากอุปกรณ์อิเล็กทรอนิกส์	For example collecting personal data via RFID/NFC through apps or cards.	<Select>	
	8.2.5 Is there the creation of comprehensive profiles on the movement and purchasing behaviour of affected persons? มีการเก็บรวบรวมประมวลเกี่ยวกับการเคลื่อนย้ายหรือพฤติกรรมการซื้อขายของที่มีผลต่อบุคคล?	For example the recording of the purchasing behaviour of different groups of people for profile building and customer retention.	<Select>	
***ควรจะทำรายการในทั้งสองแบบ หากว่าคำตอบของท่านเป็น ใช่ถึง 2 ข้อใน 8.1 หรือ เพียงข้อเดียวใน 8.2 โปรดหารือผู้รับผิดชอบ หรือ DPIA Team เพื่อทำการวิเคราะห์ผลกระทบ DPIA โดยหารือ DPO ***				



Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Source:
<https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf>

[PUBLICATIONS](#) | [GLOSSARY](#) | [FR](#) - [EN](#) | [COOKIES MANAGEMENT](#)

CNIL.

To protect personal data, support innovation, preserve individual liberties

[MY COMPLIANCE TOOLS](#) | [DATA PROTECTION](#) | [TOPICS](#) | [THE CNIL](#) |  

 > The open source PIA software helps to carry out data protection impact assessment



The open source PIA software helps to carry out data protection impact assessment

30 June 2021

The PIA software aims to help data controllers build and demonstrate compliance to the GDPR. The tool is available in French and in English. It facilitates carrying out a data protection impact assessment, which will become mandatory for some

DPIA

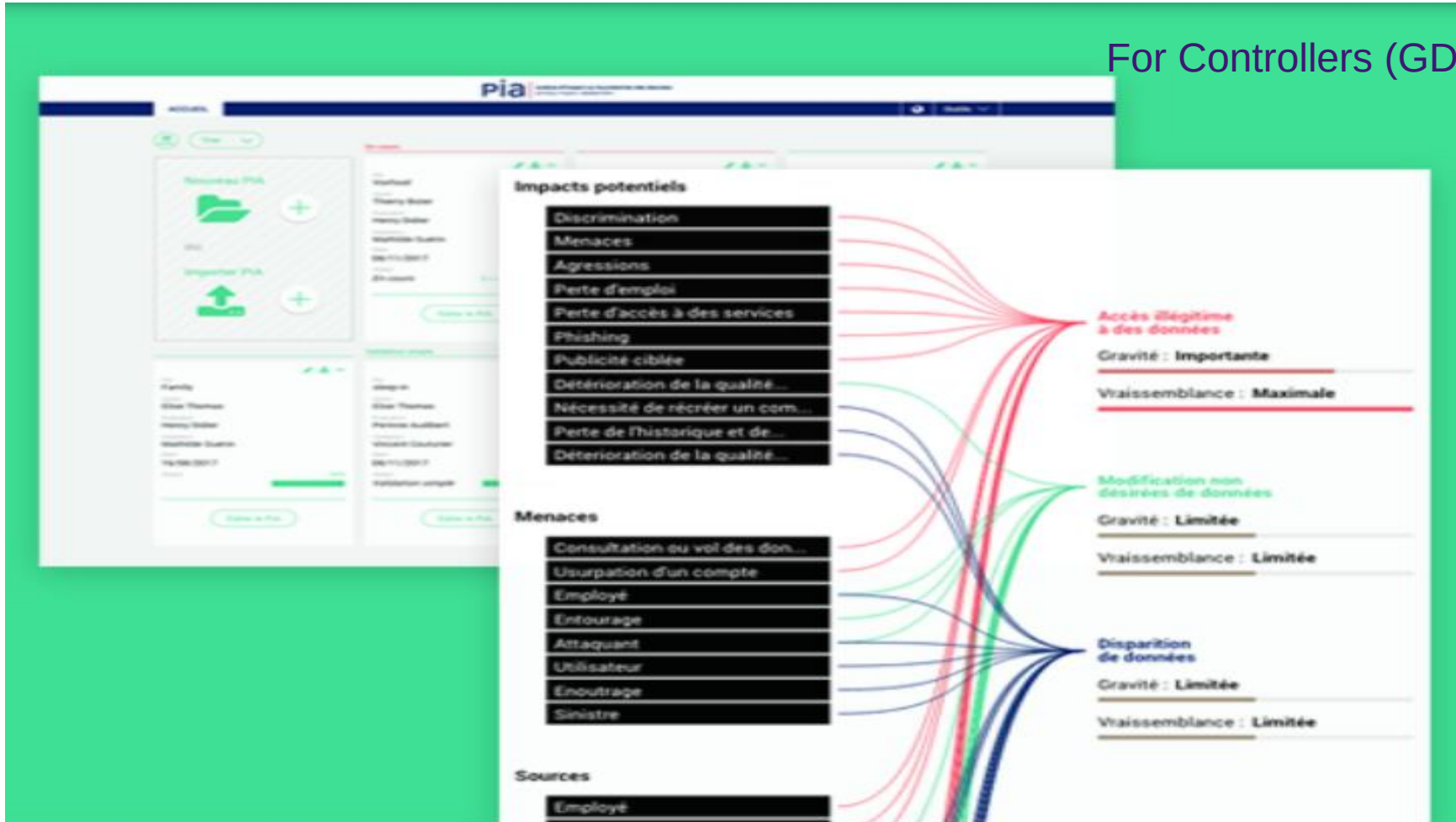
PDPA) : Quick Scan Tool



Source: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

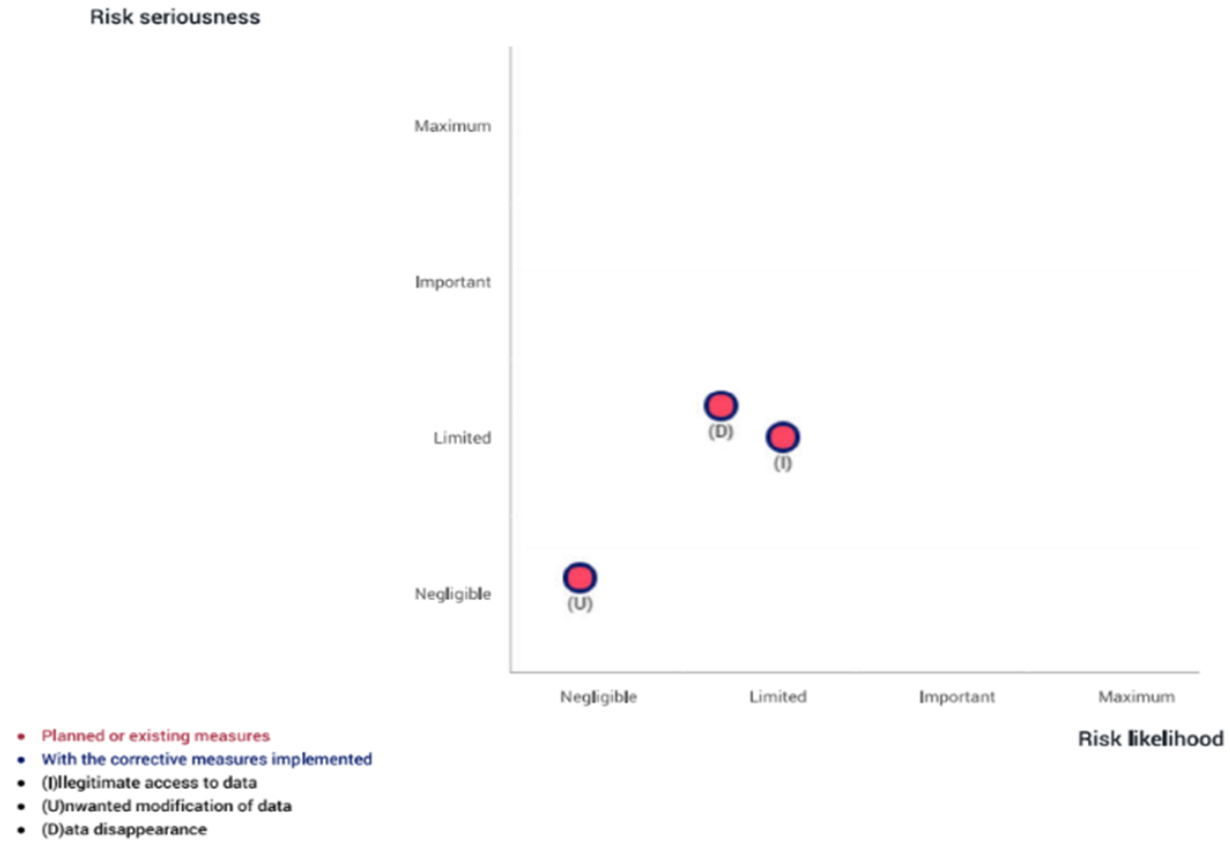
DPIA

For Controllers (GDPR vs PDPA) : Quick Scan Tool



Source: <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

Risk mapping





**KEEP
CALM
AND
GET READY FOR
PDPA**