태국 개인정보보호 법 행정 체계 현황 및 주요 위반사례

1. 법률체계

▶ 개요

- 태국 개인정보보호의 법적 근거는 ▲헌법 ▲개인정보보호법 ▲그 외 관련 법령 등 크게 세 가지의 법령을 바탕으로 함

▶ 헌법(รัฐธรรมนูญแห่งราชอาณาจักรไทย)

- 태국 헌법은 사생활을 보호받을 권리와 함께 개인정보를 보호하기 위한 명시적인 규정을 두고 있음
  - 헌법 제32조는 '개인은 마땅히 사생활과 존엄성, 명예 및 가족에 대한 권리가 있다. 상기 개인의 권리를 침해하거나 영향을 미치는 행위, 또는 개인정보를 이용하는 행위는 공익을 위해 필요한 경우 법률에 근거한 것이 아닌 한 그 방법을 불문하고 허용되지 않는다'고 규정함으로써 헌법에서 개인정보의 무단 이용을 명시적으로 금지[1)]

▶ 개인정보보호법(พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒, 영문명 Personal Data Protection Act B.E. 2562, 이하 PDPA)

- PDPA는 '19년 제정된 개인정보보호를 목적으로 하는 최초의 일반법으로 '22년 6월부터 시행 중
  - PDPA는 당초 관보 게재일인 '19년 5월 27일부터 1년이 지난 시점인 '20년 5월 27일 시행 예정이었으나 두 차례에 걸쳐 연기된 후 '22년 6월 1일 시행에 돌입
- 동법은 EU 일반 개인정보보호법(General Data Protection Regulation, 이하 GDPR)을 모델로 함으로써 GDPR과 많은 유사성을 보임
  - PDPA는 ▲정보주체, 컨트롤러 및 프로세서 등의 용어 사용 ▲열람권, 삭제권, 정정권 등 정보주체의 다양한 권리 보장 ▲처리 기록 보관, 개인정보 영향평가, DPO 지정과 같은 GDPR과 동일한 컨트롤러 의무 부과 등 GDPR과의 유사성이 매우 높음
- 한편, PDPA는 총 7장 96개 조항으로 이루어져 있으며, ▲개인정보 감독기관(제1장) ▲개인정보보호(제2장) ▲정보주체의 권리(제3장) ▲개인정보 감독기관 사무국(제4장) ▲청원(제5장) ▲민사책임(제6장) ▲벌칙(제7장) 등으로 구성

1) https://ilaw.or.th/node/5481

- 한편, 특정 정부 기관이 개인정보를 요청할 때, 컨트롤러의 PDPA 제2장(개인정보보호), 제3장(정보 주체의 권리)에 규정된 준수 의무를 면제하는 법령이 '24년 1월부터 시행됨
- 또한, PDPC 위원회의 외국 또는 국제기구의 개인정보 보호 수준이 적절한지 평가하는 제28조에서 규정된 절차를 구체화한 고시(ประกาศ)가 '24년 3월부터 시행되었고, PDPA 제29조 제1항과 관련한 '구속력 있는 기업 규칙'과 제29조 제3항에서 규정된 '적절한 보호 조치'를 구체화한 고시가 '24년 3월부터 시행됨
- 나아가, 제33조에 규정된 삭제권의 내용을 구체화하는 고시가 '24년 11월부터 시행 예정

▶ 그 외 관련 법령

- **신용정보사업법(พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต, 영문명 Credit Information Business Act, B.E. 2545)**
  - 신용정보 또는 대출 신청 고객에 대한 특정한 개인정보보호를 보장하는 법률로 '02년 제정
  - 신용정보(credit information)란 신용을 신청하는 고객에 관한 정보를 의미 (제3조)
    · 고객이 자연인일 경우 이름, 주소, 생년월일, 혼인상태, 직업, 공무원증번호, 여권, 납세자번호 등이 이에 해당하고, 고객이 법인인 경우 주소, 법인등록번호, 납세자번호 등이 여기에 포함
  - 신용정보업을 영위하는 신용정보회사는 신체장애, 유전자, 범죄수사 또는 형사소송이 진행 중인 자에 관한 정보 등을 저장해서는 안 됨 (제10조)
  - 태국 내에서 사업을 수행하는 신용정보회사 등은 태국 밖에서 개인정보를 이용, 제어, 처리할 수 없음 (제12조)
  - 동법 제10조 및 제12조를 위반하는 신용회사 등은 5년 이상 10년 이하의 징역 또는/및 50만 바트(약 1,850만 원) 이하의 벌금에 처함 (제44조)

- **국민보건법(พระราชบัญญัติสุขภาพแห งชาติ , 영문명 National Health Act, B.E. 2550)**
  - 태국 국민의 건강증진 및 질병예방과 함께 국민의 건강정보를 보호하기 위해 '07년 제정된 법률
  - 개인의 건강정보는 비밀로 유지되어야 하며, 본인의 의사가 있거나 또는 특정 법률에서 요구하지 않는 한 해당 본인에게 손해를 입힐 수 있는 방법으로 공개해서는 안 됨 (제7조)
  - 공중보건의가 서비스 수혜자를 연구 대상자로 활용하고자 하는 경우, 사전에 서비스 수혜자에게 그 사실을 알리고 서면으로 동의를 받은 후 실험을 수행해야 하며, 이러한 동의는 언제든지 철회될 수 있음 (제9조)
  - 제7조 또는 제9조를 위반하는 자는 6개월 이하의 징역 또는/및 1만 바트(약 37만 원) 이하의 벌금에 처함 (제49조)

2. 행정체계

Ⅰ. 개요

▶ **태국의 개인정보 감독기관은 Office of the Personal Data Protection Commission (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล, 이하 PDPC)로 수도 방콕에 소재**

<PDPC 로고>

- **(규모)** '23년 예산 80,436,200바트(약 29억 원), 직원 수 49명
- **(담당 업무)** 개인정보보호 및 개인정보보호에 관한 국가의 발전 장려와 지원 담당 (제43조)
- **(독립성 여부)** PDPC는 디지털경제사회부 산하 정부기관(government agency)으로서 비독립적인 조직에 해당
  - (예산) PDPC는 정부로부터 보조금을 받는 등 예산을 보유 및 운용하지만 (제46조), 해당 조직의 사무국은 예산 및 회계 처리 결과를 디지털경제사회부 사무차관이 위원으로 소속되어 있는 사무국 감독위원회에 제출하도록 규정하고 있어 (제68조 및 제69조) 정부부처로부터 예산 관련 독립성이 낮음
  - (인사) 기관 최고의결기구인 위원회의 위원장은 개인정보보호 분야의 전문가 중 선정하여 임명하지만 (제8조제1항), 부위원장은 디지털경제사회부 사무차관이, 위원회 위원은 당연직 상임위원으로서 총 5인의 정부인사에 할당되어 있어 (제8조제2항 및 제3항) 정부부처에 대한 예속성이 강함
  - (집행) PDPA 제14조는 위원회 회의의 결정에 관해 위원 1인 1표의 다수결 원칙을 규정하고 있는데, 전체 14인의 위원(상임위원 5인 및 전문위원 9인) 중 정부인사가 상당한 비율을 차지함에 따라 PDPC의 위원회가 집행 권한 행사에 있어 완전한 독립성을 확보하는 데에는 한계 존재

- **(조직)**
  - (위원장) 티엔차이 나 나콘(Thienchai Na Nakorn) ('22.1.~현재)
    · 위원장은 국가 정책에 부합하는 개인정보보호 관련 기본 계획 등을 수립하는 책임자로서, 임기 4년에 재임이 가능하나 2회를 초과하여 연임하지는 못함 (제12조)
  - (사무국장) 시와락 시와목사탐(Siwarak Siwamoksatham) ('22.10.~현재)
    · 사무국장은 감독기관 행정업무에 대한 실질적인 총괄책임자로, 임기 4년에 재임이 가능하나 2회를 초과하여 연임하지는 못함 (제60조)
  - (구성) ▲위원회 ▲사무국 ▲사무국 감독위원회 ▲전문가위원회 등으로 조직
  - (담당 법령) PDPA
  - (주소) เลขที่ 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
  - (전화번호) +66 2-142-1033, +66 2-141-6993

Ⅱ. 감독기구의 개인정보 보호 고유 업무 외의 수행 업무 (개인정보 활용, 교육 사업, 예산 지원 프로그램 등)

- PDPC는 디지털경제사회부의 정책에 기반하여 개인정보보호 업무를 수행하는 데에 국한

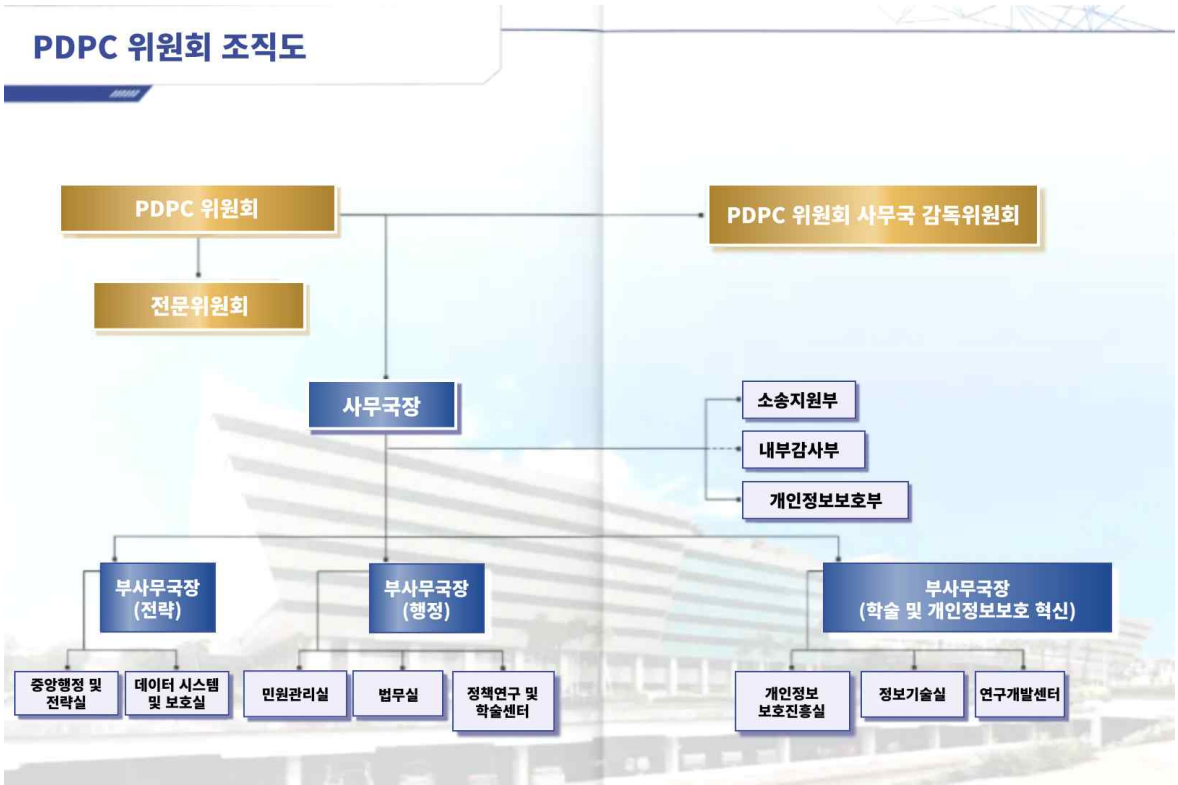
Ⅲ. 상세조직

▶ PDPC는 실질적인 감독행정을 총괄하는 사무국을 중심으로, 최고의결기구인 위원회, 사무국을 감독하는 사무국 감독위원회, 분야별 전문성 강화를 위한 전문가위원회 등으로 구성

- (사무국) 국가 전반의 개인정보보호 촉진 및 지원을 위해 위원회 등에 대한 행정업무를 책임지며, 이외에 아래의 업무를 수행
  - 국가 정책, 국가 전략 및 국가 계획 내에서 개인정보의 증진 및 보호를 위한 기본계획 초안 작성
  - 개인정보보호와 관련된 기술개발을 위한 연구 촉진 및 지원
  - 개인정보보호와 관련된 표준 또는 감독 메커니즘의 정확성 분석 및 검증
  - 개인정보보호 관련 조사 수행, 정보 수집, 최신 업데이트 수행과 함께, 국가 발전에 영향을 미치는 개인정보보호 문제에 대한 분석 및 연구 등을 수행하여 위원회에 제안
  - 개인정보보호와 관련하여 공공부문, 국영기업, 지방자치단체, 공공단체 또는 기타 조직과의 가교 역할 수행
  - 정부기관 및 민간기관에 PDPA 관련 자문 제공
  - 개인정보보호에 관한 지식과 이해를 증진하는 것을 포함하여, 정부기관, 민간기관, 국민 등에게 개인정보보호 관련 학술서비스 및 교육 제공
  - 컨트롤러, 프로세서, DPO 등의 업무 수행을 지원하기 위한 교육 제공
  - 사무국의 운영과 관련하여 국내외 단체 또는 기관과의 협약 체결 및 협력 수행
  - PDPA 준수 여부에 대한 후속 조치 및 평가 수행
- 사무국장 산하에 소송지원부, 내부감사부, 개인정보보호부가 있고, 부사무국장(전략 담당) 산하에 중앙행정·전략실, 데이터시스템 및 보호실, 부사무국장(행정 담당) 산하에 민원관리실, 법무실, 정책연구 및 학술센터, 부사무국장(학술 및 개인정보보호 혁신 담당) 산하에 개인정보보호진흥실, 정보기술실, 연구개발센터가 있음
- (위원회) 위원장, 디지털경제사회부 사무차관, 5인의 정부 고위관료, 개인정보보호·소비자보호·정보통신·사회·법률·보건·재정 등에 전문성을 갖춘 9인의 전문가, 사무국장으로 구성되어 있으며 아래의 직무를 수행 (제8조, 제16조)
  - 개인정보보호를 촉진하기 위한 기본계획을 수립하여 국가디지털경제사회위원회(National Digital Economy and Society Commission)에 제안
  - 해당 기본계획에 따른 정부기관 및 민간 부문의 개인정보보호 지원, 개인정보보호 기본계획의 운영에 대한 결과평가 수행

- PDPA를 준수하기 위해 개인정보보호와 관련된 실행 기준 및 지침 결정
- PDPA 시행을 위한 고시 및 규칙 제정
- 개인정보 국외이전과 관련한 규정 발표
- 컨트롤러와 프로세서가 준수해야 하는 지침으로서 개인정보보호 실행 기준 발표
- 내각에 개인정보보호 관련 기존 법률 또는 규칙의 제정·개정에 관해 건의하거나 그 적합성에 대한 재검토 권고
- PDPA 시행과 관련, 정부기관 및 민간 부문의 개인정보보호에 대한 자문 제공
- PDPA 시행과 관련하여 발생하는 문제에 대한 해석 및 결정
- 국민의 개인정보보호 관련 인식 제고 및 교육 지원
- 개인정보보호 관련 기술에 대한 연구 개발 촉진 및 지원

< PDPC 위원회 구성 >



출처 : PDPC '23년 연례보고서[2)]

- (기타) 조직 내부의 감독 기능과 조직의 전문성 강화를 위해 사무국 감독위원회와 전문가위원회를 둠

2) https://www.pdpc.or.th/pdpc-book/anual-report-2566/

구분	담당 업무
사무국 감독위원회 (제54조)	• 위원장, 상임위원 2인, 전문위원 6인으로 구성되어 있으며, 아래의 권한과 의무를 가짐 - 사무국의 운영 정책 및 운영 계획 승인 - 조직, 재정, 인사, 일반행정, 내부감사에 관한 규칙 제정 - 사무국의 연도별 운영계획, 지출계획, 예산 등 승인 - 사무국의 행정 및 운영이 동법 및 그 밖의 관계법령을 준수하도록 감독 - 사무국장 선정을 위한 선정위원회 구성 - 사무국장의 행정명령에 대한 이의신청 제기 시 해당 사항 결정 - 사무국의 운영 결과 및 사무국장의 업무 성과 평가
전문가위원회 (제72조)	• 위원회는 각 사안의 전문성 또는 위원회가 적절하다고 판단하는 바에 따라 하나 또는 복수의 전문가위원회를 구성 (제71조) • 전문가위원회는 아래의 직무를 수행 - PDPA에 따라 제기된 민원 검토 - 정보주체에 피해를 입히는 컨트롤러 또는 프로세서에 대한 조사 - 개인정보와 관련된 분쟁 해결

3. 개인정보 처리자 의무사항

Ⅰ. 데이터 컨트롤러

▶ (정보주체 권리강화) PDPA는 제30조~제36조에서 정보주체의 권리 조항을 두고 있으며, 정보를 제공받을 권리 및 정정권의 경우 간접적인 형태로 규정되어 있는 것이 특징

- PDPA는 열람권, 삭제권, 처리제한권, 반대권, 이동권 등 정보주체의 여러 권리를 명시적이면서도 매우 상세하게 규정
- 정보를 제공받을 권리와 관련한 내용은 동법 제30조 이하가 아닌 제23조 및 제25조에서 규정하고 있으며, 정보주체의 직접적인 권리가 아닌 컨트롤러의 의무사항으로 규정하여 정보주체가 해당 권리를 간접적으로 향유할 수 있도록 보장
- 정정권의 경우에도 직접적으로 규정되어 있지 않은 대신, 컨트롤러에 본인의 개인정보를 정확하고도 최신 상태를 유지하도록 요구할 수 있도록 함으로써 정정권과 유사한 권리를 행사할 수 있도록 함

< 정보주체 권리강화 규정 >

조항 및 권리	의무사항 세부 내용
제23조, 제25조 정보를 제공받을 권리	• 정보주체는 아래의 정보를 제공받을 권리가 있음(제23조 및 제25조제2항) - 정보주체의 동의 없이 허용된 목적을 포함하여 개인정보의 이용 또는 제공을 위한 수집 목적 - 정보주체가 법적 의무를 준수하기 위해 또는 계약 이행을 위해 개인정보가 필요한 사례에 대한 통지, 또는 계약체결을 위해 개인정보를 제공해야 하는 사례에 대한 통지(정보주체가 그러한 개인정보를 제공하지 않는 경우에 발생할 수 있는 효과 포함) - 수집할 개인정보와 개인정보 보유기간(보유기간을 지정할 수 없는 경우 개인정보 보유 기준에 따라 예상되는 기간을 명시) - 수집된 개인정보가 제공될 수 있는 개인이나 단체의 유형 - 컨트롤러(또는 컨트롤러의 대리인 혹은 DPO)의 정보와 주소, 상세한 연락처 정보 - PDPA에 따른 정보주체의 권리 • 컨트롤러는 정보주체로부터 개인정보를 수집하는 경우 수집 전, 또는 수집 시에 정보주체에게 해당 사실을 알려야 함(제23조) • 개인정보가 다른 출처에서 수집되는 경우 컨트롤러는 해당 개인정보 수집일로부터 30일 이내에 지체 없이 정보주체에게 해당 사실을 알려야 함(제25조제1항제2호, 제25조제3항) - 단, 컨트롤러가 개인정보를 정보주체와의 커뮤니케이션에 이용하는 경우에는 최초 커뮤니케이션 시 해당 정보를 제공해야 하며, 다른 사람에게 제공할 예정인 경우 첫 번째 제공이 발생하기 전에 해당 사실을 정보주체에게 알려야 함(제25조제3항)

▶ (컨트롤러 의무사항) PDPA는 제37조 이하에서 컨트롤러의 기타 의무사항을 규정

• PDPA는 ▲처리활동 기록 ▲DPO 지정 ▲보안조치 의무 등 컨트롤러 의무사항을 명시
  - PDPA는 컨트롤러에 일반적인 개인정보 영향평가 의무는 부과하지 않지만, 보안 조치 과정에서 신기술을 도입하는 경우 등 기타 필요에 따라서는 해당 보안 조치가 적절한지 여부에 대한 검토를 필수적으로 요구

3) https://www.tilleke.com/insights/thailand-issues-criteria-for-deletion-destruction-and-de-identification-of-personal-data/27/
4) 원문으로는 'ตัวระบุทางตรง'

조항 및 권리	의무사항 세부 내용
제30조 열람권	• 정보주체는 자신과 관련된 개인정보에 대해 열람하고 사본을 요청하거나 동의 없이 획득한 개인정보의 제공을 요청할 수 있음 • 정보주체가 동법 제30조에 따라 개인정보 열람을 요청하고 특별한 거부 사유가 없는 경우, 컨트롤러는 지체 없이 열람 요청을 이행해야 하며 그러한 요청을 받은 날로부터 30일을 초과할 수 없음
정정권	• PDPA는 정정권을 명시적으로 부여하지 않지만, 동법 제35조 및 제36조는 정확하지 않거나 오래된 개인정보를 바로잡을 수 있도록 하는 정보주체의 권리를 규정 - 컨트롤러는 개인정보가 정확하고, 최신 상태를 유지하고, 완전하며 오해의 소지가 없는 상태로 두어야 함 (제35조) - 정보주체가 컨트롤러에 동법 제35조에 따라 행동하도록 요청하였으나 컨트롤러가 정보주체의 요청에 대해 조치를 취하지 않는 경우 컨트롤러는 동법 제39조에 따라 해당 정보주체의 요청을 사유와 함께 기록해야 함 (제36조제1항) - 동법 제34조제2항에 따라 컨트롤러가 조치를 취하지 않는 경우 정보주체는 PDPA 제5장(청원)에 명시된 규정에 따라 임명된 전문가 위원회에 민원을 제기하여 컨트롤러로 하여금 조치를 취하게 할 권리를 보유 (제36조제2항)
제33조 삭제권	• 정보주체는 아래의 경우 개인정보의 삭제, 파기 또는 익명화를 요청할 수 있음 - 개인정보 수집, 이용 또는 제공 목적과 관련하여 더 이상 개인정보가 필요하지 않은 경우 - 정보주체가 개인정보 수집, 이용 또는 제공의 근거가 되는 동의를 철회하여 컨트롤러가 그러한 수집, 이용 또는 제공에 법적 근거가 없는 경우 - 정보주체가 개인정보 수집, 이용 또는 제공에 반대하는 경우 - 개인정보가 불법적으로 수집, 이용 또는 제공된 경우 • 컨트롤러가 공개한 개인정보를 삭제하도록 요청받거나 혹은 익명화하도록 요청받은 경우, 컨트롤러는 그러한 요청 관련 이행 조치에 대한 응답을 얻기 위해 다른 컨트롤러에 알리는 조치를 취해야 함 • 컨트롤러가 동법 제33조에 따른 삭제요청에 대해 조치를 취하지 않은 경우 정보주체는 전문가위원회에 민원을 제기하여 컨트롤러가 그러한 조치를 취하도록 요구할 권리가 있음 • 한편, 제33조에 규정된 삭제권의 내용을 구체화하는 고시가 '24년 11월부터 시행 예정임[3] - 정보주체가 컨트롤러에게 개인정보의 삭제, 파기 또는 정보주체를

조항 및 권리	의무사항 세부 내용
	식별할 수 없도록 할 것을 요청한 경우, 컨트롤러는 지체 없이, 그러나 요청을 받은 날로부터 60일을 초과하지 않는 범위 내에서 처리하여야 함 - 위 삭제, 파기 또는 정보주체를 식별할 수 없도록 하는 대상은 복사 또는 백업된 개인정보(있는 경우에 해당)도 포함하여야 하며, 합리적으로 예상 가능한 어떠한 방법을 사용하여 누구도 개인정보를 복구하거나 해당 정보를 직간접적으로 정보주체를 식별할 수 있는 상태로 되돌릴 수 없도록 해야 함 - 개인정보의 삭제, 파기 또는 비식별화를 즉시 수행할 수 없는 경우(예를 들어, 기술적 이유로 전자형태의 개인정보가 다른 개인정보로 덮어쓰기 되거나 대체될 때까지 일시적으로 저장되는 경우), 컨트롤러는 해당 개인정보의 수집, 사용 또는 공개가 어렵게 조치를 취해야 함 - 개인정보를 비식별화 하거나 익명화할 때, 컨트롤러는 ▲정보주체의 직접 식별자(direct identifiers[4])를 삭제하거나 제거하는 과정(비식별화)을 거쳐야 하고, ▲위 비식별화 후 해당 정보가 간접적으로도 정보주체를 식별할 수 없도록 추가 조치를 고려해야 하며, 정보주체를 식별할 위험이 충분히 낮은 수준이어야 함 - 컨트롤러가 정보주체의 권리행사 요청에 따라 개인정보를 삭제, 파기 또는 비식별화한 경우, 컨트롤러는 그 권리를 행사한 정보주체에게 이를 통지하여야 함
제34조 처리제한권	• 정보주체는 아래의 경우 개인정보 처리 제한을 요청할 수 있음 - 컨트롤러가 동법 제36조에 따른 정보주체의 요청에 대해 조사 절차를 보류하는 경우 - 동법 제33조제1항제4호에 따라 삭제되거나 파기되어야 하는 개인정보에 대해 정보주체가 사용 제한을 요청하는 경우 - 개인정보 수집의 목적을 위해 해당 개인정보를 더 이상 보유할 필요가 없지만, 정보주체가 법적 권리의 입증, 준수, 행사 또는 방어를 위해 보유 기간의 연장을 요청할 필요가 있는 경우 - 컨트롤러가 정보주체의 개인정보 수집, 이용, 제공에 관한 이의제기를 거부하기 위해 동법 제32조와 관련하여 입증 혹은 조사를 보류 중인 경우 • 정보주체는 컨트롤러가 제34조제1항에 따라 처리제한 요청에 대해 조치를 취하지 않은 경우 컨트롤러가 그러한 조치를 취하도록 하기 위해 전문가위원회에 민원을 제기할 권리를 가짐(제34조)
제32조 반대권	• 정보주체는 아래의 경우 개인정보의 수집, 이용 또는 제공에 반대할 권리가 있음 - 동법 제24조제4항 또는 제24조제5항에 따라 동의 요건을 면제받아

조항 및 권리	의무사항 세부 내용
	개인정보를 수집하였으나, 컨트롤러가 그러한 개인정보의 수집, 이용 또는 제공에 대해 설득력 있는 정당한 근거가 있음을 입증할 수 없거나 법적 권리의 입증, 준수, 행사, 또는 방어를 위해 처리된다고 증명할 수 없는 경우 - 직접 마케팅을 위해 개인정보를 수집, 이용 또는 제공하는 경우 - 과학적, 역사적 또는 통계적 연구를 위해 개인정보를 수집, 이용 또는 제공하는 경우. 단, 컨트롤러가 공익상의 이유로 업무를 수행할 필요가 있는 경우는 제외 • 정보주체가 반대권을 행사하는 경우 컨트롤러는 관련 개인정보를 즉시 구별하고, 해당 개인정보의 수집, 이용 또는 제공을 중지해야 함
제31조 이동권	• 정보주체는 개인정보를 타 컨트롤러로 이전 요청할 수 있는 권리를 가지며, 이와 관련하여 정보주체가 가지는 권리는 아래와 같음 - 자동화된 방식으로 수행할 수 있는 경우 컨트롤러로 하여금 이러한 형식의 개인정보를 다른 컨트롤러에 전송하거나 이전을 요청할 수 있는 권리 - 기술적인 상황으로 인해 개인정보 전송이나 이전이 불가능한 경우를 제외하고 컨트롤러가 다른 컨트롤러에 전송이나 이전하는 형식으로 자신이 개인정보를 직접 얻을 수 있는 권리 • 이동권은 ▲정보주체가 개인정보 수집, 이용 또는 제공에 동의한 개인정보 ▲동법 제24조제3항에 따른 동의 요건에서 면제되는 개인정보 ▲PDPC 위원회가 동법 제24조에 따라 별도 규정한 기타 개인정보에 한정하여 행사가 가능 • 컨트롤러는 개인정보를 자동화된 도구 또는 장비를 통해 읽을 수 있거나 일반적으로 사용되는 형식으로 배열하고 자동화된 방식으로 이용 및 공개되도록 구성해야 함

조항	의무사항 세부 내용
제37조 제1호~제3호 보안 조치	• 컨트롤러는 아래와 같은 보안 조치 의무를 짐 - 개인정보의 무단 열람, 이용, 변경, 수정, 손실 및 공개를 방지하기 위해 보안조치(PDPC 위원회에서 규정한 최소 기준 포함)를 설정해야 함 - 개인정보를 제3의 개인 또는 법인에게 제공해야 하는 경우, 개인정보를 불법적으로 또는 허가 없이 이용하거나 공개하는 것을 방지하기 위한 조치를 취해야 함 - 보유 기간 종료, 개인정보 수집 목적 초과, 정보주체의 요청, 정보주체의 동의 철회 등의 사유가 있을 경우에 대비해 개인정보의 삭제 또는 파기를 위한 검사 시스템을 구비해야 함

조항	의무사항 세부 내용
제37조 제1호 보안 조치 검토	• 컨트롤러는 필요한 경우 또는 상기 보안조치 기술에 변경이 발생한 경우 보안 조치에 대한 검토를 수행해야 함
제39조 처리 활동의 기록	• 컨트롤러는 정보주체와 PDPC 사무국이 확인할 수 있도록 서면 또는 전자 형식으로 최소한 아래의 기록을 유지 관리해야 함 - 수집된 개인정보 - 개인정보 유형별 수집 목적 - 컨트롤러의 세부사항 - 개인정보의 보유 기간 - 개인정보를 열람할 수 있는 권한이 있는 사람에 관한 요건 및 해당 개인정보를 열람할 수 있는 요건을 포함하여 개인정보를 열람할 수 있는 권리 및 방법 - 동법 제27조제3항에 따른 개인정보 이용 또는 제공 - 동법 제30조제3항, 제31조제3항, 제32조제3항, 제36조제1항에 따른 요청 거부 또는 이의 제기 - 동법 제37조제1항에 따른 적절한 보안 조치의 세부사항
제41조 DPO 지정	• 컨트롤러는 다음의 경우 DPO를 지정해야 함 - 컨트롤러가 PDPC 위원회가 지정한 공공기관인 경우 - 개인정보의 수집, 이용 또는 제공과 관련하여 컨트롤러의 활동이 개인정보 또는 시스템에 대한 대규모의 정기적인 모니터링을 요하는 경우 - 컨트롤러의 핵심 활동이 개인정보의 수집, 이용 또는 제공인 경우 • 컨트롤러는 DPO의 정보, 연락처 주소 및 연락처를 정보주체와 PDPC 사무국에 제공해야 함 • 또한, 정보주체가 개인정보의 수집, 이용 또는 제공 및 정보주체의 권리 행사와 관련하여 DPO와 연락할 수 있도록 해야 함

- 특정 정부기관이 개인정보를 요청할 때, 컨트롤러의 PDPA 제2장(개인정보보호), 제3장(정보주체의 권리)에 규정된 준수 의무를 면제하는 법령이 '24년 1월부터 시행됨
  - 컨트롤러가 ▲국가반부패위원회 또는 ▲헌법상 반부패방지법에 따라 국가반부패위원회로부터 위임받은 정부기관, ▲국가반부패위원회 사무국, ▲공공부문 반부패방지위원회 또는 공공부문 반부패방지위원회 사무국, ▲위원회가 지정한 정부기관 중 반부패 관련 법률에 따른 목적이나 임무를 수행하기 위해 개인정보를 요청할 권한이 있는 기관으로부터 개인정보 요청을 받은 경우, 해당 컨트롤러는 PDPA 제2장, 제3장의 규정을 준수

하지 않아도 됨(제6조)
- 컨트롤러가 ▲국세청, ▲관세청, ▲소비세청으로부터 세금 징수, 세금 관련 수수료 집행, 기타 수수료나 관세 등과 관련된 법적 책임이나 목적을 수행하기 위하여, 또는 이와 관련된 국제 협력 등을 위하여 개인정보를 요청받은 경우, 해당 컨트롤러는 PDPA 제2장, 제3장의 규정을 준수하지 않아도 됨(제7조)
- 컨트롤러가 위원회가 지정한 지방자치단체로부터 토지 및 건물세법에 따른 세금 징수와 관련된 법적 책임이나 목적을 수행하기 위해 개인정보를 요청받은 경우, 해당 컨트롤러는 PDPA 제2장, 제3장의 규정을 준수하지 않아도 됨(제8조)
- 컨트롤러가 내각사무처로부터 승려 서열 제정, 국왕의 권한에 속하는 공무원, 개인 또는 단체의 임명 또는 해임 등 관련 법적 책임이나 목적을 수행하기 위해 개인정보를 요청받은 경우, 해당 컨트롤러는 PDPA 제2장, 제3장의 규정을 준수하지 않아도 됨(제9조)
- 컨트롤러가 위원회가 지정한 중요한 공익과 관련된 법적 목적이나 임무를 수행하기 위해 개인정보를 요청할 법적 권한을 가진 정부기관으로부터 개인정보를 요청받은 경우, 해당 컨트롤러는 PDPA 제2장, 제3장의 규정을 준수하지 않아도 됨(제10조)

Ⅱ. 데이터 프로세서

▶ PDPA는 컨트롤러의 지시를 받아 개인정보를 처리하는 '프로세서' 개념을 두고 있으며, 프로세서에 다양한 의무를 명시적으로 규정

- 프로세서는 오직 컨트롤러의 지시에 따라서만 개인정보 수집, 이용 또는 제공과 관련된 활동을 수행해야 함 (제40조제1항제1호)
- 프로세서는 개인정보의 무단 또는 불법적인 유출, 이용, 변경, 수정 또는 제공을 방지하기 위해 적절한 보안 조치를 제공하고, 발생한 개인정보 침해에 대해 컨트롤러에 통지해야 함 (제40조제1항제2호)
- 위원회가 규정한 규칙 및 방법에 따라 개인정보 처리 활동 기록을 작성, 유지 및 관리해야 함 (제40조제1항제3호)
- 프로세서는 다음의 경우 DPO를 지정해야 함 (제41조제1항)
  - ▲프로세서가 위원회가 지정한 공공기관인 경우 ▲개인정보의 수집, 이용 또는 제공과 관련하여 프로세서의 활동이 개인정보 또는 시스템에 대한 대규모의 정기적인 모니터링을 요하는 경우 ▲프로세서의 핵심 활동이 개인정보의 수집, 이용 또는 제공인 경우
- 그밖에, 태국 역외에 소재하는 프로세서는 개인정보의 수집, 이용 또는 제공에 대해 책임의 제한 없이 프로세서를 대신하여 행동할 수 있는 권한을 가진 국내 대리인을 서면으로 지정해야 함 (제38조제2항, 제37조제5호)

4. 행정처분 법적 근거

▶ 전문가위원회는 PDPA를 위반한 컨트롤러 및 프로세서에 과징금 부과를 명할 수 있음

- 전문가위원회는 과징금을 부과하기 전 적합하다고 판단될 경우 시정명령이나 경고를 먼저 내릴 수 있음 (제90조제1항)
- 만약 전문가위원회가 과징금 부과를 결정할 경우에는 위반행위의 심각성, 컨트롤러 또는 프로세서의 업무 규모, PDPC 위원회가 정한 규칙 기타 정황을 고려해야 함
- 과징금 부과 대상인 위반행위 및 과징금의 구체적인 수준은 제82조~제89조에서 상세히 규정

조항	위반행위	과징금
제82조	• 컨트롤러가 제23조(정보제공 의무), 제30조제4항(열람권 행사에 대한 기간 내 이행), 제39조제1항(처리 활동 기록 의무), 제41조제1항(DPO 지정 의무), 제42조제2항(DPO 업무 지원) 또는 제3항(DPO 해고 금지)을 준수하지 않음 • 컨트롤러가 동의를 얻을 때 제19조제3항에 근거한 PDPC 위원회가 정한 양식이나 진술을 사용하지 않음 • 컨트롤러가 제19조제6항에 따라 동의 철회의 법적 영향에 대해 정보주체에게 알리지 않음 • 컨트롤러가 제25조제2항에서 준용하는 제23조(개인정보 수집 시 정보제공 의무)를 이행하지 않음	최대 100만 바트 (약 3,700만원)
제83조	• 컨트롤러가 제21조(목적에 따른 개인정보 수집, 이용, 제공), 제22조(목적에 따른 개인정보 수집 범위 제한), 제24조(동의 없는 개인정보 수집의 예외), 제25조제1항(타인으로부터의 개인정보 수집 제한), 제27조제1항 또는 제2항(동의 없는 개인정보 이용 및 제공 금지), 제28조(개인정보 국외이전), 제32조제2항(반대권에 따른 개인정보 수집, 이용, 제공 금지) 또는 제37조(보안 조치 의무)를 위반하거나 준수하지 않음 • 컨트롤러가 개인정보의 처리 목적에 대해 정보주체를 기만하거나 오인하게 하여 동의를 획득 • 컨트롤러가 제25조제2항에서 준용하는 제21조(개인정보 수집 시 새로운 목적 통지 의무)를 준수하지 않음 • 컨트롤러가 개인정보를 보내거나 전송하면서 제29조제1항 또는 제3항(개인정보 국외이전 요건 면제)을 준수하지 않음	최대 300만 바트 (약 1억 1,100만원)
제84조	• 컨트롤러가 개인정보와 관련하여 제26조제1항 또는 제3항(민감한 개인정보 수집 등), 제27조제1항(동의 없는 개인정보 이용 및 제공 금지) 또는 제2항(목적을 벗어난 개인정보 이용 및 제공 금지), 제26조에 규정된 개인정보	최대 500만 바트 (약 1억 8,500만원)

	(민감한 개인정보 등)와 관련하여 제28조(개인정보 국외이전 요건)를 위반 • 컨트롤러가 제29조제1항 또는 제3항(국외이전 요건 면제 사유)에 따라 제26조에 규정된 개인정보(민감한 개인정보 등)를 전송하거나 이전하지 못함	
제85조	• 프로세서가 제41조제1항(DPO 지정) 또는 제42조제2항(DPO 업무 지원)·제3항(DPO 해고 금지)을 준수하지 않음	최대 100만 바트 (약 3,700만원)
제86조	• 프로세서가 적절한 이유 없이 제40조(프로세서의 의무)를 준수하지 않거나 제29조제1항 또는 제3항(국외이전 요건 면제 사유)에 반하여 개인정보를 전송 • 프로세서가 제38조에서 준용하는 제37조제5항(국내대리인 지정)을 준수하지 않음	최대 300만 바트 (약 1억 1,100만원)
제87조	• 프로세서가 제29조 제1항 또는 제3항(국외이전 요건 면제 사유)을 준수하지 않고 제26조제1항 또는 제3항(민감한 개인정보 등)의 개인정보를 전송하거나 이전	최대 500만 바트 (약 1억 8,500만원)
제88조	• 컨트롤러 또는 프로세서의 대리인이 제39조제2항에서 준용하는 제39조제1항(대리인의 처리 활동 기록), 그리고 제41조제4항에서 준용하는 제41조제1항(대리인의 DPO 지정)을 준수하지 않음	최대 100만 바트 (약 3,700만원)
제89조	• 자연인이 전문가위원회의 명령에 따르지 않음 • 자연인이 제75조(전문가위원회의 사실 진술 요청)를 위반하여 사실관계를 진술하지 않음 • 자연인이 제76조제1항제1호(공무원의 정보 또는 증거 제공/제출 요청)를 준수하지 않음 • 자연인이 제76조제4항(공무원의 직무 수행 중 편의 제공)을 위반하여 공무원에게 편의를 제공하지 않음	최대 50만 바트 (약 1,850만원)

▶ PDPA는 행정 과징금 부과 외에도 특정 개인정보보호 위반이 단순 법률위반을 넘어 범죄로 나아갈 경우 이를 처벌하기 위한 형사처벌 조항을 둠 (제79조~제81조)

• 컨트롤러가 PDPA 제27조제1항 또는 제2항(정보주체의 동의 없는 개인정보 이용 및 제공 등)을 위반하거나 제26조(인종, 민족, 정치적 의견, 종교 또는 철학적 신념, 성적 행동, 범죄 기록 등의 원칙적 수집 금지)에 규정된 개인정보와 관련하여 제28조(개인정보 국외이전 요건)를 준수하지 않아 타인에게 피해를 입히거나, 평판을 손상시키거나, 타인이 경멸, 증오, 굴욕감을

느끼게 된 경우 6개월 이하의 징역 또는/및 50만 바트(약 1,850만원) 이하의 벌금에 처함 (제79조)

- 동법에 따른 직무를 수행한 결과 타인의 개인정보를 알게 되어 해당 정보를 타인에게 제공할 경우 6개월 이하의 징역 또는/및 50만 바트(약 1,850만원) 이하의 벌금에 처함 (제80조)
- 이때, 범죄를 저지른 행위자가 법인이고 그 법인의 위법행위가 임원, 경영진, 또는 운영 책임자의 지시 또는 행위의 결과로 발생했거나, 임원 등이 지시 또는 행위를 해태하여 해당 법인의 위법행위가 초래된 경우, 임원, 경영진, 또는 운영 책임자는 동법의 각 형사 처벌 조항에 규정된 처벌을 받음 (제81조)

▶ 국가기관(법무부 등)에 대한 개인정보보호법 적용 조항, 행정처분 및 권고 사례

- PDPA는 컨트롤러를 개인정보 수집, 이용, 제공 관련 결정 권한과 책임이 있는 개인 또는 법인이라고 정의하고 있어 (제6조) 일반적인 공공부문도 컨트롤러에 포함되는 것으로 해석[5)]
  - 동법은 법률의 적용 제외대상으로 국가 또는 공공안전, 국가의 금융 안전, 공공 안전에 관련된 국가보안을 유지할 의무가 있는 공공기관의 업무를 명시적으로 거론하고 있으므로 (제4조) 국가보안 등을 담당하는 공공기관 업무를 제외한 일반적인 공공부문의 업무는 동법의 적용대상으로 보는 것이 타당
- PDPA 제72조는 전문가위원회에 정보주체에게 피해를 입힌 컨트롤러 및 프로세서에 대한 조사 권한을 부여하고 있고, 제90조에서는 시정명령이나 경고, 과징금 처분 권한을 명시함으로써, PDPC가 국가기관의 개인정보보호 준수 여부에 대한 감독 기능 또한 수행할 수 있는 것으로 해석
- 한편, 특정 정부기관이 개인정보를 요청할 때, 컨트롤러의 PDPA 제2장(개인정보보호), 제3장(정보주체의 권리)에 규정된 준수 의무를 면제하는 법령이 '24년 1월부터 시행됨
- '23년 9월 기준으로 정부기관 및 공기업에서 발생한 개인정보 침해 사건이 154건으로, 전체 적발 건수의 80% 이상을 차지함

대상 (처분일시)	주요 내용
CSC(공무원위원회)[6)] ('24.7.)	• (사건 개요) 공무원위원회(CSC) 시스템에 저장되어 있던 10명 이상의 정부 장학생들의 개인정보가 유출됨 - '24년 4월 Microsoft Bing의 AI 검색 엔진을 통하여 10명 이상의 현재 정부 장학생들뿐만 아니라 졸업한 정부 장학생들의 신분증 사본, 여권 사본, 항공권 정보 등 개인정보가 유출됨 • (조치 내용) 태국 디지털경제사회부(MDES), PDPC에 조사 지시 - CSC는 검색 엔진의 데이터 접근을 차단하고, Microsoft

5) 실제로 태국 정부는 '20년 5월 21일 공포된 왕령을 통해 총 22개 범주에 속하는 컨트롤러를 대상으로 PDPA 적용을 1년 유예하는 조치를 내린 바 있으며, 해당 22개의 범주에 '정부기관'이 포함되기도 함 https://ilaw.or.th/node/5669

대상 (처분일시)	주요 내용
	Thailand와 협력하여 남아있는 캐시 데이터를 삭제하였다고 밝힘 - MDES는 PDPC에 위 개인정보 유출 사건 조사를 지시함 - PDPC는 추가 조사를 진행하고 있으나 아직 관련 조사 결과는 발표되지 않았고, 관련 부처와 협의하여 적절한 보상 방안을 마련할 예정임

5. 개인정보 국외이전 조항

▶ PDPA는 특정 요건을 갖춘 경우 개인정보 국외이전을 허용하거나 국외이전 요건을 면제

- 컨트롤러가 국외로 개인정보를 전송 또는 이전하는 경우, 해당 개인정보를 이전받는 외국 또는 국제기구는 적절한 개인정보보호 기준을 가지고 있어야 하며, 위원회가 규정하는 하위 법령에 따라 수행되어야 함 (제28조제1항 본문)
- 그러나 아래의 경우는 상기 국외이전 요건을 갖추지 않아도 무방 (제28조제1항 단서)
  - 법률을 준수하기 위해 개인정보 국외이전이 요구되는 경우
  - 수신지 국가 또는 국제기구의 부적절한 개인정보보호 표준과 관련해 정보주체의 동의를 얻은 경우
  - 정보주체가 계약 당사자인 계약의 이행을 위해 필요하거나 계약을 체결하기 전에 정보주체의 요청에 따라 조치를 취하기 위해 필요한 경우
  - 정보주체의 이익을 위해 컨트롤러와 다른 사람 간의 계약 준수에 필요한 경우
  - 정보주체 또는 타인의 생명, 신체, 건강에 대한 위험을 방지하거나 억제하기 위한 경우
  - 공익을 위해 국외이전이 필요한 경우
- PDPC 위원회는 수신지 국가 및 국제기구의 개인정보보호 기준에 대한 적정성을 평가 및 결정할 수 있으며, 한 번 내린 결정에 대해서는 수신지 국가 및 국제기구가 적절한 개인정보 보호 기준을 개발했음을 확실히 할 수 있는 새로운 증거가 있는 경우 재차 검토될 수 있음 (제28조제2항)
- PDPC 위원회의 외국 또는 국제기구의 개인정보 보호 수준이 적절한지 평가하는 제28조에서 규정된 절차를 구체화한 고시(ประกาศ)[7]가 '24년 3월부터 시행됨
  - PDPC 위원회가 PDPA 제28조에 따라 외국 또는 국제기구의 개인정보 보호수준이 적절한지 평가할 때 적정한 개인정보 보호 수준을 판단하기 위하여, ▲외국 또는 국제기구의 개인정보 보호와 관련된 법률이나 규정이 PDPA와 일치하는지 여부, 특히 컨트롤러의 의무와 관련하여 적절한 보안 조치, 적절한 개인정보 보호 조치, 정보주체의 권리를 행사할 수 있는 메커니즘이 있는지, 그리고 효과적인 법적 구제 조치가 있는지 여부, ▲해당 국가나 국제기구에서 개인정보 보호 관련 법률과 규정을 집행할 권한과 의무가

6) Civil Service Commission Office로, 태국 정부의 중앙 인사관리를 담당하는 정부기관임
7) https://ratchakitcha.soc.go.th/documents/14915.pdf

있는 기관이나 조직이 있는지 여부를 검토할 수 있다고 명시함
- PDPC 위원회가 PDPA 제28조에 따라 외국 또는 국제기구의 개인정보 보호수준이 적절한지 평가할 때, 컨트롤러가 제안한 사항을 검토하거나 자체적으로 정보를 수집하여 제안할 수 있음
- 적정성 결정이 없는 경우에도 개인정보를 이전할 수 있는 예외적 경우로, ▲법률에 따른 경우, ▲정보주체의 동의를 받은 경우로, 정보주체에게 개인정보를 이전받는 국가나 국제기구의 개인정보 보호 수준이 충분하지 않을 수 있다는 점을 이미 알린 경우, ▲정보주체가 당사자인 계약의 이행을 위해 필요하거나, 정보주체의 요청에 따라 계약 체결 전에 필요한 조치를 취하기 위한 경우, ▲정보주체의 이익을 위해 컨트롤러와 다른 개인 또는 법인 간의 계약을 이행하기 위한 경우, ▲정보주체가 그 시점에 동의할 수 없는 상황에서, 정보주체나 타인의 생명, 신체 또는 건강에 대한 위험을 방지하거나 억제하기 위한 경우, ▲중요한 공익을 위한 업무 수행에 필요한 경우를 명시함

• 그밖에 PDPA는 국외이전 요건이 면제되는(제28조를 준수하지 않고도 국외이전을 할 수 있는) 사유를 제29조제1항 및 제3항에 규정
- 컨트롤러 또는 프로세서가 국외의 동일 계열 사업체나 동일 기업 그룹으로 개인정보를 이전하는 것과 관련하여, 개인정보보호 정책을 시행하고 있으며 해당 정책이 PDPC 사무국에서 검토를 거쳐 승인이 완료된 경우(제29조제1항)
- 수신지 국가 또는 국제기구가 PDPC 위원회로부터 적정성 결정을 받은 적이 없거나, 동조제1항과 같은 개인정보보호 정책이 없는 경우라도 PDPC 위원회가 제정한 규칙에 따라 정보주체의 권리 행사를 보장하는 적절한 보호 조치를 컨트롤러 또는 프로세서가 제공하는 경우 (제29조제3항)

• PDPA 제29조 제1항과 관련한 '구속력 있는 기업 규칙'과 제29조 제3항에서 규정된 '적절한 보호조치'를 구체화한 고시[8]가 '24년 3월부터 시행됨
- 컨트롤러 또는 프로세서가 국외의 동일 계열 사업체나 동일 기업 그룹으로 개인정보를 이전하는 경우 구속력 있는 기업 규칙(BCRs[9])이 있어야 하고, 위 규칙은 사무국의 검토와 승인을 받아야 함
- BCRs는 컨트롤러나 프로세서가 기업 경영 또는 사업과 관련된 활동을 수행할 때 개인정보보호를 위해 채택한 정책을 의미함
- 한편, BCRs는 ▲관련된 모든 개인과 법인에게 법적 구속력이 있어야 하고, 이때 개인과 법인에는 직원, 하청업체, 컨트롤러와 프로세서가 포함되며, 개인정보를 이전받는 자와 제3자에게도 적용되어야 하며, ▲정보주체의 권리를 명시하고, 국외로 이전되는 개인정보에 대한 보호조치를 포함하여야 하며, ▲개인정보 보호와 보안 조치는 PDPA를 준수하여야 하고, 이러한 보안 조치는 BCRs에 명시되어야 함
- PDPC 위원회로부터 적정성 결정을 받은 적이 없거나, BCRs이 없는 경우라 하더라도, 수신지 국가 또는 국제기구가 PDPA 제29조제3항에서 규정된 '적절한 보호 조치'를 갖춘 경우 국외이전 요건이 면제되는데, 이러한 '적절한 보호 조치'가 무엇인지 구체화하고 있음

8) https://ratchakitcha.soc.go.th/documents/14913.pdf
9) Binding Corporate Rules

- 즉, ▲개인정보의 국외이전 또는 제3국으로의 개인정보 이전과 관련하여 개인정보 보호를 위한 계약 조항으로, 위원회가 정한 개인정보 보호를 위한 계약 조항을 사용하여 개인정보 송신자와 수신자 간의 의무와 조건을 규정한 경우, ▲컨트롤러 또는 프로세서의 개인정보 수집, 사용, 공개와 관련하여, 국외 이전 또는 제3국으로의 개인정보 이전에 대해 적절한 개인정보 보호 조치가 있다는 인증 메커니즘을 갖춘 경우, ▲태국 정부기관과 외국 정부기관 간의 개인정보 이전에 관한 법적 구속력이 있고 집행가능한 문서나 협정에 포함된 개인정보 보호 조치를 취하는 경우 중 하나에 해당하는 경우에는 국외 이전 요건이 면제됨

6. 피해 구제 체계

Ⅰ. 데이터 컨트롤러

▶ 컨트롤러는 개인정보 침해 사고가 발생한 경우 해당 사실을 PDPC 사무국 및 정보주체에게 통지해야 할 의무를 짐 (제37조)

- (PDPC 사무국) 컨트롤러는 개인정보 침해가 당사자의 권리와 자유에 위험을 초래할 가능성이 없는 경우가 아니라면 개인정보 침해 사실을 인지한 후 72시간 이내에 지체 없이 PDPC 사무국에 통지해야 함 (제37조제4호 제1문)
- (정보주체) 컨트롤러는 개인정보 침해가 영향을 받는 개인의 권리와 자유에 높은 위험을 초래할 가능성이 있는 경우 지체 없이 정보주체에게 통지해야 함 (제37조제4호 제2문)
- 통지 절차 및 통지 면제 등 관련 세부 내용은 위원회가 규정한 규칙과 절차에 따라 이루어져야 함 (제37조제4호 제2문)
- 이와 관련, PDPC 위원회는 '22년 12월 15일 왕실 관보를 통해 개인정보 침해 통지에 대한 기준 및 수단에 대한 고시를 게시
  - 해당 고시에는 개인정보 침해 통지에 대한 구체적인 요건과 함께, 이러한 의무를 준수하지 못할 경우 부과될 수 있는 과징금에 대해 규정

< 개인정보 침해 통지에 대한 PDPC 위원회 고시의 주요 내용 >[10)]

구분	세부 내용
대상	• 보안 조치 위반으로 인해 개인정보의 무단 손실, 접근, 사용, 변경, 공개를 초래하는 개인정보 침해 사고 • 고의 또는 과실로 인해 발생하거나 또는 컨트롤러/프로세서로 인해 발생하는 개인정보 침해 • ▲개인정보에 대한 무단 접근 또는 제공을 초래하거나(기밀성 침해)

10) https://hsfnotes.com/data/2022/12/21/pdpa-update-thailands-new-legislation-on-personal-data-breach-notification/

	▲잘못되거나 부정확한 개인정보를 유발하거나(무결성 침해) ▲개인정보의 용이한 사용을 저하하는(가용성 침해) 모든 침해 사고를 포함
절차	• (위험성 검사 및 평가) 컨트롤러는 개인정보 침해를 인지한 후 지체 없이 개인정보 침해 내용을 점검하고, 정보주체의 권리와 자유에 미치는 위험성 및 영향 등을 평가 • (통지) 침해의 영향에 따라 통지의 대상 범위가 구분됨 - (PDPC) 침해가 발생했다고 믿을 만한 이유가 있는 경우, 컨트롤러는 위험 수준에 관계없이 침해 사실을 인지한 후 72시간 이내에 PDPC 사무국에 통지 - (정보주체) 위험의 수준이 높은 경우에 한하여 침해의 영향을 받게 되는 정보주체에게도 통지해야 함 • (사후 조치) 컨트롤러는 침해 사고를 시정 및 완화하고 유사한 침해 사고를 미연에 방지하기 위한 최대한의 조치를 이행해야 함
통지 시 제공정보	• 침해의 성격, 관련된 개인정보 기록의 유형 및 양, DPO 연락처 정보, 영향력 혹은 파급력, 개선 조치 등
수단 및 방법	• (PDPC) 사무국이 규정하는 서면 또는 전자적 방식으로 사무국에 통지 • (정보주체) 정보주체에게 연락할 수 있는 서면 또는 전자적 방식을 사용 - 만약, 해당 방식이 불가능한 경우, 대중매체, 소셜미디어 또는 기타 정보주체가 접할 수 있는 다른 방식을 활용하는 것도 허용
통지 불가능 시 조치	• 컨트롤러가 적시에 통지가 불가능한 경우, 합리적인 사유가 있다면 침해 사실을 인지한 날로부터 15일 이내에 PDPC 사무국에 통지의무 면제를 요청할 수 있음

Ⅱ. 정보주체

▶ 정보주체는 컨트롤러 또는 프로세서에 대한 불만사항에 대해 PDPC 위원회에 민원을 제기할 수 있음

- 정보주체는 컨트롤러 또는 프로세서가 PDPA를 위반하거나 준수하지 않는 경우, 이에 대한 민원을 제기할 권리를 가짐 (제73조)
- PDPC 위원회는 전문분야에 따라 또는 위원회가 적합하다고 인정하는 경우 하나 이상의 전문가위원회를 임명해야 함 (제71조)
- 전문가위원회는 PDPA에 따른 민원을 검토하고 정보주체에 피해를 입히는 컨트롤러 또는 프로세서에 대해 조사를 수행 (제72조)
- 전문가위원회의 검토 및 조사 결과 그러한 불만 등이 해결될 수 있다고 판단되고 당사자가 분쟁을 해결하고자 하는 경우 전문가위원회는 분쟁해결 절차를 진행하고, 만약 분쟁해결이 불가능하거나 분쟁해결에 실패할 경우, 전문가위원회는 아래와 같은 명령을 내릴 수 있음

(제74조제3항제1호~제2호)
- 컨트롤러 또는 프로세서로 하여금 지정된 기간 내에 특정 행위를 수행 또는 시정하도록 명령
- 컨트롤러 또는 프로세서가 정보주체에 피해를 주는 행위를 수행하는 것을 금지하거나 혹은 컨트롤러가 지정 기간 내에 피해를 중단하는 행위를 수행하도록 명령

• 만약 컨트롤러 또는 프로세서가 제74조제3항에 따른 명령을 이행하지 않는 경우, 전문가위원회는 컨트롤러 또는 프로세서의 재산에 대해 행정절차법에서 정하는 바에 따라 압류 및 매각을 명할 권한을 가짐(제74조제4항)

▶ 컨트롤러 등은 손해를 입은 정보주체에 대해 민사책임을 부담하며, 법원은 징벌적 손해배상 지급 또한 선고할 수 있음

• 컨트롤러 등이 자신의 개인정보와 관련된 조치로 인해 동법의 규정을 위반해 정보주체에게 손해를 끼치는 경우, 고의 또는 과실을 불문하고 정보주체에게 손해를 배상해야 함 (제77조)
- 이때 ▲불가항력 또는 정보주체의 작위 또는 부작위에 따라 손해가 발생했거나 ▲동법에 따른 직무 및 권한을 행사하는 공무원의 명령에 따라 조치를 취했으나 손해가 발생한 경우 컨트롤러 등의 손해배상 의무가 면제됨

• 법원은 적합하다고 인정되는 실제 배상금 외에 징벌적 손해배상금을 지급하도록 명할 권한을 가짐 (제78조제1문 및 제2문)
- 이때 징벌적 손해배상금은 실제 배상금액의 2배를 초과할 수 없음
- 법원은 참작사유로서, ▲정보주체에게 발생한 손해의 심각성 ▲컨트롤러 또는 프로세서가 얻은 이익 ▲컨트롤러 또는 프로세서의 재무 상태 ▲컨트롤러 또는 프로세서가 제공한 구제조치 ▲정보주체가 손해를 유발하는 데 기여하는 행위 등을 고려

• 한편, 동법에 따른 배상청구는 피해자가 피해사실을 인지하고 책임 있는 컨트롤러 또는 프로세서의 신원을 안 날로부터 3년, 개인정보에 대한 부당한 행위가 발생한 날로부터 10년 내에 제기되어야 함 (제78조제3문)

7. 개인정보 법제 준수 지원 현황

지침/가이드라인	개요	발행일
동의 요청 및 개인정보 수집 시 통지에 관한 지침[11]	• 정보주체로부터 개인정보 수집 시 동의를 얻기 위한 요건 및 제공해야 할 세부 정보와 관련한 가이드 제공	'22.9.7.

▶ 동의 요청 및 개인정보 수집 시 통지에 관한 지침

11) https://www.zicolaw.com/resources/alerts/thailand-issues-pdpa-guidelines-on-consent-and-personal-data-collection/

- 컨트롤러가 정보주체의 동의를 얻을 때와, 정보주체의 개인정보 수집 시 필요한 정보를 알릴 때 따라야 할 지침사항
- (동의 요청) 컨트롤러는 특별한 사정이나 별도의 규정이 없는 경우 동 지침에 맞춰 자발적으로 표준 양식을 갖추거나 자체 동의서를 마련할 수 있으며, 컨트롤러는 다음과 같이 개인정보 수집에 대한 동의를 정보주체에게 요청해야 함
  - 동의는 개인정보의 수집, 이용 및 제공 전 또는 제공 시점에 요청해야 함
  - 컨트롤러는 동의를 요청하기 전에 동의 요청 목적과 구체적인 내용을 통지해야 함
  - 동의 요청에는 일반적인 목적이 아닌 구체적인 목적을 명시해야 함
  - 동의 요청 부분은 다른 부분과 명확하게 구분되어야 하며, 컨트롤러가 제공하는 정보 또는 양식은 이해하기 쉽고 오해의 소지가 없어야 함
  - 동의는 사기 또는 기망, 협박, 오해 없이 자유롭게 제공되어야 함
  - 동의는 조건부이어서는 안 되며 정보주체로 하여금 계약 체결 등을 강요해서는 안 됨
- 동의 요청 양식은 서면 형식이나 전자적 수단 모두 가능하고, 정보주체 또한 동의 제공 시 서면 양식 외에 전자 시스템을 통한 양식 작성, 이메일 전송, 전자 서명 사용 등 여러 방법으로 선택할 수 있음
- (개인정보 수집에 따른 통지) 컨트롤러는 특별한 사정이나 별도의 규정이 없는 경우 개인정보 수집 전 혹은 수집 시 해당 정보주체에게 다음의 내용을 알려야 함
  - ▲개인정보 수집 목적 ▲정보주체의 법적·계약적 의무와 정보주체가 개인정보를 제공하지 않을 경우의 잠재적 영향 ▲수집할 개인정보 ▲개인정보 보유기간 ▲수집된 개인정보가 제공될 수 있는 개인 또는 법인의 범주 ▲이름, 주소를 포함한 세부 정보 및 컨트롤러, 그 대리인, DPO 연락처 ▲개인정보 국외이전과 관련한 세부정보 ▲동의 철회 권리, PDPA 위반에 대한 민원을 제기할 권리 등과 같은 정보주체의 권리
- 컨트롤러는 개인정보 수집일로부터 30일 이내에 수집 목적 및 그 세부사항을 정보주체에게 통지해야 하며, 정보주체에게 연락하기 위해 개인정보를 사용하는 경우, 컨트롤러는 첫 번째 연락 시 해당 정보주체에게 알려야 함
- 만약, 컨트롤러가 정보주체가 아닌 다른 출처로부터 개인정보를 수집한 후 지체 없이, 늦어도 30일 이내에 정보주체에게 개인정보 수집 사실을 통지하지 않는 한 다른 출처에서 개인정보를 수집할 수 없음
- 정보주체의 동의 및 승인 없이 다른 출처에서 수집된 개인정보를 수집, 이용 및 제공하기 전에 컨트롤러는 다음을 수행해야 함
  - 개인정보 이용 및 제공으로 인한 잠재적 위험을 평가하고 정보주체의 권리와 자유에 영향을 미칠 수 있는지 여부를 고려하기 위해 개인정보 영향평가 실시
  - 정보주체가 쉽게 이해할 수 있는 형식이나 맥락으로 목적 또는 구체적인 내용 고지
  - 개인정보 보유 기간 지정, 개인정보 수집에 법적 근거가 있는지 검토

8. 최근 행정처분

▶ 민원 접수 숫자 및 처분 사례 건수 등

- 민원 접수 건수 총 254건[12], 금융·경제 관련 민원을 담당하는 제1전문가위원회가 6건의 행정명령을, 디지털 기술 및 기타 분야 관련 민원을 담당하는 제2전문가위원회가 66건의 행정명령을 발하였음
- 또한, '23년 9월 기준으로 PDPC에 보고된 개인정보 침해 사건은 총 382건이고, PDPC가 직접 적발한 개인정보 침해 사건은 총 192건으로, 총 개인정보 침해 사건 수는 574건

▶ 아래에서는 개인정보 침해와 관련한 MDES, PDPC의 조사 및 처분 사례를 소개

컨트롤러	일시	침해사항 개요	내역
익명의 대형 온라인 쇼핑 기업	'24.8.	• 10만 명 이상의 고객 개인정보 유출 사고 발생	• PDPC, 7백만 바트(약 2억 6천만 원) 과징금 부과
CSC(공무원 위원회)	'24.7.	• 10명 이상 장학생들의 개인정보 유출	• PDPC 조사 진행 중
익명의 네트워크, 익명의 웹사이트, Facebook	'24.2.	• 부적절한 개인정보 공개, 개인정보 판매 광고, 개인정보를 불법적으로 거래하는 네트워크가 확인됨	• 5,869건의 부적절한 개인정보 공개 사례 발견 후 시정조치 • 65건의 개인정보 판매 광고 차단 • 9명 체포

▶ PDPC, 익명의 대형 온라인 쇼핑 기업에 개인정보 유출 사고 발생에 따른 과징금 7백만 바트 부과 ('24.8.)

- (사건 개요) 익명의 대형 온라인 쇼핑 기업에서 보관하던 10만 명 이상의 고객 개인정보에 대한 유출 사고 발생
  - 유출된 정보는 콜센터 사기 조직에 의하여 불법적으로 사용됨

12) '23년 9월 30일까지의 누적 건수

• (조치 내용) PDPC, 위 기업에 과징금 7백만 바트(약 2억 6천만 원) 부과
  - 위 기업은 10만 명 이상의 고객 개인정보를 수집하고 이를 주요 사업에 이용하면서 PDPA 제41조[13]에 규정된 바와 같이 DPO를 지정하지 않았고, 이에 따라 고객의 개인정보가 유출되는 사고 발생을 야기함
  - 또한, 위 기업은 적절한 보안 조치를 취하지 않아 유출 사고가 발생하여, PDPA 제37조 제1호[14]를 위반함
  - 나아가, 위 기업은 개인정보 유출 사실을 알게 된 후에도 PDPA에서 정한 기간 내에 당국에 통지하지 아니한바, PDPA 제37조 제4호[15]를 위반함
  - 제2전문가위원회는 위 기업에 최고 수준의 총 7백만 바트의 과징금을 부과함
  - 또한, 위 기업에 보안 조치를 개선하여 추가적인 개인정보 유출을 방지하도록 명령하고, 회사 직원들에게 개인정보 보호에 관한 교육을 실시하도록 지시함
  - 나아가, 위 기업에 변화하는 기술에 맞추어 최신 보안 조치를 도입하도록 명령하는 한편, 명령을 받은 후 7일 이내에 취한 조치들을 PDPC에 보고하도록 명함

▶ PDPC, CSC의 장학생 개인정보 침해 사고에 대한 조사 실시 ('24.7.)[16]

• 본문 16페이지 표 참조

▶ MDES·PDPC, 개인정보를 불법거래하는 네트워크 관련자 9명 체포, 5,869건의 부적절한 개인정보 공개 사례 발견 후 시정조치, 54건의 개인정보 판매 광고 발견 후 차단조치 실시 ('24.2.)

• (사건 개요) MDES는 '24년 2월 개인정보 불법 네트워크에 연루된 9명을 체포하는 합동 수사 결과를 발표하고, '23년 11월부터 '24년 2월까지 웹사이트에서 개인정보가 부적절하게 공개된 사례, 개인정보 판매 광고 사례를 조사하였음

• (조치 내용) MDES, '24년 2월 개인정보 불법 거래 네트워크에 연루된 9명 체포하고, PDPC는 개인정보 침해 감시 센터인 'PDPC Eagle Eye'를 설립하고, 개인정보 보호 관련 사실 조사 및 수집을 위한 공동 작업반을 구성하여 부당한 개인정보 공개 사례를 확인하고 시정조치를 취하고, 개인정보 판매 광고 사례를 발견하고 차단조치함
  - PDPC는 익명의 여러 웹사이트에서 시민들의 개인정보가 부적절하게 공유되거나 충

13) 컨트롤러의 DPO 지정 의무 규정
14) 컨트롤러의 보안 조치 마련 의무
15) 개인정보 침해 사건 인지 시 통지의무 규정
16) https://www.pdpc.or.th/6746/

분한 보안 조치 없이 공개된 5,869건의 사례를 확인하고 시정조치를 취하였음
- 또한, PDPC는 Facebook에서 54건의 개인정보 판매 광고를 발견하고 차단하였음

9. 시사점

▶ **개인정보 국외이전 관련 규정 구체화, 특정 정부기관 요청에 대한 컨트롤러 의무 면제, 정보주체의 삭제권 강화에 대한 법 동향 파악 및 준수 필요**

- '24년 3월 개인정보의 국외이전과 관련되어 개인정보 보호 수준의 적절성 평가 기준과 국외이전 요건 면제 기준을 구체화하는 새로운 고시가 시행되어, 태국으로 진출하는 국내 기업들은 본사-현지법인 간 개인정보 이전 등에 있어 위 새로운 규정을 숙지하고 준수할 필요성이 대두됨
- 또한, '24년 1월부터 시행된 법령에 따라 특정 정부기관의 개인정보 요청 시 컨트롤러에게 부과된 일부 의무가 면제되어, 기업들은 개인정보를 요청하는 정부기관이 해당 법령에 명시된 기관인지 면밀히 확인할 필요성이 있음
- 나아가, '24년 11월부터 시행되는 고시에 따라 정보주체의 삭제권이 구체화되어, 기업들은 정보주체로부터 삭제 요청을 받은 날부터 60일 이내에 처리해야 하고, 삭제 시 정보주체를 식별할 수 없을 정도로 철저한 비식별화 조치가 요구되므로, 삭제 요청에 대한 내부 프로세스를 점검하고 개선할 필요성이 있음

▶ **PDPC가 '23년 연례 보고서 발간 및 개인정보 침해에 따른 과징금 부과, 개인정보 불법 거래 관련자 체포, 부적절한 개인정보 공개 시정조치 등 적극적인 조치를 통하여 PDPA 위반에 대한 엄정한 대응 의지를 표명하고 있어 이에 대한 각별한 주의 당부**

- PDPC는 '23년 연례보고서 발간을 통하여 PDPA의 위반에 대한 대응 의지를 명확하게 천명하였음
- 또한, PDPC는 '24년 8월 익명의 대형 온라인 쇼핑 기업의 DPO 미지정 및 적절한 보안 조치 미실시, 개인정보 유출사실의 법정 기한 내 미통지 등의 사유로 7백만 바트(약 2억 6천만 원)의 과징금을 부과하였음
- 나아가, MDES와 PDPC는 '24년 2월 개인정보 불법 거래 네트워크를 대대적으로 단속하여 불법 네트워크 관련자 9명을 체포하고 약 6천 건의 개인정보 부당 공개 사례에 대한 시정조치를 명하였음
- 이처럼, PDPC는 최근 민간 기업뿐만 아니라 정부기관, 온라인 플랫폼 등 다양한 영역에서 PDPA 위반에 대하여 적극적으로 대응하고 있는바, 태국 진출 국내 기업들은 PDPA 준수 여부에 대한 정기적인 자체 점검, DPO 지정, 개인정보 유출 사고 발생 시 신속한 대응 및 통지 절차 마련 등 PDPA 준수에 각별한 주의를 기울일 것을 당부