싱가포르 개인정보보호 법 행정 체계 현황 및 주요 위반사례

1. 법률체계

▶ 개요

- 싱가포르의 개인정보보호는 ▲개인정보보호법 ▲그 외 관련 법령 등 크게 2개의 법적 근거를 바탕으로 함
  - 개인정보보호의 헌법적 근거와 관련해서는 헌법에서 프라이버시 관련 권리를 직접 혹은 간접적으로 도출할 수 없다고 보는 견해가 우세[1)]

▶ 개인정보보호법(Personal Data Protection Act 2012, 이하 PDPA)

- PDPA는 '12년 제정된 싱가포르 최초의 포괄적 개인정보보호법으로서, '12년 10월 15일 국회를 통과하고 '12년 11월 20일 대통령이 서명한 후 총 세 단계에 걸쳐 시행에 돌입[2)]
  - ('13년 1월 2일) 적용범위 및 정의 조항, 개인정보 감독기관 및 개인정보보호 자문위원회 설립 조항, 원치 않는 전화(Do-Not-Call) 등록부 개설 조항, 기타 일반 조항
  - ('14년 1월 2일) 원치 않는 전화 관련 기타 일반 조항
  - ('14년 7월 2일) 개인정보보호에 관한 일반 규칙 조항(제11조~제12조), 개인정보 수집, 이용, 제공 조항(제13조~제20조), 개인정보 열람권 및 정정권 조항(제21조~제22조), 개인정보 관리 조항(제23조~제26조), 집행 조항(제27조~제32조)
- 이후 싱가포르는 개인정보보호에 관한 변화된 사회적 인식을 반영하고자 컨트롤러의 책임을 강화하기 위해 '20년 11월 추가 개정[3)]을 단행
  - 개정법은 기존 법률 조항을 보완하여 ▲개인정보 침해사고 시 컨트롤러의 통지 의무 도입 ▲위반행위에 대한 컨트롤러 처벌 강화 ▲개인정보의 부적절한 취급에 대한 형사처벌 조항 도입 등의 내용을 포함
- PDPA는 민간 부문 전반에 걸친 일반적인 개인정보보호 표준 법체계를 수립한 것으로, 기존의 특정 분야 법률에서 규율하고 있는 개인정보보호 조항과 공존하는 것이 특징
  - PDPA는 타 법률에 따른 개인정보보호 관련 권리나 의무에 영향을 미치지 않으며 만약 상호 충돌하는 점이 있는 경우 타 법률의 조항이 PDPA에 우선함[4)] (PDPA 제4조 제6항)

1) https://www.carter-ruck.com/law-guides/defamation-and-privacy-law-in-singapore/
https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf
https://www.privacy.com.sg/resources/scope-of-singapore-privacy-how-to-use/
2) https://www.lexology.com/library/detail.aspx?g=44345885-c855-478f-b782-578996c4bba4
3) '20년 11월 국회를 통과한 PDPA 일부개정법률안(법안명 : Personal Data Protection (Amendment) Act 2020)은 '12년 제정법률의 주요 조항을 수정, 삭제, 대체하거나 일부 내용을 추가하는 형식으로 구성
4) https://www.lexology.com/library/detail.aspx?g=d1a480ea-f12f-4680-b8ae-6880cfe43d93

- 동법은 총 13장으로 이루어져 있으며, ▲총칙(제1장) ▲개인정보 감독기관 및 행정체계(제2장) ▲개인정보보호 및 책임 관련 일반조항(제3장) ▲개인정보 수집, 이용 및 제공(제4장) ▲개인정보 열람 및 정정(제5장) ▲개인정보 관리(제6장) ▲개인정보 침해 통지(제6A장) ▲'원치 않는 전화' 등록(제9장) ▲사전 공격(Dictionary Attack) 및 주소 수집 소프트웨어 사용 금지(제9A장) ▲개인정보 및 익명화된 정보에 영향을 미치는 범죄(제9B장) ▲집행(제9C장) ▲불복(제9D장) ▲일반사항(제10장) 등으로 구성
  - 제7장 및 제8장은 '20년 PDPA 일부개정법률안의 국회 통과에 따라 폐지 (Personal Data Protection (Amendment) Act 2020 제15조)

▶ **그 외 관련 법령[5)]**

- **은행법(Bangking Act 1970)**
  - 은행, 금융기관, 신용카드 및 충전카드 발급 업무를 수행하는 기관, 기타 관련 기관의 영업허가 및 규제 등에 관한 내용을 정하는 법률
  - 동법에서 명시적으로 규정된 경우를 제외하고 싱가포르 내 은행 또는 은행 임원은 어떤 방식으로든 다른 사람에게 고객 정보를 제공해서는 안 됨 (제47조제1항)
  - 주무당국은 서면통지를 통해 싱가포르 내 은행, 신용카드 발급 허가를 받은 사업자 등을 대상으로 신용카드 또는 신용카드 발급 업무와 관련된 정보를 요청할 수 있음 (제57EB조제1항)
    · 이때 주무당국은 동조에 따라 제공받은 모든 정보를 비밀로 취급해야 하며, 다만 해당 정보가 공공 영역에 속하거나, 신원을 확인할 수 없도록 조치하거나. 해당 정보를 제공한 자의 동의를 얻은 경우 등 특별한 사정이 있는 경우에만 제한적으로 정보 공개가 가능 (제57EB조제3항 및 제4항)

- **민간병원 및 의원법(Private Hospitals and Medical Clinics Act 1980)**
  - 민간병원, 의원, 임상실험실 및 의료시설 등의 관리, 허가 및 감독 사항을 규율하는 법률로, 해당 의료시설의 정보 비밀유지 관련 조항이 포함
    · 보건부 보건담당 국장(Director-General of Health) 및 그 밖의 권한 있는 담당자는 범죄로 인해 기소되는 경우를 제외하고, 동법에 따른 조사 및 직무 수행과 관련하여 민간병원, 의원, 임상실험실, 의료시설로부터 얻은 정보가 담긴 문서를 제출하도록 누구에게도 강요할 수 없음 (제13조제1항)
    · 보건부 보건담당 국장 및 그 밖의 권한 있는 담당자는 동법에 따른 조사 및 직무 수행 과정에서 얻은 의료기록에 포함된 정보 및 개인의 상태, 치료, 진단과 관련된 정보를 타인에게 공개해서는 안 됨 (제13조제2항)
    · 동법에 따라 획득하거나 얻게 된 정보를 타인에게 제공하는 경우 정보 제공이 직무 수행의 범위 내에 있지 않는 한 범죄에 해당하며, 5,000 싱가포르 달러(약 510만원) 이하의 벌금에 처해질 수 있음 (제16조)

5) https://www.lexology.com/library/detail.aspx?g=d1a480ea-f12f-4680-b8ae-6880cfe43d93

2. 행정체계

Ⅰ. 개요

<PDPC 로고>

▶ **싱가포르의 개인정보 감독기관은 Personal Data Protection Commission (이하 PDPC)로, '12년 제정된 PDPA에 근거해 '13년 1월 2일 최초 설립**

- **(규모)** 정보통신미디어개발청(Infocomm Media Development Authority 이하 IMDA) 산하 비독립적 정부기관[6]으로서 예산 및 직원 수에 대한 공시자료 없음
- **(담당 업무)** 개인정보보호를 통해 기업-소비자 간 신뢰 환경을 조성하여 국가 경제에 기여할 수 있도록 지원하는 기관으로서, 법률에 따라 다음의 기능을 수행 (제6조)
  - 싱가포르의 개인정보보호에 대한 인식 제고
  - 개인정보보호와 관련된 자문, 기술 및 관리 서비스, 기타 전문 서비스 제공
  - 개인정보보호와 관련된 각종 사안에 대해 對정부 자문 제공
  - 개인정보보호와 관련된 사안에 대해 정부를 대표
  - 연구 수행, 세미나, 워크숍 및 심포지엄 조직 및 실시, 기타 관련 활동을 수행하는 타 조직 지원 등 개인정보보호와 관련된 교육 활동 수행
  - 자체적으로 또는 정부를 대표하여 타국 개인정보 감독기관, 국제조직 등과 개인정보 보호 분야에서의 기술 협력 수행
  - PDPA 시행 및 집행 담당
  - 타법에서 PDPC에 부여된 기능 및 정부가 PDPC에 할당한 업무 및 기능 수행

- **(독립성 여부)** PDPC는 IMDA 산하 조직으로서 예산, 인사, 집행 등에서 독립성의 한계를 지님
  - (예산) PDPC는 IMDA 조직의 일부로, 자체적으로 예산을 배정받거나 운영할 법률상의 근거가 마련되어 있지 않아 예산 관련 독립성이 없음
  - (인사) '13년 창설된 PDPC는 정보통신개발청(Infocomm Development Authority), 미디어개발청(Media Development Authority)과 함께 통합기관인 IMDA로 재편성되면서 IMDA 하위 조직으로 흡수(정보통신미디어개발청법(Info-communications Media Development Authority Act 2016) 제83조)
    · 이에 따라 PDPC가 조직 자체의 인사 권한을 독립적으로 갖지 못하며, PDPC의 고위직인 ▲커미셔너 ▲자문위원회[7] 위원장 ▲부커미셔너 등의 임면(任免)권 또한 통신정보부 장관이 행사
  - (집행) 동법 제65조는 PDPC가 '통신정보부 장관의 승인'을 받아 동법의 목적 및 각 조항의 기능을 수행하기 위해 필요한 규정을 제정할 수 있다고 명시하고 있어 집행과

6) https://www.imda.gov.sg/about-imda/data-protection/personal-data-protection
https://www.lexology.com/library/detail.aspx?g=44345885-c855-478f-b782-578996c4bba4
7) PDPC는 별도의 조직으로서 IMDA 간부급 인사와 기업, 학계, 소비자협회가 추천한 18명으로 구성된 자문위원회를 두고 있음. PDPC는 동법상의 기능 수행과 관련해 자문위원회와 협의할 수 있지만 자문위원회의 자문에 법적으로 구속받지 않음

관련해서도 독립성에 제한이 있다고 풀이됨

- **(조직)**
  - (커미셔너) 류추엔홍(Lew Chuen Hong) ('20.6.~현재)[8]
  · 류 커미셔너는 커미셔너 임명 당시 IMDA의 CEO직에도 동시 임명됨으로써, 두 가지 직무를 겸직 중
  - (구성) 커미셔너, 부커미셔너, 자문위원회 위원장 및 두 개의 대단위 부서로 구성[9]
  - (담당 법령) PDPA
  - (주소) 10 Pasir Panjang Road, #03-01 Mapletree Business City Singapore 117438
  - (전화번호) +65 6377 3131

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

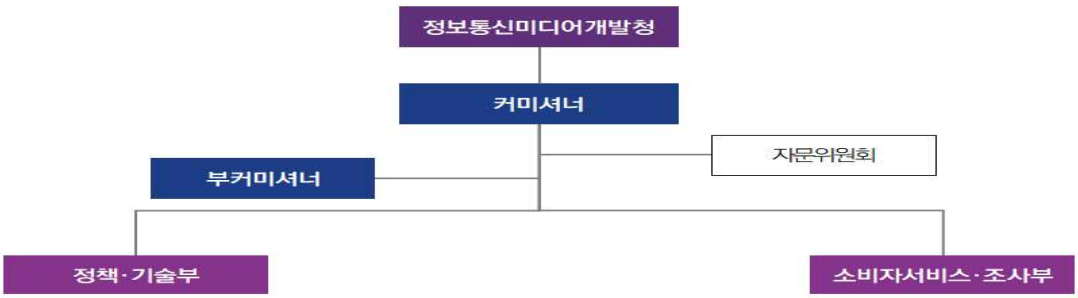
- PDPC는 IMDA 소속 기관으로 개인정보보호 기능만을 전담 수행하는 데에 국한

Ⅲ. 상세조직

▶ PDPC는 상위 감독기관인 IMDA의 지휘 아래 하위 조직으로 정책·기술부와 소비자서비스·조사부를 두고 있으며, 별도 자문 조직인 자문위원회의 자문을 받음

- PDPC는 조직도를 공개하지 않고 있으나 IMDA에서 소개하는 PDPC 관련 설명에 따라 아래와 같이 구성된 것으로 추정

< PDPC 예상 조직도 ('23.6.) >



출처 : IMDA 홈페이지 내용을 바탕으로 넥스텔리전스 재구성 ('23.6.)[10]

▶ 그밖에, PDPC의 각 부서별 업무 또는 소관사항에 대해서도 공개하고 있는 자료가 없음

8) https://www.pdpc.gov.sg/who-we-are/about-us
9) https://www.imda.gov.sg/about-imda/who-we-are/our-team/our-senior-management/data-innovation-and-protection
10) https://www.imda.gov.sg/about-imda/who-we-are/our-team/our-senior-management/data-innovation-and-protection

3. 개인정보 처리자 의무사항

Ⅰ. 데이터 컨트롤러

▶ (정보주체 권리강화) PDPA는 제21조 이하에서 정보주체인 개인의 권리에 대해 규정하고 있으며, 각 권리에 수반한 조직의 의무사항 또한 각 조항별로 열거

- PDPA는 개인의 열람권, 정정권, 이동권(시행 예정)을 명시적으로 규정하고 있으며, 정보를 제공받을 권리와 관련해서는 명시적 조항은 없지만 조직으로 하여금 일련의 정보를 제공해야 할 의무를 부과
  - PDPA는 특정 상황에서 조직으로 하여금 개인에 대해 통지를 제공해야 할 의무를 부과함으로써 개인이 특정 정보를 간접적으로 제공받는 반사적 효과를 누리도록 돕고 있음
- 동법은 삭제권, 반대권 및 처리제한권을 규정하지 않음
  - 다만, 삭제권과 관련해서는 정보주체가 삭제권을 행사할 수 없을지라도 특정 상황에서 조직에 삭제 의무를 부과
  - 반대권의 경우에도 PDPA가 '동의철회권'을 규정하여 기존 개인정보의 수집, 이용, 제공과 관련한 동의를 철회할 수 있도록 허용하여 간접적으로 반대권 행사의 효과를 향유할 수 있도록 함

< 정보주체 권리강화 규정 >

조항 및 권리	의무사항 세부 내용
정보를 제공받을 권리	• 조직은 수집, 이용 또는 제공 이전에 개인정보를 수집, 이용 또는 제공하려는 목적을 개인에게 통지해야 하며, 개인의 요청에 따라 요청일 전 1년 간 조직이 개인정보를 이용하거나 제공했을 수 있는 방식에 대한 정보를 개인에게 제공해야 함 (제20조) • 해당 권리조직은 동법 제12조에 따라 동법에서 부과하는 주요 의무를 이행하는 데에 필요한 정책 및 체제를 개발 및 구현하고 동법의 적용과정에서 발생할 수 있는 불만사항 처리 절차를 개발해야 함 (제12조) - 개인은 조직에 대해 이와 같은 정보를 제공하도록 요청할 수 있음
제21조 열람권	• 개인은 조직이 보유 또는 관리하고 있는 개인정보에 대한 접근을 요청할 수 있음 (제21조제1항 해석) • 조직은 예외적인 상황을 제외하고는 개인정보에 접근하려는 개인의 요청에 대응할 의무가 있으며, 지체 없이 개인에게 다음의 정보를 제공해야 함 (제21조제1항) - 조직이 보유 또는 관리하고 있는 해당 요청자의 개인정보 - 요청일 전 1년 간 조직이 개인정보를 이용하거나 제공했을 수 있는 방식에 대한 정보 • 다만, 조직은 아래의 경우에는 개인에 대한 개인정보 열람 거부가

조항 및 권리	의무사항 세부 내용
	가능(제21조제3항) - 요청을 한 개인 이외에 타인의 안전, 신체적 또는 정신적 건강을 위협하는 경우 - 요청을 한 개인의 안전, 신체적 또는 정신적 건강에 즉각적이거나 중대한 해를 끼치는 경우 - 요청 대응 시 타인의 개인정보를 공개하게 되는 경우 - 요청 대응 시 타인의 개인정보를 제공한 특정인의 신원이 드러나는 한편, 해당 특정인이 신원 공개에 동의하지 않은 경우 - 국익에 반하는 경우
제22조 정정권	• 개인은 조직이 보유 또는 관리하는 부정확한 개인정보를 정정하도록 조직에 요청할 수 있음 • 조직은 해당 요청을 거부할 만한 합리적 근거가 없는 가능한 한 빨리 개인정보를 정정해야 함 - 조직은 정정이 있은 날로부터 직전 1년 이내에 해당 조직이 개인정보를 제공한 다른 모든 조직에도 정정된 개인정보를 전송해야 함 - 다만 조직은 개인의 동의가 있는 경우 개인정보를 제공했던 조직 중 특정 조직에 한정하여 정정된 개인정보를 전송할 수 있음
제26H조 이동권 (※시행예정[11])	• 개인은 조직에 자신의 개인정보를 타 조직으로 이전하도록 요청할 수 있음 • 조직은 개인의 이동 요청에 명시된 개인정보를 타 조직으로 이전해야 하는데, 다만 이동 요청이 아래의 사항을 모두 충족해야 함 - 이동 요청이 요건을 모두 만족할 것 - 이동 요청을 받은 시점에 요청을 받은 조직과 개인이 지속적인 관계를 유지하고 있을 것
삭제권 관련	• PDPA는 개인에 대해 삭제권을 규정하고 있지 않음 - 다만, 조직에 개인정보 보유 중단 의무를 규정하여 개인정보를 일정 요건 하에서 제거하도록 함 • 조직은 PDPA 제25조에 따라 ① 개인정보의 수집 목적이 개인정보의 보유로써 더 이상 만족되지 않거나 ② 법적 또는 상업적 목적으로 더 이상 개인정보 보유가 필요하지 않게 된 경우, 개인정보가 포함된 문서 보유를 중단하거나 개인정보가 특정 개인과 연관되도록 하는 수단을 제거해야 함
반대권 관련 (동의철회권)	• PDPA는 개인에 대해 반대권을 규정하지 않음 - 대신 개인에게 동의철회권을 명시적으로 부여하여 반대권과 유사한 법적 효과를 누리도록 함
제16조	• 개인은 조직에 합리적인 통지를 제공하는 경우 자신의 개인정보 수집,

조항 및 권리	의무사항 세부 내용
동의철회권	이용 또는 제공과 관련한 동의 및 간주된 동의를 철회할 수 있음 - 그러나 동의 철회는 그로 인해 발생하는 법적 결과에 영향을 미치지 않음

▶ **(컨트롤러 의무사항) PDPA는 개인정보보호책임자 지정 의무, 보안 조치 의무를 비롯한 다양한 의무를 조직에 부과**

- PDPA는 EU 일반 개인정보보호법(이하 GDPR)의 DPO(Data Protection Officer)와 같은 특정 용어를 사용하고 있지 않지만, 유사한 책임을 담당하는 개인을 지정할 의무를 조직에 부과
- 또한 개인정보 수집, 이용, 제공에 적법성을 부여하는 개인의 '동의'와 관련하여, 조직이 '동의를 얻은 것으로 간주'되기 위한 특정 상황에서의 평가(assessment) 수행 의무를 규정
- 그밖에. 조직은 개인정보의 정확성 및 완전성 보장을 위한 조치 의무와 보안 조치 의무를 부담하며, 기타 컨트롤러의 의무 수행을 위한 정책 개발 등의 의무 및 개인의 불만사항에 대한 처리 절차 개발 의무를 수행해야 함

조항	의무사항 세부 내용
제11조 제3항~제5항 개인정보보호 책임자 지정 의무	• 조직은 동법을 준수하도록 보장하는 한 명 이상의 개인을 지정해야 하며, 조직은 적어도 해당 개인의 비즈니스 연락처 정보를 대중에게 제공해야 함 (제11조제3항 및 제5항) - 동 조항에 따라 법률 준수 책임자로 지정된 개인은 자신에게 부여된 책임사항을 다른 개인에게 위임할 수 있으며, 이 때 조직은 상기 개인 중 어떤 사람이든 적어도 한 명 이상의 비즈니스 연락처를 대중에게 제공하면 됨 (제11조제4항 및 제5항)
제15A조 평가 수행 의무	• 조직은 개인정보를 수집, 이용, 제공하기 위해 개인의 동의를 얻어야 하는데, 동의를 얻은 것으로 간주되기 위한 요건으로서 개인정보 수집, 이용, 제공이 해당 개인에게 부정적인 영향을 미칠지 여부에 대한 평가를 수행해야 함[12] • 조직은 평가와 관련해 아래의 사항을 수행해야 함 - 개인정보 수집, 이용, 제공이 개인에게 미칠 수 있는 부정적 영향 파악 - 부작용 제거, 부작용의 발생 가능성 최소화, 부작용 완화 등을 위한 합리적 조치 구현 - 그 외 기타 규정된 요건 준수
▬ 제23조	• 조직은 수집한 개인정보가 정확하고 완전하도록 보장하기 위해

11) 이동권 조항은 '20년 법률 개정에 따라 PDPA에 도입된 정보주체의 권리로, 이동권 조항의 시행시기는 법률에 명시되어 있지 않으며 통신정보부 장관이 별도로 관보에 고시(notification)할 때 해당 고시에 지정한 날짜에 시행된다고 규정하고 있으므로(Personal Data Protection (Amendment) Act 2020, 제1조), 시행시기는 싱가포르 정부의 결정에 전적으로 달려 있는 것으로 해석

12) 조직은 평가 수행을 통해 개인정보 수집, 이용, 제공에 있어 개인의 동의를 얻은 것으로 간주되는 등 개인이 직접 동의한 것과 같은 효과를 누릴 수 있음

조항	의무사항 세부 내용
~제24조 개인정보 관리 의무	합당한 노력을 기울여야 함 (제23조) • 조직은 ▲개인정보에 대한 무단 접근, 수집, 이용, 제공, 복제, 수정, 파기 또는 이와 유사한 위험 방지 ▲개인정보가 저장된 저장 매체 또는 장치의 손실 방지 등을 위해 합리적인 보안 조치를 취해야 함 (제24조)
제12조 정책 등 수립 의무	• 조직은 동법에서 부과하는 주요 의무를 이행하는 데에 필요한 정책 및 운영방침을 개발 및 구현하고 동법의 적용과정에서 발생할 수 있는 불만사항 처리 절차를 개발해야 함

Ⅱ. 데이터 프로세서

▶ PDPA는 타 조직을 대신해서 개인정보를 처리하는 조직으로서 '개인정보 중개자(data intermediary)'라는 개념을 두고 있으며, 개인정보 중개자에는 개인정보 침해 통지와 관련한 의무만을 규정

- 개인정보 중개자가 타 조직을 대신하여 그리고 타 조직의 목적을 위해 처리 중인 개인정보에 침해가 발생했다고 믿을 만한 이유가 있는 경우, 중개자는 과도한 지체 없이 해당 타 조직에 침해 발생 사실을 통지해야 함 (제26C조제3항)
- 개인정보 중개자가 공공기관을 대신하여 그리고 공공기관의 목적을 위해 처리 중인 개인정보에 침해가 발생했다고 믿을 만한 이유가 있는 경우, 중개자는 과도한 지체 없이 공공기관에 개인정보 침해 발생 사실을 통지해야 함 (제26E조)

※ 개인정보 침해 통지 의무에 관한 자세한 내용은 '6. 피해 구제 체계'의 'Ⅰ. 데이터 컨트롤러' 부분 참고

4. 행정처분 법적 근거

▶ PDPC는 조직의 개인정보보호 의무 위반에 대해 시정 지시를 내릴 수 있음 (제48I조)

- PDPC는 조직이 동법 제3장~제6B장, 제9장 등에 규정된 개인정보보호 의무를 준수하지 못했다고 판단하는 경우 각 조항의 준수를 보장하기 위해 아래와 같은 지시를 내릴 수 있음
  - ▲동법에 반하는 개인정보의 수집, 이용, 제공 중지 ▲동법에 반하여 수집된 개인정보 파기 ▲개인정보 열람 및 정정 거부나 타 조직으로의 이전 거부 등을 중단하고 개인정보 접근, 정정, 이전 수행 등

▶ PDPC는 고의 또는 과실로 조직이 개인정보보호 의무를 위반한 경우 서면 통지로써 과징금 부과가 가능 (제48J조)

- PDPC가 조직에 과징금을 부과할 경우 아래의 금액을 상한으로 함(동조 제3항)
  - 싱가포르 연간 매출액 1,000만 싱가포르 달러(약 102억 원)를 초과하는 조직에는 최대 싱가포르 연간 매출액의 10%
  - 그 밖의 경우 최대 100만 싱가포르 달러(약 10억 원)

▶ PDPA는 특정 행위가 단순한 위법을 벗어나 범죄로 나아갈 경우 이를 형사범죄로 규정하고 벌금 및 징역으로 처벌 (제51조)

- 권한 없이 타인의 개인정보를 대상으로 열람 또는 정정 요청을 하는 경우 5,000 싱가포르 달러 (약 510만원) 이하의 벌금 및/또는 12개월 이하의 징역에 처할 수 있음 (제51조제2항)
- 개인의 개인정보 열람권 및 정정권 행사를 회피할 목적으로 개인정보 등을 처분, 변경, 위조, 은폐, 파기하거나 타인에게 처분, 변경, 위조, 은폐, 파기를 지시하는 경우 개인은 5,000 싱가포르 달러 (약 510만원) 이하의 벌금 및/또는 12개월 이하의 징역, 그 외의 경우 5만 싱가포르 달러 (약 5,140만원) 이하의 벌금에 처함 (제51조제4항)
- 감독기관, 조사관, 공무원 등의 기능이나 의무 수행, 권한 행사를 방해하거나 감독기관, 조사관 등을 대상으로 고의 또는 무모하게 허위 진술을 하거나 허위 정보 또는 문서를 제공할 경우 개인은 1만 싱가포르 달러 (약 1,030만원) 이하의 벌금 및/또는 12개월 이하의 징역, 그 외의 경우 10만 싱가포르 달러 (약 1억 원) 이하의 벌금에 처함 (제51조제5항)
- 감독기관, 조사관에게 제공했어야 하는 정보 또는 문서를 제공하지 않았다거나 제공을 거부하는 경우, 그리고 동법에 따라 요구되는 감독기관, 조사관에 대한 출두를 거부하는 경우, 개인은 5,000 싱가포르 달러 (약 510만원) 이하의 벌금 및/또는 6개월 이하의 징역, 그 외의 경우 1만 싱가포르 달러 (약 1,030만원) 이하의 벌금에 처함 (제51조제6항)
- 조직이나 공공기관이 보유 또는 관리하는 익명 정보를 고의로 무단 재식별하거나 재식별을 유발할 경우 5,000 싱가포르 달러 (약 510만원) 이하의 벌금 및/또는 2년 이하의 징역에 처할 수 있음 (제48F조)

▶ 한편, PDPA 위반으로 피해를 입은 개인은 특정 요건 하에 소송을 제기하여 권리를 구제받을 수 있음

- PDPA 위반의 결과로 직접적으로 손실이나 피해를 입은 개인은 민사소송을 제기할 수 있으나, 소송은 PDPC가 내린 행정처분 및 행정처분에 대한 이의제기 등 기타 모든 방법을 모두 소진한 후에만 제기할 수 있음 (제48O조)

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

- PDPA는 동법의 개인정보보호 권리 및 의무를 규정하고 있는 제3장~제6B장의 각 조항이 공공기관에 의무를 부과하지 않는다고 규정함으로써 국가기관에 대한 개인정보보호법 적용이 법률상 불가 (제4조제1항)

- 현실적으로도 PDPC가 IMDA의 산하기관으로서 독립성이 결여되어 있으므로 정부부처 및 타 국가기관 등에 대상으로 집행 권한을 행사하는 것이 불가능

5. 개인정보 국외이전 조항

▶ PDPA는 개인정보 국외이전을 원칙적으로 불허하고 있고 예외적 요건이 충족된 경우에 한해 제한적으로 허용

- 조직은 개인정보에 대해 동법상의 보호와 유사한 수준의 보호 수준을 제공하는 경우에만 개인정보를 싱가포르 국외로 전송할 수 있음(제26조제1항 반대해석)
- 그러나 PDPC는 조직의 신청에 따라 서면 통지로써 해당 조직의 개인정보 국외이전과 관련하여 동조 제1항의 요건을 면제할 수 있음 (제26조제2항)
  - 요건 면제는 PDPC가 서면으로 정하는 조건을 붙여 부여될 수 있고, 관보 게재가 별도로 필요 없는 대신 PDPC가 언제든지 취소할 수 있음 (제26조제3항)
- 한편, PDPC는 동조에 따라 부과된 조건을 추가, 변경 및 삭제할 수 있음 (제26조제4항)

6. 피해 구제 체계

Ⅰ. 데이터 컨트롤러

▶ 조직은 개인정보 침해 사고가 발생한 경우 PDPC 및 영향을 받은 개인에게 통지해야 할 의무를 부담 (제26C조~제26D조)

- 조직은 보유 또는 관리 중인 개인정보에 침해가 발생했다고 믿을 만한 이유가 있는 경우, 먼저 해당 침해 사실이 통지가 필요한 침해인지 여부에 대한 평가를 합리적이고 신속하게 수행해야 함 (제26C조)
  - 통지가 필요한 침해란 ▲영향을 받는 개인에게 심각한 피해를 초래 또는 초래할 가능성이 있는 경우이거나 ▲침해가 상당한 규모이거나 또는 그럴 가능성이 있는 경우 등을 의미
- 조직이 상기 과정을 통해 통지가 필요한 침해라고 평가하는 경우 해당 평가를 실시한 날로부터 3일 이내에 PDPC에 통지해야 하며, 이후 영향을 받은 각 개인에게도 합리적인 방법으로 통지해야 함 (제26D조)
  - 특히, PDPC에 대한 통지는 PDPC가 요구하는 형식대로 제출되어야 하며, 당시 조직이 알고 있던 최선의 정보를 모두 포함해야 함
- 한편, PDPC는 개인정보 침해 사고가 발생한 조직의 통지의무를 지원하기 위해 온라인 자체 평가 도구(https://www.pdpc.gov.sg/Report-Data-Breach/Self-Assessment)를 개발하여 서비스 중이며, 통지의무를 온라인에서 간편하게 실행할 수 있도록 온라인 침해 통지 제출

웹페이지(https://eservice.pdpc.gov.sg/case/db)를 운영 중

Ⅱ. 정보주체

▶ PDPA는 개인의 PDPC에 대한 민원 제기 권리를 명시적으로 부여하고 있지 않지만 여러 조항에 걸쳐 해당 권리에 대해 간접적으로 언급하고 있으며, 권리의 행사 방법, 절차 등 자세한 내용에 대해서는 하위규정으로 위임

- 모든 조직은 동법의 적용과 관련해 발생할 수 있는 민원을 접수하고 대응하는 프로세스를 개발해야 함 (제12조제b호)
- PDPC는 조직에 대한 개인의 민원사항이 조정을 통해 해결되는 것이 보다 적절하다고 판단되는 경우, 조직 및 민원인의 동의 없이 분쟁해결 절차에 따라 해당 민원을 조정에 회부할 수 있음 (제48G조)
- PDPC는 민원인의 민원 제기에 따라, 조직의 개인정보 열람·정정·이전 거부 및 지연, 과도한 수수료 요구 등에 대해 검토할 수 있음 (제48H조)
- PDPC는 민원인의 민원 제기 혹은 자체적인 결정에 따라 동법에 따른 조사를 실시할 수 있음 (제50조)
- PDPC는 장관의 승인을 얻어 민원 제기의 형태, 방법 및 절차와 관련한 하위규정을 제정할 수 있음 (제65조)
- 한편, PDPC는 개인이 개인정보보호 권리 침해 발생 시 민원을 접수할 수 있도록 온라인 민원 신청 페이지*를 운영함으로써 민원신청의 편의를 제공 중[13)]

  * https://www.pdpc.gov.sg/Complaints-and-Reviews/Report-a-Personal-Data-Protection-Concern

7. 개인정보 법제 준수 지원 현황

지침/가이드라인	개요	발행일
AI 추천 및 의사결정 시스템에서의 개인정보 사용에 관한 지침[14)]	• AI 시스템 개발 및 배포 시 개인정보 수집의 예외적 요건, 수집 및 이용 시 조직의 의무 규정	'24.3.1.
딥페이크 사기에 대한 탐지 및 대응 권고사항[15)]	• 딥페이크 사기에 대한 탐지를 위한 접근법 및 사기 대응 방법에 대한 상세한 설명 제공	'24.3.21.
디지털 환경에서의 아동 개인정보에 관한 PDPA 지침[16)]	• 디지털 환경에서 아동의 개인정보를 다루는 조직에게 PDPA의 적용 방법을 명확히 하기 위하여 상세한 설명 제공	'24.3.28.

13) 다만 민원 제기 시 싱가포르 거주자가 발급받을 수 있는 디지털 ID인 SingPass 인증이 필요
14)https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-use-of-personal-data-in-

지침/가이드라인	개요	발행일
IoT 기기 보호에 관한 권고사항[17]	• IoT 기기 보호 방법, IoT 기기 침해 시 대응 방법에 대한 상세한 설명 제공	'24.6.5.
개인정보 보호 강화 기술(PET): 합성정보 생성에 관한 지침[18]	• 합성정보 생성 시 개인정보 보호를 위한 구체적인 방법과 고려사항 상세히 제공	'24.7.15.

▶ AI 추천 및 의사결정 시스템에서의 개인정보 사용에 관한 지침

- 본 지침은 조직이 AI 시스템을 개발하고 배포할 때 정보주체의 동의 없이 개인정보를 사용할 수 있는 예외적인 경우에 대하여 명확히 규정하는 것을 목적으로 함
- 조직이 AI 시스템 개발, 테스트 및 모니터링 시 개인정보를 정보주체의 동의 없이 사용할 수 있는 예외적인 경우로, ▲비즈니스 개선 예외(Business Improvement Exception), ▲연구 예외(Research Exception)를 명시함
  - 조직은 ▲기존 상품 및 서비스 개선 또는 새로운 상품·서비스 개발, ▲비즈니스 운영 방법 개선 또는 새로운 운영 방법 개발, ▲개인의 행동 및 선호도 이해, ▲개인에게 적합한 상품·서비스 식별 또는 맞춤화의 목적으로 동의 없이 개인정보 사용 가능
  - 조직은 연구 목적으로 개인정보를 동의 없이 사용할 수 있으나, ▲연구 목적이 식별 가능한 형태의 개인정보 없이는 합리적으로 달성될 수 없는 경우여야 하고, ▲연구 목적으로 개인정보를 사용하는 공익이 명확하게 존재하며, ▲연구 결과가 개인에게 영향을 미치는 결정에 사용되지 않아야 하고, ▲연구 결과 발표 시 개인을 식별할 수 없는 형태로 발표되어야 하는 조건을 충족해야 함
- 조직이 AI 시스템에서 개인정보 수집·이용할 때의 동의 및 통지의무(Consent and Notification Obligations), 책임의무(Accountability Obligation)를 명시함
  - 조직은 AI 시스템에서 개인정보를 수집·이용할 때 정보주체에게 개인정보 수집·사용 목적을 명확히 알려야 하고, 정보주체의 동의를 얻어야 하며, 팝업 알림에 더 자세한 정보 링크를 포함하는 등 정보를 계층화(layering)[19]하여 제공해야 함
  - 조직은 개인정보 처리에 대한 책임을 다하기 위하여, 내부 정책 및 관행을 개발해야 하고, 이러한 정책 및 관행에 대한 정보를 정보주체가 요청할 경우 제공해야 함

ai-recommendation-and-decision-systems.pdf

15) https://www.csa.gov.sg/alerts-advisories/Advisories/2024/ad-2024-006

16) https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-pdpa-for-children's-personal-data-in-the-digital-environment_mar24.pdf

17) https://www.csa.gov.sg/alerts-advisories/Advisories/2024/ad-2024-012

18) https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/proposed-guide-on-synthetic-data-generation.pdf

19) 팝업 알림을 통해 가장 기본적인 정보를 제공하고, 개인정보처리방침을 팝업의 링크를 통하여 접근가능하게 한 후, 사용자가 관심 있는 특정 주제에 대해 개인정보처리방침 내의 '더 보기'를 클릭하여 상세 정보를 확인할 수 있도록 하는 유형의 방법 의미

▶ 딥페이크 사기에 대한 탐지 및 대응 권고사항

- 딥페이크 사기(deepfake scams) 탐지를 위한 접근법과 사기 대응 방법에 대한 상세한 설명을 제공
- 딥페이크 탐지를 위한 3A 접근법 제시
  - ▲메시지의 출처를 신뢰할 수 있는지, 맥락과 목적을 확인하여 메시지를 평가(Assess the message)하고, ▲얼굴 특징이나 표정 등을 확인하여 시청각 요소를 분석하며(Analyse audio-visul elements), ▲AI 기반 분석 도구 등을 사용하여 콘텐츠 인증(Authenticate Content Using Tools)
- 의심스러운 콘텐츠 발견 시 즉시 플랫폼 관리자에게 신고하고, 국가범죄예방위원회(NCPC) 사기방지 헬프라인 또는 ScamAlert 웹사이트(scamalert.sg) 활용하여 대응
- 온라인에서 공유되는 개인정보와 이미지를 최소화하고, 소셜 미디어 플랫폼의 개인정보 설정을 정기적으로 업데이트하며, 딥페이크에 사용될 수 있는 개인 사진, 오디오, 비디오의 온라인 공유를 제한하여야 함

▶ 디지털 환경에서의 아동 개인정보에 관한 PDPA 지침

- 디지털 환경에서 아동의 개인정보를 다루는 조직에게 PDPA의 적용 방법을 보다 명확히 하기 위하여 상세한 설명 제공
- (적용 범위) 본 지침은 아동이 접근할 가능성이 있는 온라인 제품이나 서비스를 제공하는 조직에게 적용됨
  - 본 지침이 적용되는 온라인 제품 또는 서비스의 구체적인 예시로, ▲소셜 미디어 서비스, ▲기술 지원 학습(EdTech), ▲온라인 게임, ▲스마트 장난감 및 기기를 제시함
- (통지) 조직은 아동과 의사소통할 때 아동이 쉽게 이해할 수 있는 언어를 사용해야 하고, 이는 개인정보 수집 목적 통지, 동의 조항, 개인정보 보호 정책, 이용 약관 등 관련 사항에 모두 적용됨
- (동의) 13~17세 아동은 개인정보의 수집, 사용 및 공개 및 동의 철회에 관한 정책을 쉽게 이해할 수 있다면 스스로 유효한 동의를 할 수 있다고 간주되나, 13세 미만 아동은 부모나 보호자의 동의를 얻어야 하며, 조직은 필요에 따라 더 높은 연령의 동의 기준을 적용할 수 있음
- (합리적 목적) 조직은 합리적인 목적으로만 아동의 개인정보를 수집, 이용, 공개해야 함
  - 위 합리적인 목적의 예시로, ▲연령에 적합한 콘텐츠 접근을 위한 연령 확인, ▲유해하고 부적절한 콘텐츠로부터 아동 보호, ▲안전 정보 제공[20]을 위한 아동의 개인정보 활용을 제시하고 있음

20) 온라인 플랫폼이나 서비스에서 아동의 행동을 관찰하고 검색 기록, 입력한 텍스트 등 개인정보를 수집하고, 수집된 개인정보 중에서 '자해방법', '우울증', '자살 생각' 등의 검색어를 포함하여 아동이 위험에 처할 수 있음을 나타내는 신호를 식별하여 감지되면 시스템은 아동에게 자살 예방 핫라인 번호, 상담 서비스 정보 등을 포함하여 아동에게 도움이 될 수 있는 안전정보를 제공함

- (위치정보) 위치정보는 개인을 식별할 수 있는 개인정보로 간주되는데, 조직은 아동의 안전을 위해 위치정보 기능을 기본적으로 비활성화하고, 대략적인 위치정보만 수집하는 등의 안전 장치를 구현하여야 함
- (아동 개인정보 보호) 아동의 개인정보는 일반적으로 민감정보로 간주되며, 더 높은 수준의 보호가 필요하고, 조직은 PDPC의 'ICT 시스템을 위한 데이터 보호 관행 가이드'에 나열된 기본 및 고급 관행[21]의 보호 수준을 구현해야 함
- (유출 통지) 개인정보 유출 시 조직은 영향을 받은 아동에게 통지해야 하고, 가능한 경우 부모나 보호자에게도 통지하여야 하며, 통지는 아동이 쉽게 이해할 수 있는 언어로 작성되어야 함
- (책임성) 조직은 아동이 접근할 가능성이 있는 제품이나 서비스를 출시하기 전에 데이터 보호 영향평가(DPIA)를 수행하도록 권장

▶ IoT 기기 보호에 관한 권고사항

- IoT의 취약점에 따른 IoT 기기 보호 방법, IoT 기기가 침해된 경우 대응 방법에 대한 상세한 설명 제공
- IoT는 편리성, 효율성에도 불구하고, 취약한 비밀번호, 안전하지 않은 네트워크 서비스, 안전하지 않은 인터페이스, 안전하지 않은 개인정보 보호 등을 취약점으로 가짐
- IoT 기기 보호 방법으로, ▲강력한 암호와 다중 인증(MFA) 사용, ▲정기적인 펌웨어 및 소프트웨어 업데이트, ▲불필요한 인터넷 연결 제한, ▲신뢰할 수 있는 제조업체의 제품 구매 등을 제시함
- IoT 기기 침해 시 대응방안으로, 기기를 인터넷에서 분리하고, 기기 접속 정보를 변경하거나 공장 초기화를 수행하고, 제조업체에 지원 요청할 것을 제시

▶ 개인정보 보호 강화 기술(PET): 합성정보 생성에 관한 지침

- 합성정보(synthetic data) 생성 시 개인정보 보호를 위한 구체적인 방법 및 고려사항을 상세히 설명
- (PET의 정의와 유형) PET(Privacy Enhancing Technologies)는 '개인정보나 상업적으로 민감한 개인정보를 노출하지 않으면서 데이터 처리, 분석 등을 가능하게 하는 도구와 기술의 모음'을 의미
  - 본 지침에서는 PET를 ▲데이터 난독화(Data obfuscation), ▲암호화된 개인정보 처리(Encrypted data processing), ▲연합 분석(Federated analytics)로 분류함
- (합성정보의 정의) 합성정보란 '일반적으로 목적에 맞게 구축된 수학적 모델(인공지능(AI)·

21) 기본 관행(Basic Practices)에는 계정 및 접근 제어, 백업 및 보존, 비밀번호 등에 관한 정책을 포함하여 개인정보 보호를 위한 ICT 보안 정책을 개발하고 구현하며, ICT 서비스의 아웃소싱 또는 외부 업체 활용과 관련된 보안 위험을 평가하는 것이 포함되고, 고급 관행(Enhanced Practices)에는 개인정보에 대한 관리자 접근 시 일회용 비밀번호(OTP) 또는 2단계 인증, 다중 인증(MFA)을 사용하고 모든 접근을 기록화하는 것이 포함됨

기계학습(ML) 모델 포함) 또는 알고리즘을 사용하여 생성된 인공적인 데이터'를 지칭함

- (개인정보 보호) 합성정보는 인공적으로 생성된 개인정보이지만, 합성정보가 다른 공개된 정보를 결합할 경우 개인을 식별할 가능성이 있어 데이터 준비 단계 시 개인정보 보호를 위한 조치가 필요하고, 합성정보 생성 후에는 재식별 위험 평가를 수행해야 함
  - 데이터 준비 단계에서 필요한 속성만을 선택하여 불필요한 개인정보 노출을 방지하는 '데이터 최소화'가 필요하고, 이름, 주민등록번호 등 개인을 직접 식별할 수 있는 정보를 제거하거나 가명으로 대체하여야 하며, 필요한 경우 상세 정보를 더 넓은 범주로 일반화하고, 차등 프라이버시 등의 기술을 사용하여 데이터에 노이즈를 추가해야 함
  - 합성정보 생성 후 고유한 특성을 가진 개인을 식별할 수 있는지 평가하고, 합성정보와 다른 정보를 연결하여 개인을 식별할 수 있는지 평가하는 등 재식별 위험 평가를 수행해야 함

8. 최근 행정처분

▶ 민원 접수 숫자 및 처분 사례 건수 등 ('23년 기준)

- (민원 접수) PDPC에 접수된 '23년 총 문의 건수는 약 5,600건으로, 그중 2,800건은 단순 문의를 넘어선 개인정보보호 관련 민원 제기 건에 해당[22)]
- (행정처분 사례) '23년 기준 PDPC가 부과한 행정처분 사례는 총 15건[23)]

▶ 개인정보보호 위반에 대한 PDPC의 최근 행정처분 사례는 다음과 같음

대상	처분일시	위반사항 개요	내역
Horizon Fast Ferry	'24.2.	• 보안 조치 소홀로 인하여 개인정보 유출 초래	• 과징금 2만 8천 싱가포르 달러 부과
Keppel	'24.5.	• 보안 조치 소홀로 인하여 개인정보 무단 접근 및 유출 초래	• 과징금 12만 달러 싱가포르 달러 부과
CASE[24)]	'24.7.	• 보안 조치 소홀로 인하여 개인정보 유출 초래	• 과징금 2만 싱가포르 달러 부과

22) https://www.pdpc.gov.sg/help-and-resources/2020/04/enquiry-and-complaint-figures
23) 행정처분 건수에 대해 PDPC의 공식 통계자료가 존재하지 않지만 PDPC 웹사이트의 'Enforcement Decisions' 탭에서는 PDPC가 내린 행정처분 결정례를 전체 공개하고 있는데, '23년 PDPC가 부과한 행정처분은 위반사항이 없는 것으로 결론이 난 사례를 제외하면 총 15건이었음
https://www.pdpc.gov.sg/All-Commissions-Decisions?keyword=&industry=all&nature=all&decision=advisory-notice%7Cdirections%7Cfinancial-penalty%7Cwarning&penalty=all&page=1
24) 싱가포르 소비자협회(Consumers' Association of Singapore)

▶ **개인정보보호를 위한 합리적인 보안조치를 마련하지 않아 개인정보 유출 사고를 초래한 Horizon Fast Ferry에 대하여 과징금 부과('24.2.)[25]**

- (사건 개요) 싱가포르 기반의 페리 운영사인 Horizon Fast Ferry의 웹사이트를 통해 티켓을 예약한 약 10만 명의 개인정보가 유출됨
  - 유출된 개인정보에는 이름, 여권번호, 생년월일, 여권 발급일 및 만료일, 국적 등이 포함되어 있었음
  - 위 회사에는 자체 IT 부서가 없어 웹사이트 구축을 위해 외부 벤더에게 접근 권한을 부여한 후, 회사는 '23년 3월부터 개인정보가 유출되었음을 알리는 다수의 랜섬웨어 이메일을 수신하게 됨
  - PDPC는 회사가 벤더 관리를 부실하게 하였고, ICT 정책이 전혀 없었으며, 웹 서버에 보안 솔루션을 구현하지 않았다는 이유로 PDPA 제24조[26]를 위반하였다고 판단함

- (조치 내용) PDPC는 보안 조치를 다 하지 않아 개인정보 유출 사고를 초래한 회사에 PDPA 제24조 위반을 이유로 2만 8천 싱가포르 달러(약 2,800만 원)의 과징금을 부과
  - PDPC는 개인정보 유출이 약 10만 명의 정보주체에게 영향을 미쳤고, 여권 정보와 같은 민감정보가 포함되었으며, 위 회사가 '19년 5만 4천 싱가포르 달러의 과징금을 부과받고 '20년에도 경고 조치를 받은 사실이 있음에도 PDPA를 위반한 사실 등을 종합하여 위와 같은 과징금 부과함
  - 이와 함께, PDPC는 위 회사에 ▲PDPA의 의무 및 요구사항에 대하여 관리자들을 교육하고, ▲회사의 시스템과 웹사이트 접근 및 관리를 위해 IT 지원 벤더와 서면 계약을 체결하며, ▲회사로 하여금 IT 지원 벤더에게 필요한 IT 지식을 갖춘 직원을 지정하고, ▲개인정보 보호에 관한 내부 지침을 강화할 것 등을 구하는 시정 조치를 명함

▶ **개인정보보호를 위한 합리적인 보안조치를 마련하지 않아 개인정보 유출 사고를 초래한 Keppel Telecommunications & Transportation에 대하여 과징금 부과('24.5.)[27]**

- (사건 개요) 싱가포르에 본사를 둔 물류 및 데이터 센터 서비스를 제공하는 Keppel의 서버가 해킹되어 서버에 저장된 개인정보가 무단 접근된 후 유출됨
  - 회사는 자회사인 Keppel Logistics와 공유하던 서버에 있던 개인정보를 이전하면서, 원래 서버에 남아있던 개인정보를 삭제하지 아니하였고, 위 자회사를 타사에 매각하는 과정에서도 원래 서버에 남아있던 개인정보를 삭제하지 아니함
  - 이처럼 회사가 개인정보를 삭제하지 아니함에 따라, 해커가 서버에 저장된 개인정보에 무단 접근하여 약 2만 명의 개인정보[28]가 무단 접근 및 유출 위험에 노출되었고, 실제

25) https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/commissions-decisions/gd_horizon-fast-ferry-pte-ltd_21022024.pdf
26) 조직이 소유하거나 통제하는 개인정보를 보호하기 위하여 합리적인 보안 조치를 마련해야 한다는 규정
27) https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/commissions-decisions/gd_horizon-fast-ferry-pte-ltd_21022024.pdf
28) 서명 견본, 신분증 전체 이미지, 은행 계좌 번호 등이 포함됨

약 7천 명의 개인정보가 실제로 유출되었을 것으로 보임
- PDPC는 회사가 개인정보 이전 과정이나 자회사 매각 과정에서 원래 서버에 남아있던 개인정보를 삭제하였어야 함에도 과실로 보안조치 의무를 위반하였다고 판단함

• (조치 내용) PDPC는 보안 조치를 다하지 않아 개인정보 유출 사고를 초래한 회사에 PDPA 제24조 위반을 이유로 12만 싱가포르 달러(약 1억 2천만 원)의 과징금을 부과
- PDPC는 회사가 2년 이상 장기간 규정을 미준수한 점, 영향받은 정보주체의 수가 약 2만 명에 달하고 실제 유출되었을 것으로 보이는 정보주체의 수는 약 7천 명에 달하는 점, 유출위험에 노출된 개인정보의 민감성, 회사의 매출 규모 등을 종합하여 과징금 액수 산정
- 다만, PDPC는 회사가 신속하게 사후 조치와 재발 방지 노력을 다하였고, 위반 사실을 자인하였으며, 조사 과정에서의 협조적 태도를 고려하여 과징금 액수 제한

▶ 개인정보보호를 위한 합리적인 보안조치를 마련하지 않아 개인정보 유출 사고를 초래한 CASE에 대하여 과징금 부과('24.7.)[29]

• (사건 개요) CASE 공식 계정이 해킹되어 계정에 보관 중이던 소비자들[30] 의 이메일 주소가 유출되어, 해당 이메일 주소로 위 공식 계정 명의로 피싱 이메일이 발송됨
- PDPC는 CASE가 비밀번호를 얼마나 자주 변경해야 하는지에 대한 자체 정책을 채택하고 시행하지 못하였고, 벤더(Vendor)와의 계약에 ICT 시스템 및 개인정보와 관련한 명확한 보안 책임을 명시하지 아니하였다고 판단함
- 또한, PDPC의 조사 결과 CASE가 관련 벤더(vendor)와 체결한 일부 계약에 ICT 시스템 및 개인정보와 관련한 명확한 보안 책임이 명시되지 않았다고 판단함
- 나아가, CASE는 직원들에게 정기적인 보안 인식 교육(security awareness training)을 실시하지 못하였음을 자인함
- 아울러, PDPC는 CASE가 1차 데이터 유출 사고 발생 이전 보안 패치나 소프트웨어 업데이트를 다루는 ICT 정책을 시행하지 아니하였음을 확인함

• (조치 내용) PDPC는 보안 조치를 다하지 않아 개인정보 유출 사고를 초래한 CASE에 PDPA 제12조제a항[31], 제24조[32] 위반을 이유로 2만 싱가포르 달러(약 2,055만원)의 과징금을 부과
- 이와 함께, PDPC는 CASE에 ICT 정책 및 비밀번호 관련 정책을 포함하여 개인정보 보호와 관련된 정책을 업데이트하고, 보안 취약점의 해결할 것을 구하는 시정조치를 명함

29) https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/commissions-decisions/gd_consumers-association-of-singapore_09072024.pdf
30) CASE 회원이 아니라, CASE에 불만을 제기하거나 도움을 요청한 일반 소비자들
31) 조직(organization)이 PDPA에 규정된 의무 사항을 이행하기 위하여 필요한 정책과 관행을 개발하고 실행해야 한다는 규정
32) 조직이 소유하거나 통제하는 개인정보를 보호하기 위하여 합리적인 보안 조치를 마련해야 한다는 규정

9. 시사점

▶ PDPC는 사업자의 PDPA 제24조 위반을 이유로 다수의 과징금 부과 등 처분을 내리고 있어 보안 조치 강화 필요성 대두됨

- PDPC의 최근 행정처분 사례들을 보면 개인정보 유출 사고의 주요 원인을 부적절한 보안 조치로 판단하고, 기업의 PDPA 제24조 위반을 이유로 다수의 과징금 부과 등 행정처분을 내리고 있는 것으로 보임
  - 특히, PDPC의 과징금 부과 상한을 높여 기업의 매출 규모를 고려하여 12만 싱가포르 달러(약 1억 2천만 원)에 달하는 과징금을 부과한 사례가 확인됨
- 외부 벤더 활용 시 계약서에 보안 책임을 명확하게 명시하고, 벤더의 보안 수준이 유지되는지 지속적으로 모니터링할 필요가 있다고 판단됨
  - Horizon Fast Ferry 사례와 같이, 벤더 관리 소홀의 경우 기업의 책임으로 인식되어 과징금 부과의 원인이 될 수 있음
- 또한, 명확한 내부 정책 수립과 내부 직원을 대상으로 한 정기적인 보안 교육이 필수적이므로 싱가포르 진출 기업들은 위 정책을 수립하고 교육을 시행해야 함
  - CASE 사례와 같이, 특히 비밀번호 정책, ICT 시스템 관리 정책 등을 구체적으로 수립하고 이행하여야 함

▶ 싱가포르는 AI 시스템 활용 시 컨트롤러의 의무사항을 부과하고 있고, 아동의 개인정보와 관련하여 엄격한 기준을 부여하는 지침을 발행하여, 현지 진출 기업들의 지침 숙지 및 준수 당부

- PDPC는 '24년 AI 추천 및 의사결정 시스템 활용 시 컨트롤러의 동의·통지 의무를 명확히 규정하고, AI 시스템의 개인정보 처리에 대한 내부 정책 및 관행 개발 및 문서화에 대한 책임성 의무를 명시하는 지침을 발행한바, 현지 진출 기업들의 지침 준수 당부
  - 다만, 위 지침에서 비즈니스 개선 예외, 연구 예외 등 예외적으로 개인정보를 활용할 수 있는 경우를 규정하고 있으므로, AI 시스템을 활용하여 개인정보를 활용하는 현지 진출 기업들의 경우 위 예외 조항에 해당하는지 여부를 확인하여 볼 필요가 있음
- 이외에도 PDPC는 디지털 환경에서 아동의 개인정보를 다루는 기업에 대하여 연령에 맞는 동의 절차, 이해하기 쉬운 개인정보처리방침, 위치정보 보호 등에 특별한 주의 의무를 부과하는 지침을 발행한바, 아동의 개인정보를 처리하는 기업들의 경우 해당 지침 준수 당부