

# 남아프리카공화국 개인정보보호법(POPIA)의 주요 내용과 시사점

김예진 세계지역연구센터 신남방경제실 아프리카중동팀 전문연구원 (kimyj@kiep.go.kr, Tel: 044-414-1116)



## 차 례

1. 배경
2. 주요 내용
3. GDPR과의 비교
4. 평가 및 시사점

## 주요 내용

- ▶ 2020년 7월 1일에 발효된 남아프리카공화국 개인정보보호법(POPIA: Protection of Personal Information Act)의 유효기간이 2021년 6월 30일에 종료됨에 따라 2021년 7월 1일부로 모든 조항에 관한 실질적인 준수 의무가 부여됨.
- ▶ POPIA는 EU의 개인정보보호법(GDPR: General Data Protection Regulation)과 유사한 내용을 담고 있으나 적용 대상과 범위, 처벌 수준, 정보책임자의 책임범위 등에서 차이를 보임.
  - [적용 대상] GDPR은 정보주체를 살아 있고 식별 가능한 자연인으로 보나 POPIA는 법인도 정보주체로 포함함.
  - [적용 범위] POPIA는 남아공 내에 사업장이 있거나 개인정보를 처리하는 경우에 관해 법률을 적용하나 GDPR은 역외에서 개인정보를 처리하더라도 EU에 있는 정보주체에게 재화나 서비스를 제공하거나 EU 내에 있는 정보주체의 활동을 모니터링하는 경우에도 법률을 적용함.
  - [처벌] 법률을 미준수할 경우 GDPR은 과징금만 부과하고 있으나 POPIA는 이를 범법행위로 보고 구속형도 부과할 수 있음.
  - [정보책임자의 책임] GDPR과 POPIA 모두 정보책임자(컨트롤러) 및 정보처리자(프로세서)에게 개인정보의 기밀 보장 의무 준수를 위한 안전조치를 마련하도록 하고 있으나 POPIA의 경우 이에 대한 입증 및 책임은 전적으로 정보책임자에게 있음.
- ▶ POPIA와 GDPR 간 세부적인 차이점이 있지만 이미 GDPR을 준수하고 있는 기관들은 POPIA를 용이하게 준수할 수 있을 것으로 보임.
  - 2021년 7월 1일부로 POPIA가 전적으로 발효되었기 때문에 아직 개인정보보호 위반사항에 대한 해석과 감독기관(IR)의 판단이 명확하지 않은 만큼 GDPR의 해석 및 적용 사례가 유용한 참고자료가 될 것으로 보임.
- ▶ POPIA에 저촉하지 않기 위해 남아공의 주요 교역국에서 유사한 수준의 개인정보보호 규제를 마련할 것으로 보이며, 이러한 규제의 수렴을 통해 아프리카의 교역 환경 개선에 기여할 수 있을 것으로 보임.
  - 일관된 규제의 부재는 국별로 상이한 규제를 준수하기 위한 비용을 증가시키고 데이터의 자유로운 이동을 저해함.

## 1. 배경

■ 인터넷 접근성 향상과 새로운 기술 발전으로 국경간 데이터 거래가 증가하면서 여러 국가에서 개인정보보호를 위한 규제를 마련하고 있음.

- 유럽연합(EU)은 2016년에 개인정보보호법(GDPR: General Data Protection Regulation)을 발효하여 회원국별로 상이하던 개인정보보호 규제를 일원화하고 구체화하였음.
  - EU는 1995년에 개인정보보호 지침(Directive)을 마련하였으나 국내 입법 과정을 거치며 회원국별로 지침을 상이하게 적용하고 시행함. 이를 보완하기 위해 EU는 2012년에 별도의 국내 입법 과정이 불필요하여 발효 즉시 효력을 지닌 개정안을 발표함.<sup>1)</sup>
- 미국의 경우 연방 차원의 개인정보보호법은 없으나 특수 산업에 대한 개인정보보호법이 존재함. 주 단위에서는 캘리포니아가 2018년에 최초로 포괄적인 소비자정보보호법(CCPA: California Consumer Privacy Act)을 제정, 2020년 1월부터 시행함.<sup>2)</sup>
  - CCPA는 미국 내에서 개인정보보호법의 표준으로 자리매김하고 있어 뉴욕, 메릴랜드, 매사추세츠, 하와이 등에서 CCPA의 내용을 반영한 개인정보보호법을 검토, 제정 중임.<sup>3)</sup>
- 인도, 중국, 브라질, 태국, 칠레 등에서도 GDPR과 유사한 범위의 개인정보보호법을 시행 중이거나 검토 중임.
  - 브라질과 태국은 각각 2020년과 2021년에 개인정보보호법을 발효하였으며 칠레와 인도는 2021년에 발효 예정임. 중국의 경우에도 2020년에 초안을 공개하였으며 2021년 제정될 것으로 예상됨.<sup>4)</sup>

■ 아프리카에서도 디지털 접근성이 확대되면서 디지털 플랫폼의 활용이 증가하고 있음.

- 아프리카의 인터넷 접근성은 여전히 낮은 수준이나 가장 빠른 성장률을 보임.
  - 2019년 기준 아프리카의 인터넷 사용률은 29%로 아프리카 외 세계 평균인 66%와 격차가 크지만 2005~19년 아프리카 외 국가들의 인터넷 사용률은 약 4배 증가한 반면 아프리카의 인터넷 사용률은 10배 증가함.<sup>5)</sup>
  - 아프리카의 인터넷 접근성 확대 배경에는 모바일 인터넷 사용 증가가 자리하고 있는데, 2010년 1.7% 수준이었던 모바일 브로드밴드 가입 비율이 2020년에는 33%로 늘어남.<sup>6)7)</sup>
  - 특히 남아공의 경우 사하라이남 아프리카 최초로 2020년에 대규모 5G망을 구축하였고, 사하라이남 아프리카 IoT 사용률의 절반을 차지하는 등 아프리카의 모바일 산업을 선도하고 있음.<sup>8)</sup>

1) 오태현, 강민지(2018. 5. 25), 「EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안」, 오늘의 세계경제, p. 18, 대외경제정책연구원.

2) 연방 차원에서는 보건의로 분야(Health Insurance Portability and Accountability Act 1996), 금융 분야(Gramm-Leach, Bliley Act 1999), 아동(Children's Online privacy Protection Act 2000) 등 특수 산업/분야에 대한 개인정보보호법만 존재하며 데이터 보안에 대한 포괄적 법적 규제는 캘리포니아가 최초로 마련함.

3) Andy Green(2021. 2. 4), "Complete guide to privacy laws in the US," Varonis, <https://www.varonis.com/blog/us-privacy-laws/>(검색일: 2021. 6. 26).

4) Dan Simmons(2021. 1. 12), "13 Countries with GDPR-like data privacy laws," Comforte, <https://insights.comforte.com/13-countries-with-gdpr-like-data-privacy-laws/>(검색일: 2021. 6. 26).

5) 인터넷 사용률은 전체인구 대비 인터넷 사용 인구의 비율을 의미함. ITU(2020. 11), "Statistics: Global and Regional ICT Data," <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>(검색일: 2021. 6. 26).

6) *Ibid.*

7) 모바일 브로드밴드 가입 비율은 인구 100명당 256kbit/s 이상의 속도가 나오는 상품 가입자 수의 비율을 의미함.

8) GSMA(2020), *The Mobile Economy Sub-Saharan Africa 2020*, p. 20, London.

- 이와 같은 모바일 산업의 성장으로 온라인 상거래가 활성화되고 디지털 금융시장도 성장하고 있음.
  - 2020년 기준 모바일 산업은 사하라이남 아프리카 GDP의 9%(1,610억 달러)를 차지함.<sup>9)</sup>
  - 특히 코로나19로 인해 비대면 결제 및 거래가 크게 증가하였는데, Visa에서 진행한 설문에 의하면 남아공 응답자의 64%는 코로나19로 인해 온라인에서 처음으로 식료품을 구매하였다고 응답함.<sup>10)</sup>
  - 지난 2년간 Vodacom, Orange, Safaricom, Airtel, MTN 등 아프리카의 주요 통신업체들은 Visa, Mastercard, Orange Bank 등의 금융서비스 제공기관과 협력관계를 구축하고 모바일 결제 시스템을 확대함.<sup>11)</sup>

■ 이에 아프리카연합(AU)과 회원국들은 아프리카의 디지털 경쟁력을 강화하고 국제 규범과 조화를 이루고자 범아프리카 공동의 목표를 설정하고 국별로 개인정보보호를 위한 법적, 제도적 장치를 마련하고 있음.

- 현재 28개 아프리카 국가에서 개인정보보호법을 시행하고 있으며 9개국에서 법안을 입안 중이나 국별로 개인정보를 적용하는 범위나 정보책임자 및 처리자의 의무가 달라 오히려 무역 확대, 투자 증진 및 ICT 산업의 성장에 저해가 될 수 있다는 시각이 존재함(그림 1 참고).<sup>12)</sup>
  - 일관된 규제가 부재할 경우 국별로 상이한 규제를 준수하기 위한 비용이 증가하고, 데이터의 자유로운 이동을 저해해 기업들이 아프리카가 아닌 해외에 데이터 서버를 구축하게 되고, 이에 따라 기밀 또는 전략적 중요성이 높은 데이터를 해외 서버에 저장할 수밖에 없는 안보적 위협 또한 증가함.<sup>13)</sup>
- AU 및 회원국들은 아프리카의 경제통합과 디지털 경쟁력 강화, 사이버보안 강화를 위해 일관된 규제가 필요함을 인식, 아프리카 내 디지털경제 관련 정책 및 규제를 조화시키고 단일의 디지털시장을 형성하기 위한 여러 전략 및 정책을 마련함.
  - AU는 2008년에 정보통신 정책 및 규제의 조화에 대한 연구보고서를 통해 정책 조화의 중요성을 강조하였으며, 2014년에 'AU 사이버보안 및 개인정보보호 협약'을 채택하고 개별 국가 단위에서 협약 이행을 구체화할 수 있는 가이드라인을 발표함.<sup>14)</sup>
  - 2021년에는 '아프리카 디지털 변환 전략(2020~30)'을 발표하여 아프리카의 산업화를 위한 디지털 기술 개발과 혁신을 지원하는 전략을 제시함.
  - 30개의 아프리카 국가들로 구성된 '스마트아프리카연합(Smart Africa Alliance)'은 AU, 국제전기통신연합(ITU), 세계은행, 아프리카개발은행(AfDB), 유엔아프리카경제위원회, 세계이동통신사업자연합회(GSMA) 등과 협력 관계를 구축하여 아프리카 내 단일 디지털 시장을 이루고자 함.
  - AU, EU 및 ITU의 공동 계획인 '디지털 아프리카를 위한 정책 및 규제 이니셔티브(PRIDA: Policy and Regulation Initiative for Digital Africa)'는 아프리카 국가간 데이터 정책과 규제의 조화를 추구하고, ICT와 타 산업의 융합을 지원하며, 디지털 경제 관련 국제 논의에서 아프리카 이해관계자들의 목소리를 높이고자 함.

9) GSMA(2019), *The Mobile Economy Sub-Saharan Africa 2019*, p. 15, London.

10) GSMA(2020), *The Mobile Economy Sub-Saharan Africa 2020*, p. 23, London.

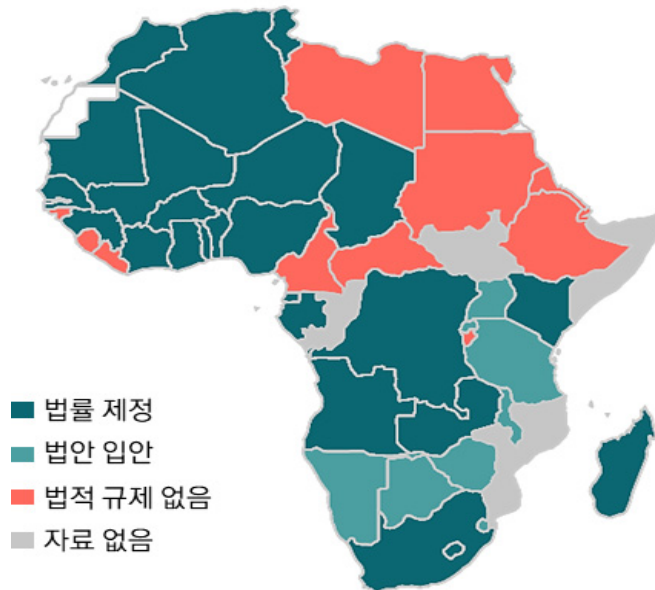
11) *Ibid.*, p. 22.

12) AUC, OECD(2021), *Africa's Development Dynamics: Digital transformation for quality jobs*, Addis Ababa/Paris, p. 60; Oloyede Ridwan(2019. 3. 20), "The African Continental Free Trade Agreement and cross-border data transfer: maximising the trade deal in the age of digital economy," African Academic Network of Internet Policy, <https://aanoip.org/the-africa-continental-free-trade-agreement-and-cross-border-data-transfer-maximising-the-trade-deal-in-the-age-of-digital-economy/>(검색일: 2021. 6. 26).

13) <https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2>(검색일: 2021. 6. 26).

14) AU 사이버보안 및 개인정보보호 협약(AU Convention on Cybersecurity and Personal Data Protection)이 발효되기 위해서는 15개국의 비준이 필요하나 55개국 중 현재까지 14개국만 서명하고 8개국(앙골라, 가나, 기니, 모잠비크, 모리셔스, 나미비아, 르완다, 세네갈)만 비준함. 2018년에 발표된 가이드라인(Personal Data Protection Guidelines for Africa)의 주요 목적은 개인정보 처리에 대한 신뢰를 구축하고 책임 있는 개인정보 처리를 지원하는 것임.

그림 1. 아프리카의 개인정보보호법 규제 추진 현황



자료: UNCTAD, "Data Protection and Privacy Legislation Worldwide," <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>(검색일: 2021. 6. 26).

## 2. 주요 내용

### 가. 개요 및 목적

■ [개요] 총 12장, 115개조로 이루어진 남아공의 개인정보보호법(POPIA)은 2021년 7월 1일부터 전적으로 적용됨.

- POPIA는 2013년 11월에 제정된 이후 2014년 11월부터 단계적으로 적용되어 2020년 7월 1일에 발효되었으나, 1년간의 유예기간이 주어짐.
- 제1조(정의), 5장 39~54조(감독기구의 설립, 권한, 역할, 행정체계, 재정 등), 제112조(일반규칙) 및 제113조(일반규칙 작성 및 개정 절차)는 2014년 4월 11일부터 시행되었으며 제110조(법의 개정) 및 제114(4)조(정보 접근증진법의 기능 이전)를 제외한 나머지 조항은 2020년 7월 1일부로 적용됨.<sup>15)</sup>
- 1년간의 유예기간이 종료되는 2021년 7월 1일부로 제110조 및 제114(4)조 또한 적용됨에 따라 POPIA의 전문이 발효됨.

15) 정보접근증진법(Promotion of Access to Information Act, 2000)은 남아공 국가인권위원회에서 기존에 관할하였으나 POPIA의 도입으로 그 권한이 남아공의 개인정보 감독기관인 'Information Regulator(IR)'로 이전됨.

표 1. POPIA의 구성

구분	내용	세부 내용
제1장	정의 및 목적 (Definitions and Purpose)	용어 정의, 목적
제2장	적용 규정 (Application Provisions)	적용 및 해석, 정보 주체의 권리, 예외 조항
제3장	개인정보의 합법적인 처리를 위한 원칙 (Conditions for lawful processing of personal information)	일반적인 개인정보의 처리를 위한 원칙, 민감정보 처리를 위한 조건, 아동의 개인정보 처리를 위한 조건
제4장	개인정보 처리 조건의 면제 사항 (Exemption from conditions for processing of personal information)	면제 조건, 면제 시 감독기구의 역할
제5장	감독 (Supervision)	감독기관(IR), 정보관리 담당자의 역할 및 권한
제6장	사전 승인 (Prior authorisation)	감독기관(IR)의 사전 승인이 필요한 사항
제7장	행동강령 (Codes of conduct)	행동강령의 발행 조건, 절차, 등록 및 개정
제8장	요청하지 않은 전자통신, 디렉토리 및 자동 의사 결정을 통한 직접 마케팅과 관련된 정보주체자의 권리 (Rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making)	마당의 수단을 통한 직접 마케팅 및 이와 관련된 정보주체자의 권리
제9장	초국경적 정보 이전 (Transborder information flows)	남아공 역외로 이전하는 개인정보에 관한 사항
제10장	시행 (Enforcement)	법 위반 시 정보주체, 정보책임자 및 감독기관의 조치 사항
제11장	범죄 행위, 처벌 및 과징금 (Offences, penalties and administrative fines)	범죄 행위의 내용 및 이에 대한 처벌 사항
제12장	일반규정 (General provisions)	법의 개정, 수수료, 절차 등

자료: 남아프리카공화국 개인정보보호법(POPIA)의 목차를 정리 및 재작성.

■ [목적] POPIA는 헌법에 보장된 개인정보보호 권리 보장과 국제규범에 부합하는 합법적인 개인정보 처리 환경 조성, 그리고 정보주체(data subject)의 개인정보 관련 권리 행사 강화를 목적으로 함.

- POPIA는 헌법 제2조에 명시된 기본권과 제14조에 명시된 사생활 보호권을 보장하기 위해 개인의 정보 접근권을 강조하면서도 정보의 자유로운 이동 또한 보호하고자 함.
- POPIA는 합법적인 개인정보 처리 환경을 수립함과 동시에 이를 이행하기 위한 자발적이고 의무적인 조치를 마련하고자 함.

## 나. 세부 조항

■ [주요 원칙] POPIA는 여덟 가지 원칙을 제시하고 있으며 정보책임자는 반드시 이를 준수하여 개인정보를 수집하고 처리해야 함(제3장).<sup>16)</sup>

- POPIA는 ① 책임성(accountability) ② 처리제한(processing limitation) ③ 목적 구체성(purpose

16) '정보 처리'에 대하여 POPIA는 '정보의 수집, 인수, 기록, 정리, 저장, 수정, 변경, 전달, 파괴 등 개인정보와 관련된 모든 수단의 활동'으로 정의하고 있음(제1조).

specification) ④ 추가적인 정보 처리제한(further processing limitation) ⑤ 정확성(information quality) ⑥ 투명성(openness) ⑦ 안전보장(security safeguards) ⑧ 정보주체 참여(data subject participation)의 원칙을 제시함.

- [책임성의 원칙] 정보책임자(responsible party)는 상기 원칙의 준수 및 입증에 대한 책임을 지며, 정보책임자의 감독 아래 정보를 처리하는 정보처리자(information operator)의 원칙 준수에 대한 책임 또한 정보책임자가 부담함.
  - [처리제한의 원칙] 개인정보의 처리는 정보주체의 동의를 있을 경우 또는 계약이나 법률상의 의무 이행 시, 정보주체의 이익을 보호할 경우에만 가능함. 개인정보 처리의 목적이 분명해야 하고, 개인정보의 처리는 최소한의 범위에서 이루어져야 하며, 개인정보는 정보주체자로부터 직접 받아야 함.
  - [구체성의 원칙] 개인정보 수집 목적이 명확해야 함. 개인정보 저장 기간은 법 집행이나 연구의 목적을 제외하고는 필요 이상의 기간 동안 저장할 수 없으며, 개인정보 파괴 시 복구가 불가하도록 파괴해야 함.
  - [추가적인 정보 처리제한의 원칙] 정보책임자가 정보주체로부터 동의를 받은 최초의 목적을 이루기 위해 추가로 개인정보를 처리해야 할 경우 최초의 목적에 부합해야 함.
  - [정확성의 원칙] 개인정보는 완전하고 정확해야 하며 필요하면 적정한 때에 갱신해야 함.
  - [투명성의 원칙] 정보책임자는 정보 처리과정 전반을 기록해야 하며 개인정보 수집 시 정보주체에게 수집 대상 정보의 내용과 정보주체의 권리에 대해 고지할 의무가 있음.
  - [안전보장의 원칙] 정보책임자는 개인정보의 기밀성을 보장해야 하며, 정보처리자는 개인정보의 보안 유지를 위해 안전수단을 마련하고, 정보책임자의 승인을 얻은 후에만 개인정보를 처리할 수 있음. 개인정보가 노출되었을 경우 즉시 감독기관(IR)과 정보주체에게 고지할 의무가 있음.
  - [정보주체 참여의 원칙] 정보주체는 정보책임자가 수집한 정보에 대한 접근 및 수정 권한이 있음.
- 기본적으로 POPIA의 원칙은 2013년에 개정된 「OECD 프라이버시 가이드라인」에서 제시하고 있는 주요 원칙과 유사함.
- OECD의 8대 원칙은 ① 수집제한(collection limitation) ② 정확성(data quality) ③ 목적 구체성(purpose specification) ④ 이용제한(use limitation) ⑤ 안전보장(security safeguards) ⑥ 투명성(openness) ⑦ 개인 참여(individual participation) ⑧ 책임성(accountability)의 원칙임.

■ [적용 대상 및 범위] POPIA는 살아 있는 자연인 또는 법인을 정보주체(적용 대상)로 정의하고 있으며, 정보책임자가 남아공에 정주하거나 남아공에서 개인정보를 처리하는 경우(적용 범위)에만 법을 적용함.<sup>17)</sup>

- 사망하거나 신원이 불분명한 사람의 정보는 적용대상이 아님(제1조).
- 성별, 인종, 나이 등 정보주체의 인적사항뿐만 아니라 정보주체의 의견 및 성향, 통신 내역, 개인을 식별할 수 있는 기호나 생체정보 등도 개인정보로 간주함(제1조).
- 개인적인 용도를 위한 경우, 위법 행위 또는 국가 안보와 관련된 경우, 언론보도나 문학적, 예술적 활동을 위한 개인정보 처리도 적용 대상에서 제외됨(제6조, 제7조).
- POPIA는 정보책임자가 남아공에 정주하거나 정주하지 않더라도 남아공 내에서 정보를 처리하기 위한 수단을 활용할 경우 적용됨.
- 단 정보가 단순히 남아공을 거쳐서 다른 국가로 전달되는 경우에는 예외로 함.

17) 법률적으로 자연인이라 유기적인 생물학적 육체를 가진 인간으로 생존하는 동안 권리와 의무가 주어지는 주체이며 법인이라 법에 의하여 인격을 부여받아 권리와 의무가 주어지는 주체임.

■ [민감정보] POPIA는 민감정보를 별도로 규정하고 있으며 민감정보를 처리할 때에는 더욱 엄격한 규정이 적용됨(제 26~35조).

- 민감정보에는 종교적·철학적 믿음, 인종, 노조 가입사항, 정치적 성향, 생체 및 생물학 정보, 위법 행위 등이 포함됨.
- 다만 아래와 같이 특수한 경우에는 민감정보 처리를 예외적으로 허용함.
  - △정보주체의 동의를 받은 경우 △관련 정보가 이미 공개된 경우 △연구 목적으로 활용되는 경우 △국제법의 준수, 또는 법 이행을 위한 경우 개인정보처리를 위한 적절한 안전조치가 마련되었고 공공의 이익에 부합한다는 감독기관(IR)의 판단하에 관련 개인정보를 처리할 수 있음.
  - 정보주체가 속한 종교기관이나 노동조합이 회원관리 또는 기관의 목표 달성을 위해 정보주체의 개인정보를 처리할 경우에도 예외적으로 허용됨.
  - 정보주체의 보건생활과 관련된 정보가 의료기관이나 의료인, 의료보험, 아동의 경우 학교 등에 제공될 때는 정보책임자 및 정보주체 간 기밀 유지에 대한 서면합의가 이루어져야 함.
- POPIA는 아동의 개인정보 처리와 관련된 별도의 지침서를 마련하여 아동과 관련된 개인정보를 원칙적으로 금하고 있으나, 공공의 이익에 부합하거나 아동의 개인정보를 보호할 수 있는 적절한 안전수단이 마련되었을 경우에는 사전 승인을 통해 처리할 수 있도록 함.

■ [정보주체의 권리] POPIA는 정보주체의 권리를 강화하기 위한 일환으로 정보주체에게 통지권, 수정권, 삭제권, 반대권 등의 권한을 부여함(제5조).

- [통지받을 권리] 정보주체는 개인정보의 수집 및 활용 시뿐만 아니라 허가되지 않은 방식 또는 주체에 의해 개인정보가 노출되었을 때 통지받을 권리가 있음.
- [개인정보에 접근할 권리] 정보주체는 정보책임자에게 자신의 개인정보 수집 여부 확인을 요청할 수 있으며 정보책임자가 개인정보를 가지고 있으면 자신의 개인정보 내용 및 개인정보를 전달받은 제3자에 대한 정보를 요청할 권한이 있음.
  - 개인정보 수집 여부 확인 요청 시에는 정보책임자가 별도의 비용을 부과할 수 없으나 개인정보 내용을 요청할 시에는 비용을 청구할 수 있으며 이에 대해 사전에 고지해야 함.
- [수정권 및 삭제권] 정보책임자가 수집한 개인정보의 내용이 정확하지 않거나, 관련이 없거나, 필요 이상으로 수집되었을 경우 정보주체는 이에 대한 수정 또는 삭제를 요청할 권한이 있으며, 정보주체의 요청으로 개인정보가 수정 또는 삭제되었을 시 정보책임자는 해당 조치에 대해 정보주체에게 알릴 의무가 있음.
  - 정보책임자가 타당한 사유로 개인정보의 수정 또는 삭제를 거부할 경우 정보주체가 수정을 요청하였으나 거절되었음을 해당 개인정보에 표기해야 함.
- [개인정보 수집 및 처리를 거부할 권리] 정보주체는 개인정보 처리를 거부할 권한이 있으며, 특히 개인정보가 직접 마케팅으로 활용될 경우 거부권을 행사할 수 있음.<sup>18)</sup>
- [자동 의사결정의 대상이 되지 않을 권리] 자동 의사결정이란 수집한 인적정보를 기반으로 개인의 업무역

18) 직접 마케팅이란 잠재적 고객에게 직접적으로 판촉활동을 하는 것을 의미함(예: 광고 문자 메시지).



량이나 신용성, 건강 상태, 취향에 대한 자동적인 처리가 이루어지는 것으로 정보주체는 본인이 제공한 개인정보가 자동 의사결정의 대상이 되지 않을 권리가 있음.

- [항의 및 민사소송 권리] 개인정보를 보호받지 못할 경우 정보주체는 감독기관(IR)에 항의하고 민사소송을 제기할 권리가 있음.

■ [정보책임자의 책임] POPIA는 개인정보의 수집과 처리에 관한 최종적인 책임을 정보책임자에게 부여하고 있음(제11조).

- 개인정보의 선별, 처리 기간, 처리 방법 등에 대한 결정권은 정보책임자에게 있음. 정보처리자는 정보책임자와 계약을 통해 단순히 정보를 처리하는 업무로 제한되어 있어 모든 의사결정권은 정보책임자에게 있음.
  - 정보처리자가 POPIA를 위반하였다 하더라도 감독기관(IR)은 정보책임자에게 책임을 물을 수 있음.
  - 추후 문제 발생 시 정보주체의 개인정보 수집 및 처리 동의여부에 대한 입증 책임도 정보책임자에게 있음.
- 정보책임자는 반드시 서면 계약을 통해 정보처리자의 POPIA 준수를 위한 안전장치를 마련해야 함.

■ [정보관리자(Information Officer) 지정] 공공 및 민간주체 모두 개인정보 관리를 총괄하는 정보관리관을 지정해야 함(제55조).

- 정보관리자는 반드시 감독기관(IR)에 등록되어야 하는데 공공기관의 경우에는 정보담당자가 자동적으로 정보관리자가 되며, 법인과 개인 사업체를 포함한 민간주체의 경우에는 해당 주체의 대표가 정보담당자가 됨.
- 정보관리자는 사업장 내 개인정보보호법의 원칙 준수 독려, 감독기관(IR)과 협업, 정보주체의 요청에 따른 관련 자료 마련 등의 업무를 담당함.

■ [역외 이전] POPIA는 개인정보의 역외 이전을 원칙적으로 금하고 있으나 특정 조건이 충족될 때에는 가능하도록 함(제9장).

- 개인정보의 역외 이전은 ① 개인정보를 전달받는 제3자가 개인정보의 역외 이전과 관련, POPIA와 유사한 수준의 개인정보보호법 또는 법적 효력이 있는 내규가 지배하고 있거나 ② 정보주체가 동의한 경우 ③ 정보주체와 정보책임자 간의 계약 이행을 위한 경우 ④ 개인정보의 이전이 정보주체에게 유익할 경우에만 가능함.

■ [개인정보 침해 발생 시 조치사항] 개인정보가 유출되었을 경우 정보처리자는 정보책임자에게, 정보책임자는 감독기관(IR) 및 정보주체에게 반드시 통지해야 함(제21조, 제22조).

- 정보책임자는 개인정보 유출을 인지한 즉시 감독기관(IR) 및 정보주체에게 통지하도록 규정하고 있으나 구체적인 기한은 명시되어 있지 않음.
  - 정보주체에게는 반드시 서면으로 통지해야 하며 예상되는 유출의 영향, 유출에 대한 정보책임자의 대응방안, 개인정보를 습득한 기관 등 정보주체가 유출에 충분히 대응할 수 있는 정보를 제공해야 함.

- 정보책임자가 정보유출에 대한 통지를 미룰 수 있는 유일한 경우는 정보책임자가 정보주체에게 통지함으로써 진행되고 있는 범죄 수사가 방해될 가능성이 있다는 감독기관(IR)의 판단이 있을 때임.

■ [처벌조항] 개인정보보호에 대한 법적 의무 불이행 시 과징금 부과뿐만 아니라 징역도 가능함(제11장).

- 위반사항별로 처벌 수준이 상이함.
  - △감독기관(IR)의 업무 방해 △위반통지 불응 △위증 △금융계좌 개설 및 처리 시 8대 원칙 미준수 △정보책임자의 승인 없는 금융계좌 정보 처리, 금융계좌 정보 판매 또는 판매 제안 시에는 약 70만 달러(1,000만 랜드)의 과징금 또는 최대 10년의 징역형, 또는 과징금과 징역형이 동시에 부과될 수 있음.
  - △감독기관(IR)의 사전 승인이 요구되는 개인정보를 사전 승인 없이 처리 △기밀유지 의무 위반 △영장 집행 방해 △감독기관(IR)의 정보요청서에 허위로 응답 △재판 참석 및 참여 요구에 불응 시에는 약 70만 달러(1,000만 랜드)의 과징금 또는 최대 12개월의 징역형, 또는 과징금과 징역형이 동시에 부과될 수 있음.<sup>19)</sup>

## 다. 감독기관의 설립 및 권한

■ POPIA는 개인정보보호를 위한 독립적인 감독기관(Information Regulator)을 신설하도록 명시하고 있는바, 감독기관은 관리, 감독, 집행 및 처벌 등의 포괄적인 기능 및 권한을 갖고 있음.

- 감독기관(IR)은 헌법 및 기타 법률에만 예속되어 있으며 업무 수행을 위한 목적으로 수행한 활동에 대해 형사 또는 민사 책임을 지지 않음.
- 감독기관(IR)은 POPIA의 이행 및 적용을 위해 △교육자료 및 정보 제공 △새로운 기술의 발달과 그 영향에 관한 연구 진행 △관찰 및 평가를 통한 이행 여부 감독 △위반사항 조사 및 갈등 중재 △행동강령 발행 및 개선 등의 기능을 가짐.
- 감독기관(IR)은 POPIA의 8대 원칙에 어긋나더라도 개인정보 처리를 승인할 수 있는 권한이 있는데 이는 개인정보를 보호하는 것보다 공공의 이익, 또는 정보주체자의 이익이 더 크다고 판단될 때에 한해 가능함.
- 감독기관(IR)은 기관의 활동과 관련된 보고서를 발행하여 감독기관이 추구하는 개인정보보호의 정책 방향성에 대한 정보를 제공할 수 있음.
  - 감독기관(IR)이 2016년 12월에 업무를 개시한 이후 정기적으로 감독기관의 활동 내용 및 계획에 대해 적극 게시하고 있음.
  - 행동강령 작성 요령, 정보관리자 등록 양식, 사전 승인 신청 안내문 등의 행정자료와 중기 전략, 성과지표를 포함한 연간계획, 활동보고서 등을 게시함.<sup>20)</sup>

■ 감독기관(IR)은 또한 특정 산업 또는 전문 분야에 대한 행동강령 공표를 승인할 수 있음.

19) 정보책임자는 ① 고유 식별자 처리 ② 위법 또는 범죄 행위 관련 정보 처리 ③ 신용 평가 ④ 개인정보의 역외 이전 시 감독기관의 사전승인을 받아야 함. 단, 특수 산업에 대한 행동 강령이 별도로 명시할 경우에는 사전승인이 요구되지 않음(제57조).

20) 관련 자료는 IR 홈페이지(<https://www.justice.gov.za/inforeg/index.html>)에 게시되어 있음.

- 의료, 연구, 금융 등 특수 산업 또는 분야의 경우 분야의 특수성을 적용할 수 있는 일련의 규정들을 행동 강령으로 제시할 수 있으며 이 또한 8대 원칙을 준수해야 함.
- 행동강령은 분야 대표자/대표기관이 공표 요청을 접수하거나 감독기관이 자체적으로 해당 분야의 전문가 및 이해관계자들과 상의 후 공표할 수 있음.
  - 감독기관(IR)은 이해관계자들의 의견을 충분히 수렴하기 위해 행동강령 공표 전 행동강령 공표를 위한 검토가 이루어지고 있음을 관보에 게시해야 하며, 공표 이후에도 해당 내용을 관보에 게시해야 함.
  - 최종 강령 공표 여부에 관한 결정은 공표 요청 후 13주 이내에 이루어져야 함.

■ 감독기관(IR)은 1명의 기관장과 4명의 위원으로 구성되며, 기능 수행을 위한 집행부와 개인정보보호 위반사항에 대한 처벌 및 조율 권한을 가진 집행위원회를 반드시 구성해야 함.

- 기관장과 위원들은 의회의 승인을 받은 후 대통령이 직접 임명할 수 있음.
  - 위원의 경우 2명은 상근직, 2명은 비상근직이며, 이해상충 방지를 위해 공무원 또는 선출직, 정당 소속 직원 일 경우 임명을 제외함.
  - 위원직의 상실은 위원이 자발적으로 사직하거나 의회에서 과반수를 얻을 경우에만 박탈할 수 있도록 하여 기관의 독립성을 확보하고자 함.
  - 위원의 임기는 5년이지만 무기한 연장 가능함.
- 감독기관(IR)은 최고경영자(Chief Executive Officer)를 임명하여 기관장의 업무를 보조하는 집행부를 구성하고 운영할 수 있음.
- 또한 집행위원회(Enforcement Committee)를 반드시 구성하여야 하는데 이는 조사 및 처벌 기능을 구분하기 위함.
  - 개인정보보호 위반 시 조사는 감독기관(IR)이 수행하고, 조사 내용을 바탕으로 집행위원회에서 관련 처벌에 관한 결정을 내리도록 함.

### 3. GDPR과의 비교

■ POPIA는 EU의 개인정보보호 지침(Directive)과 GDPR의 내용을 반영하여 작성되었기 때문에 개인정보에 대한 정의 및 원칙 등에 대한 내용이 대체로 유사하나 적용 범위, 처벌 수준, 정보책임자의 책임 범위 등 세부적인 차이점이 존재함.

- POPIA가 2013년에 제정되었음에도 불구하고 2020년에 발효된 것은 2018년에 발효된 GDPR의 내용을 참고하여 필요할 경우 법을 개정하기 위한 것임.
- POPIA가 GDPR을 참고하여 작성된 이유는 유럽이 남아공의 주요 교역국인 동시에 GDPR이 역외에서의 개인정보처리에 대해서도 적용되어 남아공 기업들이 유의할 필요가 있기 때문임.
  - 남아공은 사하라이남 아프리카에서 EU의 최대 교역국으로 2019년 기준 남아공-EU의 상품 무역규모는 419억 유로(약 496억 달러)였으며 서비스 무역규모는 114억 유로(135억 달러)에 달함.<sup>21)</sup>

- POPIA는 남아공 영토 내에서 처리되는 정보에 한해 적용되나 GDPR은 EU 외 지역에서 EU 회원국 국민의 개인정보를 처리할 때에도 적용됨.
- 뿐만 아니라 GDPR은 현재까지 개인정보보호와 관련하여 가장 포괄적이고 지역적으로 넓게 적용되는 법으로 글로벌 표준으로 정립되고 있어 많은 국가들이 개인정보보호법을 작성할 때 GDPR을 참고하고 있음.
- POPIA와 GDPR 모두 개인정보보호법의 기초가 되는 「OECD 프라이버시 가이드라인」을 기반으로 작성되어 용어 정의, 주요 원칙, 감독기관의 권한 등이 유사함.
- POPIA와 GDPR은 정보주체, 정보책임자, 정보처리자, 정보관리자의 역할을 구분하여 명시함.<sup>22)</sup>
- POPIA의 원칙과 마찬가지로 GDPR의 원칙도 개인정보 처리의 적법성과 투명성, 수집 목적의 구체성, 개인정보의 정확성, 기밀성 등을 강조하고 있음.<sup>23)</sup>
- POPIA는 감독기관을 ‘Information Regulator,’ GDPR은 ‘supervisory authority’로 명시하고 조사권과 중재권, 시정명령권 등 폭넓은 감독권한을 부여함.
- 그럼에도 불구하고 POPIA는 역외에서 처리되는 정보에 대한 법률 적용 여부, 처벌 수준, 익명화 조치 등에서 GDPR과 다르게 접근하고 있는데 주요 차이점은 아래에서 서술함.

■ 근본적으로 GDPR은 POPIA와 달리 국가가 아닌 지역공동체(EU)가 발효한 법률로서 회원국의 자유재량이 존중됨.

- GDPR은 99개 조문 중 약 69개 조문이 EU 회원국에 일종의 자유재량을 위임하는 형식의 오프닝 조항으로 규정되어 있는바, 향후 각국의 개인정보보호법 입법과정에 대한 모니터링이 필요함.<sup>24)</sup>
- 예를 들어 GDPR은 국별 감독기관의 설립 권한 및 회원자격 설정 등을 회원국에 일임하고 있으며 사망한 개체에 대한 정보처리나 부모 또는 보호자의 동의가 요구되는 아동의 나이를 개별 국가 차원에서 규제할 수 있도록 함.

■ [적용 대상 및 범위] 정보주체에 대한 정의는 POPIA가 더 포괄적이나 개인정보 처리의 적용 범위는 GDPR이 보다 넓게 적용됨.

- POPIA와 GDPR 모두 개인정보의 주체를 살아 있고 식별 가능한 사람을 대상으로 규정하고 있으나 POPIA는 법인도 개인정보의 주체로 포함하여 법인의 개인정보 또한 보호받을 권리가 있음.
- POPIA와 GDPR 공통으로 △영토 내에 사업장이 있을 경우, 또는 △ 사업장이 없을 시 영토 내에서 개인정보를 처리할 경우 규정을 준수하도록 하였으나, GDPR은 △EU에 있는 정보주체를 대상으로 재화 및 서비스를 제공하는 경우와 △EU 내에 있는 정보주체의 활동을 모니터링하는 경우에도 법률을 준수하도록 함.
- 위의 경우 정보관리자는 정보주체가 거주하는 회원국 중 하나에 대리인을 지정하여야 하는데 이는 대리인이 사업장으로 간주되기 때문임.

21) European Commission(2021. 4. 26), “Countries and regions: South Africa,” <https://ec.europa.eu/trade/policy/countries-and-regions/countries/south-africa/>(검색일: 2021. 6. 26).

22) GDPR은 정보책임자와 처리자, 정보관리자를 컨트롤러(controller) 및 프로세서(processor), 개인정보보호책임관(data protection officer)로 표현함.

23) GDPR의 원칙은 ① 개인정보 처리의 적법성·공정성·투명성 ② 수집 목적 제한 ③ 개인정보처리 최소화 ④ 정확성 ⑤ 보관 기간 제한 ⑥ 무결성·기밀성임(GDPR 제2장 5~11조).

24) 오태현, 강민지(2018. 5. 25), 「EU 개인정보보호법(GDPR) 발효: 평가 및 대응방안」, 오늘의 세계경제, KIEP.

- [개인정보 비식별 조치] POPIA는 개인정보를 삭제함으로써 개인정보를 식별 불가능하게 하고 있지만 GDPR은 익명화도 허용하고 있음.
  - 개인정보의 저장에 더 이상 필요하지 않을 때 POPIA는 정보주체를 식별할 수 있는 정보, 또는 추가적인 정보와 수단을 통해 정보를 재구축할 수 있을 만한 정보를 삭제하도록 되어 있음.
  - 반면 GDPR은 개인정보를 보호할 수 있는 수단과 조치가 마련될 경우 개인정보의 익명화도 허용하고 있음.<sup>25)</sup>
  
- [아동의 개인정보 처리] POPIA와 GDPR 모두 아동의 개인정보 처리를 특별사항으로 관리하고 있으나, 아동의 연령과 아동의 개인정보 처리를 위한 조건이 다름.
  - POPIA는 아동을 18세 이하의 자연인으로 제한하는 반면 GDPR은 아동의 연령을 16세로 규정함. 단, 개별 국가에서 아동에 대한 연령을 13세까지 자율적으로 적용할 수 있도록 함.
  - 아동의 개인정보 처리를 위해서는 ‘법적 대변인’의 동의가 필요하며 GDPR은 이를 부모 또는 보호자로 정의하나 POPIA의 경우 ‘법적 대변인’은 단순히 법적 자격이 되는 자로만 표기함.
  - 아동과 관련된 개인정보를 처리할 때 GDPR은 정보관리자가 해당 아동의 개인정보 처리와 관련된 정보를 아동이 이해할 수 있는 언어로 쉽게 작성하여 아동에게 직접 제공하는 의무를 부과하고 있으나 POPIA는 해당 사항이 없음.
    - POPIA는 ‘법적 대변인’이 요청할 경우 정보관리자에게 해당 정보를 제공할 의무를 부과하나, 정보를 받는 대상은 구체적으로 명시하지 않음.<sup>26)</sup>
  
- [개인정보 처리 기록 의무] 개인정보의 처리와 관련된 일련의 활동에 대한 기록 의무는 GDPR이 보다 구체적으로 요구하고 있음.
  - 개인정보 처리 시 POPIA와 GDPR 모두 관련 활동을 기록하도록 규정하고 있으나 GDPR은 필히 기록해야 하는 명단을 제시한 반면 POPIA는 ‘서류 보관’ 수준에 그침.
    - GDPR의 정보관리자는 정보관리자의 이름 및 연락처, 개인정보의 처리 목적, 개인정보의 종류, 개인정보 공개 대상, 정보 삭제 시까지의 예상 기간, 개인정보보호를 위한 안전 수단에 대한 기록을 남겨야 함.
    - 정보처리자는 정보처리자의 이름 및 연락처, 정보관리자를 대변하여 처리하는 활동의 종류, 역외 이전 정보 수취인에 대한 식별정보 및 준비된 안전조치에 대한 서류를 기록하여야 함.
    - 처리에 대한 기록사항은 서면 또는 전자형태로 이루어져야 하며 감독기관에서 요청 시 관련 기록사항을 제출해야 함.

25) 익명화란 “추가 정보를 사용하지 않고는 개인 데이터가 특정 데이터 주체에 더 이상 귀속될 수 없도록 하는 방식으로 개인 데이터를 처리하는 것”이며 “이러한 추가 정보는 별도로 보관되며 기술적 및 조직적 수단으로 개인 데이터는 식별되거나 식별 가능한 자연인의 속성이 되지 않도록 해야 함(GDPR 제4조 5항).

26) Information Regulator(2021. 6. 28), “Guidance note on processing of personal information of children,” South Africa, p. 7.

- [개인정보 유출 발생 시 처리사항] POPIA와 GDPR 모두 개인정보가 유출되었을 시 통지 의무와 조치 사항을 명시하고 있으나 GDPR은 구체적인 통지 기한을 둠.
  - 정보처리자 및 책임자는 개인정보 유출을 방지하기 위해 정기적으로 안전조치를 점검하고 갱신해야 하며 개인정보 유출을 인지한 즉시 감독기관 및 정보주체에게 유출된 정보의 범위, 유출로 인한 영향 등을 통지해야 함.
  - GDPR은 정보 유출 인지 시점부터 72시간 이내에 감독기관에 보고하도록 하였으나 POPIA는 ‘합리적으로 가장 이른 시일’이라고 명시할 뿐 구체적인 기한은 없음.
  
- [개인정보보호 영향평가] GDPR은 ‘protection by design’ 원칙을 적용하여 새로운 기술 활용과 같이 개인정보 침해 위험이 클 경우 개인정보보호 영향평가를 반드시 실시하도록 규정함.
  - POPIA는 개인정보보호 영향평가를 정보관리자의 책임 중 하나로 명시하고 있으나 의무사항으로는 규정하지 않으며, 단순히 개인정보의 합법적 처리를 위한 환경 조성의 수단 중 하나로 봄.
  
- [개인정보 이동권] GDPR은 개인정보 이동권을 보장하기 위해 정보주체가 개인정보를 여러 서비스에 걸쳐 사용할 수 있도록 하고 있으나 POPIA의 정보주체는 이러한 권리가 없음.
  - GDPR에서는 정보주체가 자신의 개인정보를 다른 정보책임자 또는 처리자에게 전송 요청할 경우 정보처리자는 이에 응해야 함.
  - 이는 정보의 상호유용성을 강화하기 위한 조치로 정보주체의 개인정보에 대한 통제권 강화뿐만 아니라 기업의 정보 독점을 완화하여 공정한 경쟁 환경을 조성함.
  
- [처벌조항] GDPR의 과징금 규모가 훨씬 크나 POPIA는 법률 위반을 범법행위로 간주하여 구속도 가능함.
  - GDPR과 POPIA에서 처벌 여부 및 처벌 수준은 개인정보의 성격, 위반의 중대성, 손해의 정도 등을 고려하여 감독기관에서 결정함.
  - 다만 GDPR의 과징금은 위반 사항에 따라 ① 최대 전 세계 연간 매출액의 2% 또는 1,000만 유로 중 더 큰 금액 ② 최대 전 세계 연간 매출액의 4% 또는 2,000만 유로까지 중 더 큰 금액을 부과함.
  - POPIA의 과징금은 최대 1,000만 랜드(49만 유로)까지 가능하나 위반성격에 따라 12개월 이내 또는 최대 10년 이내의 징역형에 처할 수도 있음.

## 4. 평가 및 시사점

- POPIA와 GDPR의 내용이 대체로 유사하기 때문에 이미 GDPR을 준수하고 있는 기업 및 개인은 POPIA에 쉽게 적응할 수 있을 것으로 예상되나 세부적인 차이점을 유의할 필요가 있음.

- 2018년도에 IT 보안업체인 소포스(Sophos)가 남아공에서 진행한 설문에 의하면 응답자의 약 80%가 이미 POPIA 규정을 준수하고 있거나 발효 시점에 준비가 되어 있을 것이라고 답변하였는데 이는 상당수의 남아공 정보책임자 및 기업들이 GDPR을 준수하고 있기 때문으로 보임.<sup>27)</sup>
- 2021년 7월 1일부로 POPIA의 전 조항이 효력을 발휘하였기 때문에 아직 개인정보보호 위반사항에 대한 해석과 감독기관(IR)의 판단이 명확하지 않은 만큼 GDPR의 해석 및 적용 사례가 유용한 참고자료가 될 것으로 보임.

■ 특히 코로나19의 확산으로 개인정보 수집 및 처리의 필요성이 커진 만큼 개인의 정보보호권과 공공의 이익 간 균형을 잡는 데 감독기관(IR)의 역할이 중요할 것으로 보임.

- 체온 측정, 전화번호 수집, 여행 이력 수집, 감염자 관리 등 코로나19 예방 및 치료 차원에서 다중적인 정보 수집이 이루어지고 있어 개인정보 관리의 중요성이 확대됨.
- 이와 관련하여 감독기관(IR)은 2020년 4월에 코로나19 관리 및 예방을 위한 개인정보 수집에 관련된 가이드라인을 발표함.<sup>28)</sup>
  - 가이드라인은 POPIA가 전격 발효되기 이전에 작성된 것으로 감독기관은 능동적인 준수를 격려했.
- 감독기관(IR)은 POPIA 제15조 3항에 명시된 바에 따라 가이드라인을 통해 코로나19에 대응하기 위한 개인정보 처리를 지지함.
  - 감독기관(IR)은 공공의 보건질서 유지가 헌법에 보장된 개인의 권리로 인해 제한되어서는 안 된다고 판단, 정보주체의 코로나19 검사 거부권을 제한하고 코로나19의 확산 방지를 위한 위키기반 정보 수집 및 대규모 감시를 허용함.
- 코로나19 상황과 같이 정보주체의 동의 없이 처리할 수 있는 예외조항이 POPIA에 다수 명시된 만큼 향후에도 개인의 정보보호권과 공공의 이익 또는 정보관리자의 정보 접근권 간의 균형을 유지하는 데 감독기관의 전문성과 객관성, 독립성 확보가 반드시 필요할 것으로 보임.

■ 과거 남아공에서 다수의 개인정보 유출 사건이 발생하였기에 POPIA 시행으로 남아공 국민들의 개인정보보호 시스템에 대한 신뢰가 회복되고 인식 개선에 긍정적인 영향을 미칠 것으로 보임.

- 최근 5년 사이 다수의 대규모 개인정보 유출 사건이 발생하였는데 유출 규모가 가장 큰 'Master Deeds' 사건의 경우 사망자에 대한 정보를 포함해, 약 6,000만 명의 주민번호, 고용 정보, 부동산 소유 정보 등 개인정보가 공개된 웹 서버에 저장됨.<sup>29)</sup>

27) Sophos(2018), *POPI Survey Report-2018*, p. 6, <https://www.sophos.com/en-us/medialibrary/pdfs/marketing-material/protection-of-personal-information-survey-report-2018.pdf>.

28) Information Regulator(2020. 4. 3), "Guidance note on the processing of personal information in the management and containment of COVID-19 pandemic in terms of the Protection of Personal Information Act 4 of 2013(POPIA)," <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf>(검색일: 2021. 6. 26).

29) 2017~18년에만 5건의 대규모 개인정보 유출 사건이 발생함: ① Master Deed 사건 ② Ster-Kinekor 사건(현지 엔터테인먼트 기업인 Ster-Kinekor에서 7백만 명의 개인정보 노출) ③ 페이스북 사건(전 세계적으로 5천만 명의 회원 정보가 해킹) ④ ViewFines 사건(온라인 교통범죄금 지불 사이트에서 94만 3천 명의 개인정보가 유출) ⑤ Liberty사 사건(랜섬웨어 공격으로 320만 명의 고객정보가 해커의 협상 도구로 사용). Tehillah Niselow(2018. 6. 19), "Five massive data breaches affecting South Africans," *fin24*, <https://www.news24.com/fin24/Companies/IC/T/five-massive-data-breaches-affecting-south-africans-20180619-2>(검색일: 2021. 6. 26).

- 남아공 인구가 약 5,800만 명인 것을 고려하면 대다수 국민의 개인정보가 노출되었다고 볼 수 있어 남아공에서 큰 논란이 되었으나 최초 유출자는 찾지 못했음.
- 2019년도에 남아프리카공화국대학(University of South Africa)에서 진행한 설문에 의하면 응답자의 94%는 개인 신원의 안전에 대한 우려를 하고 있었으며, 개인정보가 유출되었을 시 위반사항 신고 방법에 대한 지식을 가지고 있는 응답자의 비율은 37%에 불과함.<sup>30)</sup>
- 감독기관(IR)이 설립된 이후 POPIA의 효율적인 이행을 위한 가이드라인 및 행동강령이 지속해서 공표되었고 개인정보보호법 준수의 중요성에 대한 인식개선 활동이 적극적으로 이루어지고 있어 개인정보보호에 대한 신뢰가 높아질 것으로 보임.

■ 아프리카대륙자유무역지대(AfCFTA: African Continental Free Trade Agreement)의 효과적 이행을 위해서 공동의 디지털 정책 및 규범이 필수적인 만큼 남아공의 개인정보보호법(POPIA)은 아프리카의 교역 환경 개선에 기여할 수 있을 것으로 보임.

- AfCFTA가 효과적으로 이행될 경우 아프리카의 역내 무역은 2040년까지 15~20% 상승하고 아프리카의 소득은 2035년까지 4,500억 달러 증가할 것으로 분석되었는데, 국경간 무역, 특히 전자상거래에서 요구되는 개인정보보호에 관한 통일된 규제의 부재는 AfCFTA의 효과적 이행을 저해하는 제약요소로 지목됨.<sup>31)</sup>
- AfCFTA는 서비스교역의정서 제15조에서 개인정보처리 시 개인정보를 보호하기 위한 법적 의무 준수를 강조하였으나 이는 국별로 개인정보보호법 도입을 격려하는 수준에 그침.
- 아프리카에서 남아공의 정치·경제적 영향력을 고려할 때 남아공이 개인정보보호법을 도입하면 이에 저촉하지 않기 위해 주요 교역대상국도 유사한 수준의 법률을 제정할 것으로 기대됨.
- 남아공은 사하라이남 아프리카에서 나이지리아 다음으로 경제규모가 큰 국가이며, 특히 남부아프리카 국가들의 남아공 경제에 대한 의존도가 높아 우선 남부아프리카 국가들을 중심으로 개인정보 관련 규제 수립이 이루어질 수 있을 것으로 보임.<sup>32)</sup> KIEP

30) *Ibid.*

31) UNECA(2015), *Industrializing through trade*, Addis Ababa, p. 161; World Bank Group(2020), *The African Continental Free Trade Area: Economic and Distributional Effects*, Washington D.C., p. 3; Sogbetun and Moshood, *The impact of data protection rules on the digital economy aspect of the African Continental Free Trade Agreement(AfCFTA)*, Africa Law Practice NG&Co, p. 3; Brian Daigle(2021. 2), "Data Protection Laws in Africa: A Pan-African Survey and Noted Trends," USITC Journal of International Commerce and Economics, p. 2.

32) 남아공은 남아프리카개발공동체(SADC: Southern African Development Community)의 총 GDP에서 52%를 차지하며 남아프리카관세동맹(SACU: Southern African Customs Union) 총 관세수입의 98%를 차지함. OECD(2017. 7), *OECD Economic Surveys South Africa*, OECD Publishing, Paris, p. 33; Statistics South Africa(2020. 6. 25), "A 110-year-old trade venture," <http://www.statssa.gov.za/?p=13385> (검색일: 2021. 6. 26).