논문 18-43-02-29 The Journal of Korean Institute of Communications and Information Sciences '18-02 Vol.43 No.02
https://doi.org/10.7840/kics.2018.43.2.427

General Data Protection Regulation(GDPR) 시행에 따른 정보보호담당관(DPO)의 국내 정착 방안에 대한 연구

박 민 정◆, 채 상 미°, 이 명 준*

A Study on the Establishment of Data Protection Officer(DPO) Position under GDPR Enactment

Minjung Park◆, Sangmi Chai°, Myoungjun Lee*

요 약

2018년 5월, GDPR이 시행됨에 따라 유럽연합을 비롯하여 이를 대상으로 비즈니스를 하는 모든 국가의 기업들에 GDPR이 적용된다. 따라서 국내 대다수의 기업들도 GDPR이 적용되어 국내에서도 GDPR은 중요한 비중을 차지하게 되었다. GDPR은 개인정보 처리와 관련된 다양한 사항의 준수를 요구하는 동시에 GDPR 준수 여부를 모니터링 하고, 개인정보 처리를 관리하는 정보보호담당관(DPO)의 의무 임명을 함께 규정하였다. 하지만 국내 기업 환경에서 DPO는 생소한 개념으로 현재, 국내 대부분의 기업이 DPO 임명의 어려움을 겪고 있다. 이에 본 연구에서는 GDPR 및 유럽정보보호위원회에서 제시한 DPO 가이드라인을 바탕으로 DPO의 지정 요건, 자격, 역할 및 책임 등에 대한 분석을 수행하여 국내 기업의 DPO 관련 이해를 도모하고자 한다. 또한 현재, 국내 개인정보보호법 등이 규정하는 CIO, CPO, CSO, CISO와 DPO의 비교를 수행하며 DPO 임명을 완료한 해외 글로벌 기업의 사례를 분석한다. 마지막으로 국내 DPO의 성공적인 도입과 정착을 위한 방안으로 1) 국내 제도적 장치 마련, 2) 한국형 DPO 모델 개발, 3) DPO 도입의 단계적 프레임워크를 제시하였다. 이를 통하여 본 연구의 결과는 향후, 국내 DPO 관련 가이드라인 개발의 토대가 되는 동시에 국내 기업의 DPO 선임을 통한 정보보안 수준 향상을 기대할 수 있다.

Key Words : DPO(Data Protection Officer), GDPR(General Data Protection Regulation), Information security, Personal data

ABSTRACT

The General Data Protection Regulation(GDPR) will be enactive in the European Union(EU) in May 2018, GDPR applies to all organizations across EU and beyond. The importance of GDPR has increased due to the almost domestic companies have duties to comply with GDPR, in Korea. GDPR requires to appoint a Data Protection Officer(DPO) who takes a responsibility for managing the processing of personal data and monitoring organizations' compliance with GDPR, however most organizations have experienced difficulties in designating DPO.

DPO is not provided definitely by GDPR and is an unfamiliar concept, in Korea. To improve domestic

◆ First Author : (ORCID:0000-0003-1268-2056)Ewha Womans University, Department of Business, mjpark67@ewhain.net, 학생회원
° Corresponding Author : (ORCID:0000-0003-4889-7737)Ewha Womans University, Department of Business, smchai@ewha.ac.kr, 정회원
* (ORCID:0000-0002-6780-3559)하모니 법률사무소 대표변호사, badook98@naver.com
논문번호 : KICS2017-11-362, Received November 28, 2017; Revised January 11, 2018; Accepted January 11, 2018

organizations' understandings of DPO, we review carefully GDPR's Articles and Guidelines on DPO presented by European Data Protection Board. Finally, providing a plan for the successful adoption and establishment of DPO, in Korea as followings; 1) institutionalize DPO system, 2) develop a Korean DPO Model, and 3) provide a DPO framework. The results of this study will be the basis for the development of DPO guidance, in the future and it can be expected the improvement of each organization's information security through the appointment of DPO.

Ⅰ. 서 론

2018년 5월 25일, 유럽연합 회원국 전체에 구속력을 갖는 법규로서 GDPR(General Data Protection Regulation, 유럽연합 개인정보보호 일반법)이 시행 예정이다. GDPR은 유럽연합 회원국과 더불어 역외 적용이 인정됨에 따라 유럽연합 정보주체에게 서비스를 제공하거나 유럽 내 거주하는 정보주체에 대한 모니터링을 실시하는 국내 기업까지 GDPR의 적용 대상이 된다. 특히, GDPR은 일정한 요건에 해당하는 개인정보처리자 등에게 정보보호담당관(Data Protection Officer, 이하 "DPO")을 의무적으로 지정하도록 하였다. 기업의 GDPR 위반은 최대 약 270억원 혹은 글로벌 매출액의 4%중 높은 금액의 벌금이 적용되어 기업의 심각한 경제적 손실의 초래할 수 있음에 따라 GDPR에 대한 전 세계적인 관심과 중요성이 오늘날 증가하고 있다.

GDPR의 도입에 따라 전 세계적으로 약 7만 5천명, 국내는 약 1천 4백명의 DPO가 필요할 것으로 발표되었다[1]. 그런데 일정한 요건에 따른 DPO 임명이 의무규정 임에도 불구하고 GDPR은 DPO의 자격 요건 등을 구체적으로 명시하지 않는다. 이는 DPO의 지정이 유럽연합 회원국을 비롯한 다수의 글로벌 기업에 적용되기 때문에 각 국가, 기업의 특성을 고려하여 DPO를 선임할 것을 권장하는 것이다. 이와 같이 DPO의 자격 및 역할에 대한 상세 조건이 GDPR에 제시되지 않음에 따라 기업은 어떠한 역량을 보유한 DPO를, 어떻게 선임하여, 어떠한 업무 및 책임 의무를 부여할 것인지에 대한 문제에 오늘날 직면하였다. 이에 본 연구에서는 국내 기업 환경에서 생소한 DPO의 개념을 GDPR 규정 및 유럽정보보호위원회(European Data Protection Board)에서 발간한 DPO 가이드라인의 분석을 통하여 DPO의 지정 요건, 자격, 역할 및 책임에 대하여 제시한다. 추가적으로 DPO와 국내 정보보안 관련 책임자의 비교를 통하여 국내 DPO 임명의 필요성을 밝히고, 해외 글로벌 기업의 실제 DPO 임명 사례를 분석함에 따라 현재 국내 기업이 당면한 문제 해결의 토대를 제공한다.

국내 기업의 DPO 지정은 GDPR의 준수라는 목적 이외에 기업의 정보보안 수준을 향상시킬 것으로 예상된다. 최근, 국내 일부 금융회사의 최고정보보호책임자(Chief Information Security Officer, 이하 "CISO") 임명이 의무화됨에 따라 이와 관련된 연구가 활발히 진행되었다[2]. 연구 결과, CISO의 임명 및 역할 인식이 조직의 정보보호 성과를 실제로 향상시키는 바와 같이[3], 국내 기업의 DPO 선임 역시 조직의 정보보안 환경에 긍정적인 영향을 줄 것으로 판단된다.

본 연구에서는 국내 환경에서의 DPO 정착을 위한 방안으로 1) 관련 법적 제도 마련, 2) 한국형 DPO 모델 개발, 3) DPO 도입의 단계적 프레임워크를 제시한다. 이는 국내 기업 환경에 적합한 DPO 모델 개발 및 DPO 정착 방안을 제안함에 따라 향후, 기업의 자발적인 DPO 임명을 유도하는 토대가 된다. 또한 국내 기업 환경에서 DPO의 중요성을 인식시킴에 따라, DPO를 통한 기업의 능동적인 정보보호 문화를 형성하고 실제 정보보안 수준의 향상을 기대할 수 있다.

Ⅱ. 정보보호담당관 DPO(Data Protection Officers)

2.1 DPO 지정 요건

GDPR은 다음의 세 가지 항목 중 하나의 경우에 포함되는 경우, DPO의 필수적인 지정을 규정하고 있다. 1) 법원이 사법능력을 행사하는 경우를 제외하고 공공기관이나 공공기구에 의해 개인정보 처리가 수행되는 경우, 2) 컨트롤러 또는 프로세서의 '핵심 활동(core activities)'이 처리의 성격과 범위, 목적이 정보 주체에 대한 정기적이고 체계적인 대규모의 모니터링을 요하는 개인정보 처리활동들로 구성되는 경우, 3) 컨트롤러 또는 프로세서의 핵심 활동이 제9조에 따른 특정 범주의 개인정보 및 제10조에 규정된 범죄 경력 및 범죄 행위에 관련된 개인정보에 대한 대규모 처리 활동으로 구성되는 경우이다. GDPR은 사법적 권한을 행사하는 법원의 경우 DPO 선임의 예외로 인정하고 있으며, GDPR에서 기술하는 '핵심 활동'은 컨트롤러 혹은 프로세서의 목표를 달성하는 데 필요한 역할 수행에 데이터 처리가 제외될 수 없는 경우를 포함한다. 유럽정

보보호위원회의 가이드라인에 따르면, 병원의 핵심 활동은 의료 서비스 제공이다. 하지만 환자의 건강 기록과 같은 의료 관련 데이터를 병원이 처리하지 않고는 병원의 본래 목적인 의료 서비스를 안전하게 제공할 수 없다. 따라서 병원은 GDPR에서 규정한 '핵심 활동'을 수행하는 것으로 간주됨에 따라 DPO 선임의 의무 기관에 해당된다. 또한 쇼핑센터 및 공공장소의 감시를 수행하며 영상 기록 데이터를 의무적으로 처리하는 보안 회사의 경우, DPO를 반드시 지정해야 한다. 보안 회사의 '핵심 활동'은 영상 기록을 비롯한 개인 데이터를 처리하는 것에 있기 때문이다. 하지만 조직 내부에 고용된 직원에게 임금을 지불하기 위한 목적 혹은 직원 대상의 일반적인 IT 지원 활동만을 수행하는 기업의 개인정보 처리 활동은 '핵심 활동'이 아닌 비즈니스 기능의 일환으로 간주되어 '핵심 활동' 이행 여부에 따른 DPO 선임 의무 기업 대상에서 제외된다.

유럽정보보호위원회에 따르면, GDPR이 규정한 정보 주체에 대한 '정기적이고 체계적인 모니터링(regular and systematic monitoring)'은 온라인상의 모든 형태의 추적 및 프로파일링을 포함 한다. 예를 들어, 웨어러블 디바이스를 통한 사용자의 건강 체크, 광고성 이메일 발송, 신용평가 조회를 통한 신용평가등급 부여, 위치 추적 등이 모두 포함 된다. 즉, 정보 주체에 대한 모니터링이 시스템을 통하여 특정 기간 동안 반복되어 발생하거나 조직적 차원에서 특수한 목적을 가지고 지속적으로 사용자의 데이터 수집을 실시하는 경우이다.

GDPR은 각 사업장에서 쉽게 DPO에게 접근 가능할 경우, 사업체 그룹의 1인 DPO 선임을 인정하고 있다. 즉, 여러 공공기관이 단일 DPO를 임명할 수 있으며, 그룹 형태의 기업은 그룹 전체에 해당하는 1인의 DPO 선임이 가능하다. 또한 GDPR은 컨트롤러를 포함한 컨트롤러 조직 내부 직원 및 서비스 계약과 같은 절차를 통하여 외부인에 대한 DPO의 선임도 허용 한다.

아래의 Fig. 1은 유럽의 DPO Network Europe에서 제공하는 각 기업의 DPO 임명 의무 여부를 알아보기 위한 의사 결정 나무를 국문으로 번역한 것이다. 이를 바탕으로 국내 각 기업은 자사가 DPO 선임 의무를 수반하는지 자율적으로 판단할 수 있다.

2.2 DPO 자격 기준

DPO에게 요구되는 전문성 및 자격 기준에 대해서 GDPR은 엄격하게 정의하지 않았지만, 데이터보호법 및 관련 관행에 대한 전문적 지식과 데이터 처리 등의 실무 작업을 수행 할 수 있는 기술 능력을 DPO가 보유할 것을 권장한다[4]. 유럽정보보호위원회의 DPO 가이드라인에 따른 DPO의 자격 요건을 종합적으로 살펴보면 첫째, DPO는 기업이나 기관의 개인정보 처리의 특성을 고려한 전문 지식을 갖추어야 한다. 즉, 기업이 처리하는 데이터의 민감도, 복잡성 및 양에 DPO의 전문성은 비례해야 하며 기업의 개인정보 국외 이전 여부에 따라서 DPO의 보유 전문성에도 차이가 있어야 할 것을 명시하고 있다. 예를 들어, 데이터 처리 활동이 복잡하거나 방대한 양 혹은 민감 데이터를 주로 처리하는 기업의 DPO는, 그렇지 않은 기업에 비하여 보

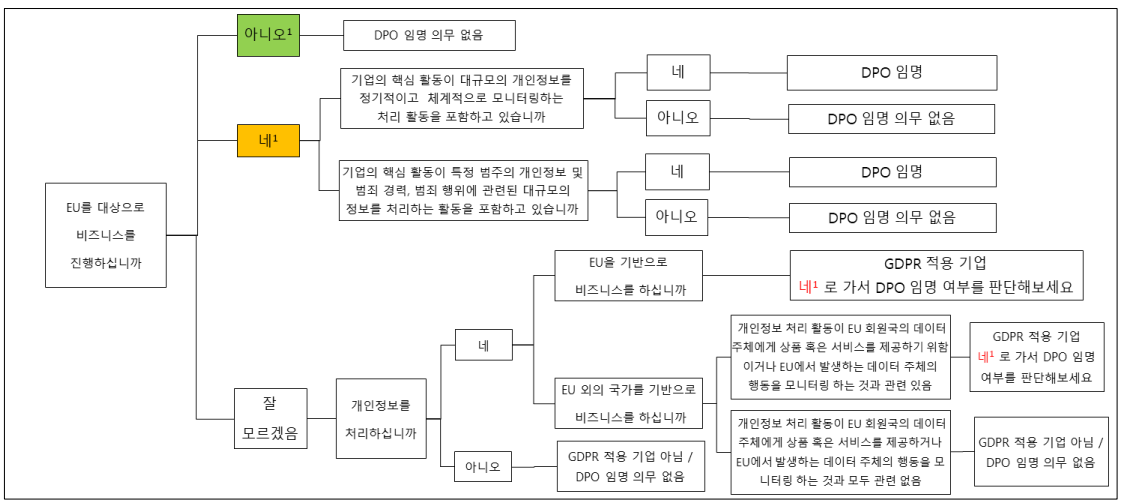

그림 1. DPO 의무 지정 기업 구분
Fig. 1. SHOULD YOUR COMPANY APPOINT A DATA PROTECTION OFFICER (DPO) UNDER THE EU GDPR?

다 높은 수준의 전문 지식을 보유하여야 한다. 둘째, DPO는 자국 및 유럽연합 회원국의 개인정보보호법 및 관행, GDPR에 대한 상세한 이해가 필요하다. 또한 DPO는 개인정보처리 작업, 정보 기술 및 보안 전반에 대한 기술 처리 능력도 요구되며 기업 및 기관의 규칙 등에 대한 이해가 수반되어야 한다. 마지막으로 높은 수준의 직업 윤리 의식이 DPO에게 요구된다. DPO의 주된 역할은 GDPR 준수에 있음에 따라 DPO는 기업 내에서 개인정보보호 문화를 활성화 할 수 있어야 한다. 이를 위하여 데이터 처리 원칙, 데이터 주체의 권리 보호, 데이터 보안과 같은 GDPR의 핵심 요소를 구현하는 데 앞장서서 조직의 개인정보보호 문화를 정착시킬 수 있는 선도 능력이 필요하다.

2.3 DPO 역할

GDPR은 개인정보보호를 위하여 DPO의 역할을 제39조에서 다음과 같이 정의하였다. DPO는 1) GDPR 및 유럽연합 회원국의 개인정보보호 법규를 바탕으로 컨트롤러, 프로세서 및 임직원에게 관련 정보, 조언 제공, 2), GDPR 및 개인정보보호 법규의 준수 이행 여부 모니터링, 내부 정보보호 활동 관리, 정보보호 관련 인식 제고 및 훈련 실시 촉구, 3) 개인정보 영향평가(DPIA, Data Protection Impact Assessment)에 대한 자문 및 평가 이행 감시, 4) 개인정보보호 감독기관과 협조, 5) 개인정보처리 과정에 있어서 감독기관의 연락처의 역할을 수행하고 자문을 제공 한다. 다음의 표 1은 유럽정보보호위원회의 DPO 가이드라인에서 제시한 DPO의 주요 업무이다.

표 1. DPO 역할 및 상세 업무 수행 사항
Table 1. The roles and duties for DPO

DPO 역할	DPO 상세 업무
GDPR 준수 여부에 대한 모니터링	· 처리 활동을 식별하기 위한 정보 수집 · 처리 활동에 대한 준수 여부 확인 및 분석 · 컨트롤러 또는 프로세서 대상으로 조언, 자문 제공
개인정보 영향평가에 대한 역할	· 개인정보 영향평가 수행 여부 · 개인정보 영향평가 수행을 위한 방법론 · 개인정보 영향평가의 조직 자체 수행 혹은 아웃소싱 여부 · 데이터 주체의 권리와 이익에 대한 위험을 완화하기 위해 적용되는 어떤 보호 장치 (기술 및 조직 조치 포함) · 개인정보 영향평가의 적절한 수행 여부 및 평가결과 (추가적으로 적용할 보호 조치의 필요 여부 등) 및 평가 과정의 GDPR 준수 여부

2.4 DPO 지위 및 책임

GDPR은 DPO의 지위를 보장하고자 조직에서 DPO의 의견이 항상 비중 있게 다루어질 것을 강조하며 DPO의 의견이 수용되지 않는 경우, 이에 대한 사유를 공식적으로 문서화할 것을 권고 한다. 또한 DPO는 고위 및 중간 관리 경영진의 회의에 정기적으로 참여할 수 있어야 하며 개인정보 유출 등의 사건 발생 시, DPO가 사건에 적시에 대응할 수 있도록 신속하게 DPO에게 통지하여야 한다. 이외에 GDPR은 기업이 DPO가 전문 지식을 유지하고 업무를 수행하기 위하여 제공 받아야 할 자원 및 지원 사항을 포함하고 있다. 기업은 1) DPO의 역할을 위한 고위급 경영진의 적극적 지원, 2) DPO가 업무 수행을 위하여 필요한 충분한 시간의 보장, 3) 재정적 지원 및 적절한 인프라 제공, 4) 조직 내 모든 임직원 대상의 DPO 선임에 대한 공식적 통지, 5) DPO가 필요시 조직 내 타 부서로부터 정보 및 자원의 지원을 받기 위한 조치 마련, 6) DPO의 지속적인 훈련 기회를 제공하여야 한다.

GDPR의 제5조 2항에 따르면, 컨트롤러는 동조 1항에 따른 개인정보 처리 원칙을 준수할 책임과 이에 따른 준수를 입증할 수 있어야 하는 책임성(accountability)을 갖는다. 이에 제24조 1항은 컨트롤러가 GDPR 규정의 준수에 따라 개인정보를 처리함을 보장하고 이를 입증할 수 있는 적절한 기술적 · 조직적 조치를 이행할 것을 명시하고 있으나 DPO의 위반 사항에 대해서는 별도로 상정하고 있지 않다. 또한 제83조에서는 컨트롤러 및 프로세서가 DPO의 업무를 지원하지 않는 경우에 대하여 과징금 부과를 규정하고 있으나, DPO에게는 별도의 과징금 부과 원인이 되는 의무를 부여하지 않는다. 이외에 GDPR은 DPO를 고용한 기업은 DPO의 독립적인 임무 수행 및 해당 임무를 수행함에 따라 해고나 불이익을 당하지 않을 것을 보장하여야 하며, DPO가 기업 조직의 최고 경영층에 보고할 것을 명시하였다.

Ⅲ. 국내 DPO 유사 제도 및 해외 임명 사례 분석

제3장에서는 국내 기업 환경에서 생소한 DPO의 개념을 구체적으로 제시하고자 한다. 이를 위하여 현재, 국내에서 시행되고 있는 정보보안 관련 유사 제도와 DPO의 비교, 분석을 수행하여 국내 DPO 임명의 필요성을 확인한다. 또한 향후, 국내 기업의 DPO 적임 요

건을 형성하기 위한 토대로 DPO 임명을 완료한 실제 해외 글로벌 기업의 사례를 분석한다.

3.1 국내 CISO, CIO, CPO, CSO 및 DPO 비교

정보통신기술의 발달과 보급은 정보의 다양한 활용을 가능하게하며 기업 환경에서 정보 자산의 가치를 높였다. 이는 국가의 구분을 막론하고 기업 환경에서 정보보안의 중요성을 증가시키며 보안 패러다임을 변화하게 하였다. 이에 기업은 과거에 비하여 높은 수준의 보안 환경을 추구하게 되었으며 이는 기업이 정보보호 및 보안 관리체계를 총괄할 수 있는 담당자 역할의 필요성을 인지하게 하였다. 이로 인하여 오늘날 등장한 대표적인 직책이 최고정보보안책임자(CISO), 최고정보책임자(CIO), 개인정보관리책임자(CPO), 최고보안책임자(CSO)이다. 이들은 기업의 안전한 보안 환경 구축 및 유지를 통하여 개인정보보호, 정보보안이라는 공통적인 목표를 달성하고자 각각의 직위에 맞는 업무를 수행한다.

전세계의 기술 담당자 약 2천 5백명을 대상으로 실시한 설문 조사에 따르면, 32%가 CIO, 21%는 CISO, 14%는 최고경영자(CEO)를 GDPR의 책임자로 적합하다고 응답하였다[4]. 앞선 설문 조사의 결과와 같이, 전세계 다수의 기업에서 CISO, CIO, CPO, CSO를 선임하였음에도 불구하고 기업에서 요구하는 이들의 업무, 자격 요건, 특징 등이 다르다. 따라서 GDPR 책임자에 적합한 역할도 기업마다 상이한 응답을 보였다. 이에 관련 책임자의 역할을 획일적으로 정의하기에는 무리가 있다. 이는 정보보안의 환경이 각 국가들 마다 다르기 때문에 각 책임자의 업무 및 특징도 국가와 기업에 따라 차이를 갖기 때문이다. 본 연구에서는 국내 현행 법령과 국내 기업 환경의 범위에서 CISO, CIO, CPO, CSO의 자격 요건, 역할 및 특징을 바탕으로 GDPR에서 규정한 DPO와 차이점을 밝히고자 한다. 이는 본 연구의 목적이 국내 기업에서 적합한 DPO 모델을 도출하여 이를 효과적으로 운용 및 정착시키기 위한 방안을 모색하는 것에 있음에 따라 국내 상황에 제한하여 살펴보고자 한다.

국내 업종별 정보보호 관련 책임자 임명 현황을 살펴보면 2016년 기준, CPO는 10.5%, CIO는 9.4%, CISO는 8.9%이다[5]. 국내 기업에서 가장 높은 임명 비율을 차지하고 있는 CPO는 기업의 정보기술 활용을 지휘하며 정보기술전략을 통합적으로 관리 및 설계하는 책임자이다. 개인정보보호법 제31조, 정보통신망법 제27조에서는 정보통신서비스 제공자 등의 국내 일부 기업에 대하여 개인정보보호책임자 즉, CPO의 임명을 의무화하고 있다. CPO는 개인정보를 수집, 이용, 제공, 파기하는 개인정보 라이프 사이클 전체를 관리하며 정보 주체의 고충을 처리하는 책임자이다. 국내 기업에서는 CPO와 CISO를 주로 겸직하는 형태로 나타나고 있으나 사실상 업무 성격에 있어 차이를 보인다. 정보통신망법 제 45조의 3항에서 기술한 CISO의 업무 내용을 살펴보면 CISO는 기업의 정보보호관리체계의 수립 및 관리, 운영 등을 총괄하는 정보보호최고책임자이다. 따라서 CISO는 정보보안을 위협하는 외부 요소를 식별하여 정보유출 방지 및 정보보안을 위한 기술적 대책을 마련하고 관련 법률에 대응한다. 또한 CISO는 기업의 지적 자산을 보호하고 예기치 못한 외부의 침해 혹은 내부자의 유출로 인하여 기업의 손실을 방지하기 위한 수단의 마련을 강구한다[3,6]. 이와 같이 CISO는 기술의 관점에 주안을 둔 반면에 CPO는 정보보안의 관리적 측면의 역할이 크다. 국내에서는 금융회사 등을 비롯한 전자금융업의 기관에 대해서는 CISO의 설치를 의무화 하였다. CSO는 기업의 보안 환경 전체를 관장하는 역할로 IT 보안과 더불어 사옥의 물리적 보호와 같이 포괄적인 보안업무를 담당하는 직책으로 CISO와 다소 차이를 보인다. 하지만 최근 들어 CISO와 CSO를 크게 구분하지 않는 추세이다[7]. CIO는 IT자원을 효율적으로 운영하고자 이를 위한 전략 수립 및 수행을 총괄한다. 국내 공공기관의 CIO 지정은 의무화 되어 있으며 과거, 국내 대부분의 기업은 CIO가 CISO를 겸임하는 추세였다. 하지만 CIO는 IT 비즈니스 및 운영 관리의 책임을 지니는 반면에 CISO는 기업의 보안 책임자로서 두 지위의 역할과 책임의 분리 필요성이 줄곧 제기되어 왔다[8]. 특히, 2014년 발생한 은행과 카드사의 대규모 개인정보 유출 사건은 CISO와 CIO의 겸직을 법적으로 금지하도록 하는 전자금융거래법 제21조의2 제4항을 신설하는 주요 배경이 되었다. 국내 현행법에서 규정하고 있는 CISO, CIO, CPO, CSO와 GDPR에서 제시한 DPO는 다음과 같은 차이를 갖는다.

첫째, 국내법에서 개인정보 및 정보보안 책임자의 선임 대상은 무조건 해당 기업의 내부 직원으로 한정되어 있다. 이에 반해 GDPR에서 규정하는 DPO는 조직 내부의 직원도 가능하나 아웃소싱 형태의 고용도 인정하고 있어 DPO의 소속을 폭넓게 인정한다. 또한 DPO는 임명 요건으로 직위가 아닌 업무 능력, 실무와 관련된 전문지식을 요구하고 있으나 국내 책임자는 모두 특정 직위가 필수 조건이다. 공공기관의 경우, 특정 직위의 공무원이어야 하며 개인정보처리 기업은 임원, 사업주, 부서장과 같은 조직 내 지위를 법률상 조건으

표 2. 국내 CPO, CIO, CSO, CISO 및 DPO
Table 2. CPO, CIO, CSO, CISO & DPO

구분	CPO	CIO	CSO	CISO	DPO
	개인정보보호 책임자 (Chief Privacy Officer)	정보화책임관 (Chief Information Officer)	정보보호 최고책임자 (Chief Security Officer)	정보보호책임자 (Chief Information Security Officer)	정보보호담당관 (Data Protection Officer)
근거 법령	개인정보보호법 제31조 정보통신망법 제27조	국가정보화기본법 제11조	정보통신망법 제45조의3 전자금융거래법 제21조의2 정보통신기반보호법 제5조 제4항		GDPR 제37조
임명 요건	종업원 수 5명 미만인 정보통신서비스 제공자	국가기관과 지방자치단체	자산 2조원 이상, 종업원 수 300명 이상의 금융회사 또는 전자금융업자		1) 공공기관에 해당되는 경우, 2) 기업 및 단체의 핵심활동이 정보주체의 활동을 대규모로 모니터링 하는 경우, 3) 기업 및 단체의 핵심 활동이 민감 정보나 범죄정보의 대규모 처리에 관여된 경우
자격 요건	임원, 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장	해당 기관 및 단체의 장이 임명하는 자	유관 자격 및 학력 보유 여부		데이터보호법에 대한 전문성 및 데이터 처리 수행 능력
책무	개인정보 처리 업무 총괄 및 개인정보 유출 사고 발생 시 책임 수행	조직의 정보기술을 감독하고 전략을 세워 정보 자원 관리 총괄	조직 전반의 보안 위험 감소를 위하여 모든 보안 분야에 대한 관리, 감독	전사적 차원에서 정보 시스템 관련 인적, 물적 보안 관리체계를 수립, 운영, 통제	개인정보보호를 위해 GDPR이 정하고 있는 활동에 대한 모니터링 및 GDPR 준수 여부 감독
고용 형태	내부 직원으로 한정됨				내부 직원 및 아웃소싱 형태의 고용 인정
특징	정보보안의 비즈니스 관리적 측면에 주안을 둠	CISO 겸직 금지	-	금융기관은 의무적 설치이며 CPO 대비 정보보안의 기술적 측면의 역할이 큼	강력한 독립성 보장

로 규정하여 해당 직위 이상을 가진 자만이 정보보안 책임자로서의 요건에 충족한다.

둘째, GDPR은 DPO의 업무상의 독립성, 업무에 따른 책임 소재를 조항으로 보호하고 있으나 국내는 이에 대한 별도의 보호조치가 마련되어 있지 않다. DPO는 업무에 따른 책임과 불이익으로부터 비교적 자유로운 반면에 국내법은 이와 상반된다. 2014년 국내 보안 담당자들을 대상으로 실시한 설문조사의 응답자들은 기업의 보안 침해 사고의 법적 책임자로 CEO(약 36%) 및 보안 관련 임원, 보안 실무 책임자(약 30%)를 지목하였다[14]. 이는 국내 개인정보보호법의 법령 및 고시에서 보안 관리를 IT 문제와 더불어 기업의 리스크 관리를 포함하는 정보보호 거버넌스 개념으로 다루고 있기 때문이다[15]. 따라서 국내 기업은 보안 관리의 실패를 기업의 경영 관리 실패로 간주하며 이에 대한 법적 책임을 CEO 및 CISO를 비롯한 정보보안 임원이 져야 한다는 인식이 확산되어 있다. 반면에 GDPR의 제38조 3항에 따르면, DPO는 DPO의 책무를 이행하는 것과 관련하여 컨트롤러 혹은 프로세서로부터 처벌 및 해고당할 수 없음을 규정하여 업무에 따른 불이익으로부터 DPO를 보호한다. 또한 DPO 가이드라인의 3.4.는 업무를 수행함에 있어서 DPO는 기업의 특정 비즈

니스 목표 달성에 미치는 영향을 고려해서는 안되며 DPO의 업무에 대해서 타인으로부터 강요 혹은 지시 받지 않아야 함을 DPO의 자율권으로 보장한다. 또한 DPO는 사내 정보보안 정책 및 관련 법규에 대하여 특정 입장을 상사로부터 강요받지 않아야 하며 스스로 특정 관점을 취해서는 아니됨을 명시한다. 위의 표 2는 CPO, CIO, CSO, CISO 및 DPO의 임명 요건, 역할, 책무 등을 비교한 것이다.

3.2 해외 글로벌 기업의 DPO 임명 사례

GDPR 시행을 앞두고 다수 기업의 DPO 채용 공고가 활발히 진행되고 있으며 현재까지 주요 유럽연합 회원국 및 미국에 본사를 둔 기업을 중심으로 DPO 선임이 활발히 이루어졌다.

본 연구에서는 DPO 채용이 완료된 글로벌 기업의 사례를 분석하여 DPO의 보유 역량 및 특징을 구체화 하고자 한다. 이는 실제 선행 사례를 분석함에 따라, DPO에게 요구되는 역량을 평가하기 위한 보다 객관적인 지표가 되며 향후, 국내 기업의 DPO 임명을 용이하게 한다. GDPR은 조직 내 DPO의 지위 및 채용 프로세스를 구체적으로 규정하지 않으며 DPO의 고용 형태에 대해서도 포괄적으로 인정하여 기업의 DPO 선임에 대한 어려움을 가중시켰다.

현재, 임명된 DPO의 조직 내 지위 및 고용 형태를 살펴보면, 외부 적임자 발굴을 통한 DPO 채용의 비율이 높다. 대표적으로 글로벌 광고 기업인 영국의 Dentsu Aegis Network 및 독일의 전자 기업인 Siemens의 사례가 있다. 이들은 대부분 IT 전문 글로벌 기업에서 데이터보호 및 프라이버시 관련 업무의 책임자를 자사의 DPO로 고용하였다. 이외에 독일의 IT 솔루션 개발 업체인 GFT Technologies와 같이 기존의 내부 CPO를 DPO로 임명한 경우도 있으며, Live Nation Entertainment 및 DataXu은 현재 기업의 부회장이 DPO를 겸직하는 등, 내부의 임원이 DPO를 역임하고 있다. 따라서 GDPR에서는 DPO의 조직 내 위치를 엄격히 제시하지 않았지만, 현재 대다수의 DPO가 임원, 책임자 등을 비롯한 비교적 상위 서열에 랭크되는 점을 확인할 수 있다. 이는 과거 CPO 및 타 기업의 프라이버시 책임자 등이 DPO로 선임됨에 따라 DPO의 조직 내 위치가 주로 상위 직급에 배치된 것으로 판단된다.

현재까지 DPO를 임명한 기업의 유형은 IT 기술 연구 전문 기업, 제조업을 비롯하여 독일의 Deutsche Post DHL Group과 같은 우편·물류 전문 기업도 DPO 고용을 완료하였다.

DPO 임명 이전의 기업 채용 공고를 분석한 결과, 대부분 7~10년 이상의 데이터 보호 관련 수행 경력을 요구하였으며 컴퓨터 공학 및 법학 학위를 요구하는 경우도 소수 존재하였다. 이에 따라 실제 대다수의 DPO가 CIPP/E(Certified Information Privacy Professional credential for EU professionals), CIPM(Certified Information Privacy Manage) 등의

표 3. 주요 글로벌 기업의 DPO 선임 사례
Table 3. Cases for global firms' DPO

기업	Yoti Ltd	MasterCard Worldwide	Capgemini Group	Gartner	Valmet	DataXu
기업 소재 (DPO 임명 시기)	영국 (2016.10 ~)	미국 (2013.07 ~)	프랑스 (2015.11 ~)	영국 (2017.04 ~)	핀란드 (2017.02 ~)	미국 (2014.02 ~)
기업 분류	소프트웨어 개발	카드사	IT 컨설팅	IT 연구 및 컨설팅	펄프 제조 및 기술 개발	소프트웨어 개발
정보 보호 보유 자격	CIPP/E, CIPM, FIP	CIPP/US, CIPP/G, CIPT, CIPM, CIPP/A, CIPP/E, CIPP/C	CIPP/E, CIPM	CIPP/E, CIPP/US, CIPM	CIPP/E, CIPT, CIPM, FIP	CIPP/US, CIPP/G, CIPT
보유 경력	약 10년 이상의 데이터보호 컨설팅, 법률 자문 활동	약 20년 이상의 자사 프라이버시 변호사 활동	15년 이상의 IT 전문 변호사 활동	약 20년 이상의 데이터보호 관련 컨설팅 수행 및 변호사 활동	약 20년 이상의 IT, SW 개발 전문가	약 5년 이상의 IT 컨설팅 및 본사 법무팀 총괄 경력
특징	ICO 대표 및 LLM 취득	CPO 역임 및 JD 취득	LLM 취득	JD 취득	-	JD 취득

정보보호 관련 자격증과 법학 학위를 소유한 것으로 확인되었다. 즉, 데이터보호법에 대한 전문성 및 데이터 처리 능력을 GDPR이 DPO의 자격 요건으로 제시함에 따라, 해당 역량의 보유 여부를 기업은 정보보호 자격증 및 법학 학위의 취득 여부로 평가한 것으로 볼 수 있다. 따라서 현재 활동 중인 DPO 대부분이 장기간 프라이버시 관련 전문 변호사를 역임하거나 기업 내 법률 자문가로서의 역할을 수행하였다. 앞서 제시된 사례 이외에 주요 글로벌 기업의 DPO 임명 사례를 추가적으로 살펴보면 다음의 표 3과 같다.

Ⅳ. 국내 DPO 정착 방안

GDPR 실효에 따라 새롭게 등장한 DPO는 국내 기업 환경에서 생소한 개념으로 DPO의 국내 정착을 위해서는 다방면의 노력이 요구된다. GDPR을 준수하지 않음에 따라 발생하는 벌금은 기업의 존폐에 영향을 미칠 만큼의 경제적 손실을 발생시키고 장기적으로 기업의 브랜드 이미지에 부정적인 영향을 미친다.

따라서 사전에 이를 준수하고자 하는 대응책을 마련하는 것은 매우 중요하다. 이에 본 연구에서는 DPO의 성공적인 국내 정착과 효과적 운용을 도모하고자 1) 국가 차원의 DPO 제도화 방안, 2) 한국형 DPO 모델 개발, 3) DPO 도입 단계적 프레임워크를 제시한다.

4.1 국내 DPO 제도화 방안

GDPR이 탄생한 유럽연합 회원국을 살펴보면 대부분 GDPR에서 제시한 큰 틀을 바탕으로 각 국가의 특성과 기업 환경에 맞춘 DPO의 선임을 추구한다. 이는 GDPR에서 DPO 임명의 구체적인 방식 및 상세한 DPO의 선임 요건을 명시하지 않고 각 국가 및 기업의 환경적 특성에 따른 적합한 DPO 임명의 자율성을 인정하였기 때문이다. 이에 따라 유럽연합의 회원국은 각 국가의 주도적인 노력을 바탕으로 자국 기업의 DPO 임명을 도모하고 있다. 이들은 정부에서 자체적으로 개발한 GDPR 가이드라인에서 DPO 임명을 비중 있게 다루거나 DPO 선임의 구체적 요건을 제시하는 등 DPO 선임을 국가 차원에서 권장한다. 프랑스 국가정보위원회(CNIL, Commission Nationale Informatique et Libertes)는 GDPR 실효에 앞서 정부주도의 태스크포스를 구성하여 GDPR 준수를 위한 가이드라인을 발표하였으며, 1단계로 DPO 임명을 선정하였다. 특히, 해당 가이드에서는 DPO 의무 임명 기관이 아니더라도 DPO 임명을 권고하여 자국 기업을 대상으로 DPO 역할의 중요성을 인지시킨다. 독일은 기존의 개인정보보호법(German Data Protection Amendment Act)을 개정하여 개인정보의 자동 처리 업무를 담당하는 종업원이 10명 이상인 경우 DPO 임명을 의무화할 것을 규정하였다. 이는 GDPR 적용 대상을 종업원 수 250명을 기준으로 규정하여 이에 따른 DPO 임명을 규정한 GDPR보다 엄격한 DPO 지정 요건이다. 영국의 정보위원회(ICO, Information Commissioner's Office)는 GDPR 준수 12가지 원칙을 발표하며, GDPR의 핵심 항목으로 'DPO 임명'을 선정하였다.

오늘날 국내에서도 프랑스, 영국, 독일의 사례와 같이 정부 차원의 DPO 가이드라인을 개발하여 국내 기업에 배포하는 것이 DPO의 성공적인 도입과 정착을 위한 가장 대표적인 방안이다. 조직을 대상으로 제공된 정보보안 관련 가이드라인은 실제 구성원의 정보보안 행동을 유도하는데 필수적이기 때문에[9] DPO 역시 가이드라인의 개발이 선행되어야 한다. 하지만 유럽정보보호위원회 및 해외 다수의 기관에서 이미 개발하여 배포한 DPO 가이드라인이 존재하고 있으나, 이는 전 세계의 기업에서 바로 적용 가능한 포괄적인 내용을 다루고 있기 때문에 국내 기업 환경을 상세히 반영하지 못하는 한계를 지닌다. 따라서 국내 기업의 환경적 특수성을 반영한 가이드라인의 개발 및 배포는 기존의 유럽에서 개발된 가이드라인보다 높은 수준의 실효성 즉, 국내 DPO의 성공적인 정착과 활성화를 기대할 수 있다.

DPO 가이드라인의 개발이 정부 주도의 단기적 방안이라면 장기적인 관점에서 국내 관련 법령의 개정 등과 같은 방식을 함께 검토해볼 수 있다. 현재, 개인정보보호법, 정보통신망법에서 규정하고 있는 CISO, CPO 등은 앞서 제시한 바와 같이 GDPR에서 요구하는 DPO와 역할, 자격 요건 등에서 차이를 보인다. 그리고 앞서 본 바와 같이 DPO는 자국 및 유럽연합 회원국의 개인정보보호법 및 관행, GDPR에 대한 상세한 이해가 필요하다. 따라서 현재 국내 각 기업이 보유한 CISO를 비롯한 보안 관련 책임자가 DPO를 대체할 수 없기 때문에 향후, GDPR 시행에 따른 기업의 DPO 선임은 피할 수 없게 되었다. 또한 기존 법규가 CISO 등의 관련 책임자의 역할 및 지위를 보호하지 못함에 따라 GDPR이 규정한 DPO의 독립성 보장 등이 국내 기업 환경에서 구현되기 어렵다. 이는 향후 국내 환경에서의 DPO의 정착을 저해하게 된다. 따라서 국내 기업에서는 DPO를 선임함에 따라 DPO를 합법적으로 관리 및 감독할 수 있는 기업의 권한과 더불어 DPO의 지위를 보장할 수 있는 법적 근거의 마련이 필요하다고 본 연구는 판단하여 다음과 같은 법령 검토의 방식

을 제안한다.

첫째, 기업의 DPO에 관련한 별도의 법규를 신설하여 국내 기업에 고용된 DPO를 규제하는 방식이다. 이는 현행 법규에서 DPO 관련 조항이 존재하지 않음에 따라 이와 관련된 별도의 법률을 제정하고 이를 근거로 국내 DPO를 관리하는 방식이다. 해당 법률의 제정은 DPO 의무 기업 대상의 지정 요건부터 상세히 규정이 가능한 점과 국가 차원에서 효과적으로 DPO를 관리 및 보호할 수 있다는 점에서 의의가 있다. 하지만 앞선 표 2에서 제시하였던 바와 같이, 국내의 경우 개인정보보호법 제31조, 정보통신망법 제27조, 전자금융거래법 제21조의2에 따라 적용 대상이 되는 기업은 개인정보보호책임자 및 정보보호담당자의 의무 설치를 이미 규정하고 있다. 이들의 책임과 역할 및 고용형태가 모두 동일하지 않지만 사내의 정보보안 및 개인정보보호를 수호하고자 하는 동일한 목적으로 형성되었으며 DPO 역시 이와 유사한 목적을 갖는다. 따라서 유사한 목적의 지위를 지정하기 위하여 DPO 도입에 따른 추가적인 법령을 제정하는 것은 필요하지 않을 수 있다. 구체적으로 개인정보보호법 제 31조의 2항은 개인정보보호책임자에게 개인정보 처리 실태에 대한 정기적인 모니터링을 실시할 것을 요구하고 있으나 이는 DPO가 갖는 역할 의무와 동일하기 때문에 이를 별도의 독립된 법률로 각각 규정하는 것이 필요하지 않을 수 있다. 또한 법령의 제정을 단기간에 구현하기 어렵다기 때문에 DPO 도입이 얼마 남지 않은 현 시점에서 한계점을 갖는다.

둘째, 국내 현행법에서 각각 규정하고 있는 개인정보보호책임자 관련 법규에 GDPR에서 요구하는 DPO의 보장 조건 등을 추가하는 방식이다. 개인정보보호법 제31조, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제 45조의3, 전자금융거래법 제 21조의2를 각각 검토하여 해당 조항에서 다루고 있는 관련 책임자의 범위에 DPO의 지위를 추가적으로 인정하는 것이다. 이는 기존의 법규가 규정하지 못하였던 관련 책임자의 업무 독립성 및 자격 요건 등에 대한 추가를 통하여 DPO와 더불어 이들의 법적 지위를 확보할 수 있는 토대가 된다. 또한 현재 개인정보보호법, 정보통신망법에서 규정하고 있는 CPO, CISO 등은 기업 내부 직원에 한정되어 임명할 것을 의무화 하고 있다. 즉, 아웃 소싱 형태를 금지하고 있는 것으로 GDPR에서 인정하는 DPO의 고용 형태와는 차이를 보인다. 따라서 이와 같은 차이의 균형을 맞출 수 있도록 하여 향후 GDPR 시효에 따른 국내에서 발생 가능한 문제를 대비할 수 있도록 하여야 한다.

앞서 제시된 법령의 제정 및 관련 조항의 신설은 단기간에 이루어질 수는 없으나 법적 구속력이 있는 제도를 마련함에 따라 장기적으로 국내 기업에서 DPO의 정착과 효과적인 운용을 도모할 수 있다. GDPR이 도입됨에 따라 국내 기업은 GDPR을 규율하는 유럽연합 감독당국의 규율 이전에 국내 법규를 바탕으로 국가가 DPO 관련 사항을 사전에 감독 및 통제할 수 있다는 점에서 기대효과가 있다. 또한 국내에서도 GDPR에서 요구하는 DPO 관련 의무조항이 새로운 법이나 기존법의 개정 내용으로 포함된다면, 국내기업도 이미 국내법에 따라 DPO 관련 자격이나 의무를 지키고 있을 가능성이 높기 때문에 국내 기업의 GDPR 위반 가능성이 감소하는 동시에 국내 기업의 수월한 유럽 시장 진출을 도모하게 된다.

4.2 한국형 DPO 모델 개발

GDPR은 각 국가 기업 환경의 다름을 인정하기 때문에 DPO의 자격 요건 및 보유 기술, 전문성 등에 대하여 상세하게 제시하지 않으며 오히려 국가와 기업의 특징에 맞는 DPO의 임명을 권장한다. 따라서 DPO의 역할, 자격 기준 등 모든 요건을 유럽 국가의 DPO 사례를 모방하여 국내 기업에 동일하게 도입하는 것은 바람직하지 못하다. 이와 같이 획일화된 DPO 모델의 적용은 DPO 임명의 원초적인 목적을 달성할 수 없다.

GDPR 발표에 따른 DPO 의무 임명이 전세계적으로 이슈화됨에 따라, 다수의 관련 전문가가 공통적으로 선정한 DPO의 요건은 GDPR과 더불어 국내 및 유럽의 개인정보보호법에 대한 수준 높은 이해와 개인정보 처리와 같은 실무 IT 능력이다. 이외에 유럽 감독 당국과 자유롭게 소통할 수 있는 커뮤니케이션 능력이다. 올해 페이스북에서 공고한 DPO의 필요 역량을 추가적으로 살펴보면 현재의 정책 이슈를 다룰 수 있는 능력, 신기술 관련 지식 및 관심 보유, 자사의 비즈니스 모델, 제품과 플랫폼에 대한 높은 식견 까지를 요구하고 있다. 따라서 DPO는 특정 법률에 대한 전문성을 가진 변호사, 정보보안 IT 전문가 혹은 IT 전문 컨설턴트도 아닌 융합적 능력을 보유한 인재를 필요로 함에 따라 이에 적합한 인물을 찾는 것이 현재 전세계 기업이 직면한 문제이다. 이를 위하여 CIPP/E 및 CIPM 등과 같은 관련 인증 보유를 자격 요건으로 제시하는 경우도 있으나[13] 해당 자격증의 보유는 특정 기술 이해 및 법률에 대한 전문성만을 보장할 뿐 거시적 환경에서 기업의 이해를 담보하지 않는다. 이에 국내 환경에 적합한 DPO의 자질을 도출하여 한국형 DPO 모델 개발이 필요하다.

DPO의 도입은 유럽연합 회권국의 언어와 통화를 지원하여 유럽연합을 대상으로 상품 및 서비스를 지원하는 경우, GDPR 적용 기업으로 인정됨에 따라 대상 범위가 매우 폭넓다. 즉, 대규모의 제품을 생산하여 공급하는 대기업의 형태가 아니어도 GDPR의 적용 대상으로 인정될 수 있다. 따라서 20인 이하의 종업원으로 구성된 대다수의 소규모 기업도 GDPR의 준수를 의무를 수반하게 되며 DPO 선임의 문제에서 자유로울 수 없게 된다. 특히, 국내의 경우, 5명 이하의 종업원 수로 구성된 형태의 온라인 쇼핑몰의 수가 매우 많은 동시에 국내 시장 구조에서 이들이 형성한 영향력은 매우 크다. 따라서 국내 온라인 쇼핑몰에 대한 이해는 국내 시장 전반을 이해하기 위한 토대로 볼 수 있으며 소규모의 형태를 갖고 있음에도 불구하고 간과되어서는 아니 되는 영역이다.

국내 온라인 쇼핑몰의 시장 규모는 2018년 기준, 100조원으로 예상된다[10]. 특히, 국내 온라인 쇼핑몰의 해외 진출 에 따른 매출 성과는 꾸준히 증가하고 있으며, 2017년, 3분기 해외 직접 판매 매출액이 약 7,500억원에 도달하였다[11]. 따라서 국내 시장과 더불어 해외 시장을 상대로 운영 중인 온라인 쇼핑몰의 경우, 유럽연합 회원국의 언어와 통화를 지원하여 해당 국가로 상품을 배송하기 때문에 GDPR의 적용 대상이 되는 동시에 DPO 임명의 의무를 갖는 경우가 다반사이다. DPO 선임의 의무를 수반하지 않는 기업이라 하더라도 GDPR의 적용 대상이 됨에 따라 총괄적으로 GDPR 준수 여부를 관리 및 감독하여야 하는 DPO의 역할은 반드시 필요하다. 하지만 이와 같은 국내 대부분의 온라인 쇼핑몰은 소규모의 형태로 형성되어 있으며 상임 DPO를 고용할 자본의 여유를 가진 경우가 드물다. 또한 국내에 존재하는 IT 기반의 창업 및 중소벤처기업 역시 유럽연합 회원 국가 등의 해외를 주로 대상으로 자사의 기술 및 상품을 납품하여 온라인 쇼핑몰과 유사한 소규모 형태를 갖는다. 따라서 이와 같은 국내의 기업은 소규모임에도 불구하고 주요 거래 시장이 해외임에 따라 국내의 특수한 기업 형태로 고려하여야 한다. 그러므로 국내 기업에 고용되는 DPO의 경우, 이와 같은 국내 기업 환경 및 국내 시장의 특수성에 대한 이해가 추가적으로 요구된다. 특히, 경제적 자본을 비롯한 기반시설의 확립과 장시간의 경영을 통하여 노하우를 축적한 기업의 경우 DPO의 선임에 대한 사전 준비를 다양한 정보와 경험을 활용하여 비교적 수월하게 대비할 수 있으나 온라인 쇼핑몰과 같은 소규모 창업 기업의 경우 사전 준비에 취약할 수밖에 없다. 따라서 소규모 형태의 기업 등에 대하여 GDPR을 비롯하여 DPO 관심을 제고시키고 이러한 국내 시장 규모의 특수성을 이해할 수 있는 DPO의 능력이 필요하다.

GDPR과 국내 개인정보보호법은 모두 정보 주체의 권리를 보장하고 정보의 안전성을 확보하는 것에 목표가 있지만 GDPR과 개인정보보호법은 개인정보에 대한 접근 방식의 차이가 존재한다. GDPR은 온라인에 축적된 방대한 양의 개인정보 즉, 빅데이터의 활용 가치에 중점을 둔 반면에 국내 개인정보보호법은 정보 주체의 개인정보보호에 주안을 둠에 따라 GDPR과 개인정보보호법 사이에는 개인정보에 대한 관점의 차이가 존재한다. GDPR은 개인정보의 가치를 극대화하고자 익명처리와 가명처리를 구분한다. 따라서 재식별 가능성을 필연적으로 수반하는 가명처리정보는 개인정보로서 GDPR의 적용범위에 포섭시켜 법률요건을 충족하는 경우, 목적 외 처리가 허용하는 반면에 익명처리정보는 개인정보에 해당하지 않는 것으로 간주하여 GDPR의 적용을 배제한다. 또한 공익을 위한 기록 보존 및 통계, 학술 목적의 개인정보 처리 활용에 대한 예외를 GDPR은 폭넓게 인정하고 있는 반면에 국내 개인정보보호법은 예외 사유를 동법 제18조 2항과 제58조의 1항에 명시하여 이에 한하여 인정한다. GDPR에 따르면, 마케팅 목적으로 최초로 수집한 개인정보는 이후 가명처리 하여 제 3자의 컨트롤러에게 별개의 동의 없이 제공이 가능하다. 따라서 GDPR은 본래의 개인정보 수집 목적이 아닌 그 이외의 목적에 따른 추가처리를 별도의 법적근거 없이 허용함에 따라, 엄격하게 개인정보의 목적 외 이용을 제한하는 국내 개인정보보호법과 대조된다. 이에 따라 국내 기업의 DPO는 GDPR과 더불어 국내 개인정보보호법에 대한 충분한 이해를 바탕으로 자사의 개인정보 처리를 관리 및 감독하는 동시에 내부의 규정을 조율할 수 있는 능력을 갖추어야 한다.

GDPR에서는 그룹의 형태로 이루어진 기업의 경우, 단일의 DPO 선임을 허용한 바와 같이, 국내 소규모 형태의 기업들은 단일 DPO가 관리하여도 GDPR에 저촉되지 않는 기업 간의 계약 체결 등이 고려되어야 하며 이에 능동적으로 업무를 수행할 수 있는 능력이 국내 DPO에게 요구된다. 이에 따라 국내 DPO 1인이 다수의 기업에 고용될 경우, 각 기업의 비즈니스 기밀을 보장할 수 있는 보다 엄격한 윤리적 의식을 갖추어야 한다.

4.3 국내 DPO 도입의 단계적 프레임워크

독일 및 벨기에를 비롯한 유럽의 국가에서 DPO 임명을 촉진 및 운용을 위하여 관련 법률의 개정 및 제정

표 4. DPO 도입을 위한 단계적 프레임워크
Table 4. Frameworks for adopting DPO

시기	도입기	확산기	정착기
	GDPR 시행 전		GDPR 시행 후
목표	기업의 동기부여를 통한 자율적인 DPO 선임 권고	지정 의무 기업의 DPO 선임 지원	의무 대상이 아닌 기업의 DPO 선임 장려
수행 방법	DPO 임명 기업에 대한 정부 인센티브 제공 (세제 혜택, 재정적 보상 등)	DPO 임명 선행 사례를 바탕으로 DPO 선임 및 운용 활동 지원	DPO 임명에 따른 기업의 개인정보보호 수준 향상 등 우수 사례 발굴 및 확산

을 진행하였다. 현재까지 유럽연합 회원국을 중심으로 법률 제정의 방법을 통하여 DPO 선임 및 운영을 지원하고 있을 뿐이다. 즉, 국내를 비롯하여 전세계적으로 DPO 임명을 유도하기 위한 지원 및 혜택 사항이 구체적으로 형성되지 않았다. 이에 본 연구에서는 단계적 프레임워크를 바탕으로 국내 기업의 성공적인 DPO 도입 및 운용 방안을 도출하고자 한다. 이는 개발된 정책 및 제도의 성공적인 도입과 정착 방안의 강구 과정에서는 단계적 프레임워크가 주로 활용된다[12]. 이는 기업문화의 진화 방식에 따라 도입기-확산기-정착기로 구분하여 각 단계마다의 정책 도입 방안을 제시하는 방식이다.

먼저, DPO 임명의 도입기는 GDPR이 시행되는 이전의 준비 단계로 실질적으로 DPO 선임의 의무에서 모든 기관과 기업이 자유로운 단계이다. 따라서 자율적인 DPO의 선임을 권고하되, 정부 차원의 인센티브 제공 및 적극적인 지원을 통하여 DPO의 임명을 촉구하여야 한다. 현행 국내 법규상 GDPR을 준수하지 않는 것에 대하여 국가 차원에서 강력한 규제 및 처분이 어렵기 때문에 혜택 지원과 같은 보상 체계를 마련하여 국내 기업의 자발적인 DPO 지정을 장려하는 시기이다. 예를 들어, DPO 임명을 완료한 기업에 대하여 세제 혜택을 제공하거나 DPO에게 요구되는 필수 교육 및 훈련 프로그램 등에 수반되는 비용을 국가 차원에서 부담하는 방식으로 재정적 지원이 이루어질 수 있다. 확산기에는 도입기에서 이루어진 DPO 임명 및 운용의 선행 사례를 바탕으로 DPO 지정 의무 대상 기업의 임명을 촉구하는 시기이다. 이와 동시에 해당 시기에는 도입기에서 지정된 DPO의 관리 및 감독이 함께 이루어지는 시기이다. 이는 선임된 DPO가 유명무실한 지위로 전락되지 않기 위해서 DPO의 역할에 대한 기업의 꾸준한 관리를 제고하기 위해서이다. 특히, 확산기의 단계에서는 DPO를 지정하지 않은 의무 대상 기업에 대하여 GDPR을 준수하지 않음에 따라 수반되는 기업의 막대한 경제적 손실 등의 위험성을 강조하여 조속한 DPO 선임을 지원한다. 이 시점의 DPO 선임에는 정부 차원의 혜택 지원 방식이 아닌 DPO를 임명하지 않음에 따라 초래되는 부정적 결과에 대하여 국내 기업이 인지할 수 있도록 하여야 한다. 또한 마지막 정착기는 GDPR이 시행된 시점으로 DPO 임명의 의무 기업을 넘어 의무 대상이 아닌 기업을 바탕으로 DPO 선임을 장려하는 시기이다. 데이터를 보호하는 전담 요원의 설치는 GDPR에서 규정하는 DPO의 의무적 임명 여부와 상관없이 기업의 개인정보보호 수준을 향상시키기 때문이다.

References

[1] B. C. Won, *Two things to remember when preparing for GDPR: Understanding of Employees and DPO*, boannews, Retrieved Oct., 15, 2017, from http://www.boannews.com/media/view.asp?idx=57464&kind=.

[2] H. Im and T. S Kim “The impact of CISO exclusively appointed for the post on the performance of information security,” *Conf. Korea Business Rev.*, pp. 815-820, Aug. 2014.

[3] J. S. Kim, J. B. Kim, and Y. T. Shin, “A study on the effect of CISO’s recognition of the role to the information security performance.,” *Korean Management Consulting Rev.*, vol. 12, no. 4, pp. 21-34, Dec. 2012.

[4] C. Tikkinen-Piri, A. Rohunen, and J. Markkula, “EU general data protection regulation: Changes and implications for personal data collecting companies,” *Computer Law & Security Rev.*, pp. 1-20, Jun. 2017.

[5] *Survey on Information Security Business*, Korea Internet & Security Agency(KISA), 2016. Retrieved Oct., 11, 2017, http://www.kisa.or.kr/eng/usefulreport/surveyReport_View.jsp?cPage=1&p_No=262&b_No=262&d_No=70&ST=&SV=

[6] J. S. Park, D.W. Lee, and J. Y. Jeon, “A study on IS performance and CIO leadership,” *J.*

KSII, vol. 7, no. 2, pp. 103-120, Apr. 2006.

[7] E. S. Kang, *CxO needs to know information security*, Published by HANBIT Media, 2005.

[8] B. S. Cho, "A study into the method of application of information security governance for financial institutions- clarification of the roles and responsibilities between the CIO and CISO from a working level standpoint," M.S. Thesis, Graduate School of Information Security Korea University, Dec. 2016.

[9] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness" *MIS Quart.*, vol. 34, no. 3, pp. 523-548, Sept. 2010.

[10] H. Y. Cho, *An awesome online marketplace... in 2018*, The Asia Business Daily, Retrieved Nov., 11, 2017, from http://www.asiae.co.kr/news/view.htm?idxno=2016112507034231641.

[11] Statistics Korea, *Online Shopping in March 2017*, Report material, Retrieved Oct., 09, 2017, from http://kostat.go.kr/portal/eng/index.action

[12] J. Y. Kim, "A case study about a successful knowledge-management construction strategy," *J. Korea Business Edu.*, vol. 6, pp. 31-49, Jun. 2005.

[13] E. Lachaud, "Should the DPO be certified?," *Int. Data Privacy Law*, vol. 4, no. 3, pp. 189-202, Aug. 2014.

[14] J. Y. Kim, *Should personal information infringement, chief security officer be responsible?*, boannews, Retrieved Oct., 12, 2017, from http://www.boannews.com/media/view.asp?idx=42387.

[15] S. H. Hwang and J. D. Kim, "A study on the goals and processes of privacy governance," *Korea Inst. Inf. Secur. and Cryptol.*, vol. 21, no. 5, pp. 7-11, Aug. 2011.

박 민 정 (Minjung Park)

2014년 8월 : 성신여자대학교 법학과 졸업

2016년 8월 : 이화여자대학교 빅데이터분석학 석사

2016년 9월~현재 : 이화여자대학교 경영학과 박사 과정

<관심분야> 정보보안, 개인정보보호, 정보보안 정책, 데이터 감시 위협(Dataveillance)

채 상 미 (Sangmi Chai)

1999년 2월 : 이화여자대학교 정치외교학과 졸업

2002년 8월 : 서울대학교 경영학과 석사

2009년 6월 : SUNY at Buffalo 경영학 박사

2012년 3월~현재 : 이화여자대학교 경영학과 교수

<관심분야> 정보기술과 인간행동, 정보보안과 조직, 빅데이터 분석

이 명 준 (Myoungjun Lee)

1998년 : 서울대학교 법학과 졸업

2008년 : 사법시험 합격

2011년 : 사법연수원 수료

현재 : 하모니 법률사무소 대표변호사

<관심분야> 개인정보보호, 인공지능과 법