

법무법인 세안(世按)

서울 서초구 서초대로 274 (블루콤 타워, 1201호) / T : 02-3473-0999/F:
02-3473-0997

시행일자 : 2021. 2. 3.

수 신 : (주)아이티아이즈

제 목 : 정보보호정책서의 법적 준거성 검토 요청에 대한 답변

표제의 업무와 관련하여 당 법무법인은 다음과 같은 법률검토의견을
드리오니 업무에 참고하시기 바랍니다.

- 다 음 -

1. 질의의 요지

(주)아이티아이즈에서 클라우드컴퓨팅서비스를 제공하기 위한 운영문
서로서 검토하고, 시행 예정인 정보보호 정책서가 법적 준거성을 충
족하는 지 여부

2. 법적 준거성 검토

가. 정보보호 정책서 작성 목적

- (주)아이티아이즈에서 제정한 정보보호정책서는 (주)아이티아이즈 클라우드 서비스 제공을 위해서 컨설팅, 마이그레이션, 매니지드, XaaS 서비스 등을 대상으로 작성되었음
- 기업의 정보보호정책서는, 개인정보 및 기업 정보보호를 위한 조직 구성, 위험관리, 위반시 이를 제거할 수 있는 조치유무 등 관련규정을 준수하여 작성되어야 한다.

나. 정보보호 관련 법령

- (1) 기업내에서 관리하는 정보에 대한 정보보호 정책서 작성 기준이 되는 근거법으로는, 개인정보보호법, 정보통신망이용촉진 및 정보보호 등에관한법률, 클라우드컴퓨터의 발전 및 이용자 보호에 관한법률을 들 수 있고, 본 정보보호정책서의 목적상 클라우드컴퓨터의 발전 및 이용자 보호에 관한법률이 주요한 준거법률이 될 것이다.

(2) 클라우드컴퓨터의 발전 및 이용자 보호에 관한 법률 및 시행규칙

클라우드컴퓨터의 발전 및 이용자 보호에 관한 법률

[시행 2020. 12. 10.] [법률 제17344호, 2020. 6. 9., 타법개정]

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2020. 6. 9.>

1. “클라우드컴퓨팅”(Cloud Computing)이란 집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원(이하 “정보통신자원”이라 한다)을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신속적으로 이용할 수 있도록 하는 정보처리체계를 말한다.
4. “이용자 정보”란 클라우드컴퓨팅서비스 이용자(이하 “이용자”라 한다)가 클라우드컴퓨팅서비스를 이용하여 클라우드컴퓨팅서비스를 제공하는 자(이하 “클라우드컴퓨팅서비스 제공자”라 한다)의 정보통신자원에 저장하는 정보(「지능정보화 기본법」 제2조제1호에 따른 정보를 말한다)로서 이용자가 소유 또는 관리하는 정보를 말한다.

제23조(신뢰성 향상)

- ① 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스의 품질·성능 및 정보보호 수준을 향상시키기 위하여 노력하여야 한다.
- ② 과학기술정보통신부장관은 클라우드컴퓨팅서비스의 품질·성능에 관한 기준 및 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함한다)을 정하여 고시하고, 클라우드컴퓨팅서비스 제공자에게 그 기준을 지킬 것을 권고할 수 있다. <개정 2017. 7. 26.>

제25조(침해사고 등의 통지 등)

제26조(이용자 보호 등을 위한 정보 공개)

제27조(이용자 정보의 보호)

제29조(손해배상책임)

제35조 벌칙규정

클라우드컴퓨팅서비스 정보보호에 관한 기준

[시행 2017. 8. 24.] [과학기술정보통신부고시 제2017-7호, 2017. 8. 24., 타법개정]

과학기술정보통신부(사이버침해대응과), 044-202-6438

제1조(목적)

제3조(관리적 보호조치)
제4조(물리적 보호조치)
제5조(기술적 보호조치)
제6조(공공기관용 추가 보호조치)
제7조(정보보호 기준의 준수여부 확인)

- 클라우드컴퓨터의 발전 및 이용자 보호에 관한 법률에서는, 과학기술
정보통신부장관은 클라우드컴퓨팅서비스의 품질·성능에 관한 기준
및 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함
한다)을 정하여 고시하도록 규정하고 있으며, 침해사고 통지, 이용자
정보보호 위반시 손해배상 책임과 벌칙을 규정하고 있다.
- 위 법률의 위임에 따라 '클라우드컴퓨팅서비스 정보보호에 관한 기준'
이라는 과학기술정보통신부 고시내용에서 클라우드컴퓨팅서비스제공
자가 지켜야 할 내용을 상세하게 고시하고 있는 바, 클라우드컴퓨터
서비스 제공자는 위 법률 및 고시내용을 모두 준수하여야 하며 정보
보호정책서 작성시에도 위 기준에 적합하게 작성하여야 한다.

다. 법적기준 준수여부

(1) (주)아아티아이즈 정보보호정책서 제5조에서 정보보호 조직의 구성

운영에 관한 사항에 대하여 정보보호 최고책임자, 정보보호 담당자, 정보보호 관리자, 개인정보보호 관리자 및 개인정보보호 담당자로 구성하는 정보보호 실무조직에 관하여 체계적으로 규정하고 있다.

(2) 또한, 같은 정책서 제 5조 제 6항에 따라, 이용자의 정보보호 관련 책임 및 역할에 대하여 이용자와의 계약서 또는 서비스 수준 협약 내용을 반영하여 작성할 것을 규정하고, 제12장 개인정보 처리 안전 관리 규정을 통해 이용자 및 개인정보 보호 관련 규정을 상세히 규정하고 있다.

(3) 정책서 제 6조(내부인력 보안)에서는 클라우드컴퓨팅 서비스제공자가 위 서비스의 안전성 및 신뢰성 확보를 위한 기술적 보호조치에 대하여 비밀유지서약서 부속문서 포함, 서비스 설비, 자원, 자산에 대한 접근 권한 규정 및 이에 대한 관리체계를 명확히 규정함으로써 기술적, 물리적, 관리적 보호조치를 유기적이고 복합적으로 규정하고 있다.

(4) 상기 정책서는 기업정보 및 개인정보보호를 위한 외부인력의 보안

및 내부적 비밀유지 서약을 통한 비밀유지 의무를 부과하는 규정을 두고, 관리적 보호조치와 관련된 정보보호교육 규정을 두어 지속적인 교육 및 관리가 가능하도록 하고 있다.

(5) 위 정보보호정책서에는 또한 관련 법률에서 요구하는 침해사고 대응에 대하여 대응절차 수립, 대응절차 마련, 이용자, 제공자의 책임 및 절차규정, 침해사고에 따른 보고 및 협력체계, 대응체계에 대하여 규정하고 사후관리에 대하여도 상세히 규정함으로써 법률에서 요구하는 기준을 충족하고 있다고 볼 수 있다.

(6) 클라우드서비스의 핵심이라고 할 수 있는 정보보호에 대하여는 별도의 규정을 두어 접근통제(제8장), 네트워크보안(제9장), 데이터보호 및 암호화(제10장) 규정으로 세분화하여 관리함으로써 전문적인 클라우드 서비스 제공자로서의 보안관리에 만전을 기하고 있고, 특히 공공기관의 보안에 요구되는 추가 보안요구사항에 대한 기준도 만족하고 있다(제11장 공공지간보안요구사항).

3. 결론

가. (주)아이티아이즈의 정보보호정책서는 관련 법률 및 동 법 시행규칙에서 요구하는 관리적, 물리적, 기술적 보호조치 및 개인정보보호, 공공기관보안추가요구사항 및 침해시 대응 등에 대하여 상세하고 법적 기준을 충족하여 작성되어 있다.

나. 각 규정이 다소 중복되는 면이 있으나, 이는 관련 규정을 오히려 상세하고 중첩적으로 보호하는 규정으로 선해 해석이 가능한 부분이라고 판단된다.

2021. 2. 3.

법무법인 세안(世按)

담당변호사 이 임 표



본 의견서는 귀사로부터 제출받은 자료를 기초로 귀사의 업무처리와 판단에 도움을 드리기 위한 목적으로 작성되었으므로 다른 용도로 사용할 수 없으며, 제3자에게 이 의견서 또는 그 사본을 제공하고자 하실 때에는 반드시 사전에 본 법무법인의 동의를 받으시기 바랍니다.