개인정보보호위원회, 전문성 개인정보 보호책임자 도입

-대규모 의료기관 개인정보 보호책임자 제도 개선-

2023. 3. 14. 개정되어 2024. 3. 15. 시행 예정인 개인정보 보호법 제31조는 개인정보 보호책임자의 독립성을 보장하고, 개인정보 보호책임자 협의회를 운영하도록 하고 있습니다. 개인정보보호위원회(이하 '개인정보위'라 합니다)는 그 세부내용을 규정하기 위해 동법 시행령 개정을 추진하고 있으며, 특히 개인정보 보호 분야에 전문성과 경험을 갖춘 전문인력이 의료기관의 개인정보에 관한 보호업무를 총괄하여 책임지도록 관련 제도 개선을 본격 추진하고 있습니다.

1. 개정 개인정보 보호법상 개인정보 보호책임자 제도의 주요 변경 사항

개정 개인정보 보호법 제31조는 개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하고, 개인정보 보호책임자를 구성원으로 하는 개인정보 보호책임자 협의회를 설립할 수 있도록 하는 법적 근거를 마련하였습니다.

개인정보 침해 위험이 높아지고 있는 상황에서 조직 내 개인정보 보호책임자 운용의 실효성이 높아지고 있고, 개인정보 보호책임자 제도는 개인정보처리자의 개인정보보호 활동을 촉진하기 위한 자율적 규제 장치로서 도입되었던 것입니다. 그런데 우리나라의 개인정보 보호책임자 제도는 EU GDPR의 개인정보보호 관리자(Data Protection Officer; DPO) 제도와 비교하여 독립성이 부족하다는 비판이 있었습니다. 그리하여 개인정보 보호책임자가 업무를 독립적으로 수행할 수 있도록 보장하는 근거가 이번에 추가로 마련된 것입니다(개정 개인정보 보호법 제31조제6항).

그에 더하여 개정법은 개인정보의 안전한 처리·보호, 정보의 교류 등의 사업을 수행하기 위해 개인정보 보호 수준을 제고하고, 자율보호 문화 확산의 소통창구 역할을 수행하는 별도 기구인 개인정보 보호책임자 협의회를 구성할 수 있도록 하였습니다(개정 개인정보 보호법 제31조제7항). 유사입법례로는 정보통신망의 침해사고에 대한 공동 예방 및 대응, 정보의 교류, 정보보호 강화를 위한 정책 조사 등의 연구를 수행하기 위하여 정보보호 최고책임자(Chief Information Security Officer; CISO)를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있도록 규정한 「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」 제45조제5항이 있습니다.

구법 및 현재 시행되고 있는 개인정보 보호법 제31조 제6항에 따른 시행령은 개인정보 보호 책임자 요건을 공공기관 및 그외 개인정보처리자로 구분하고는 단순히 직위 요건만 규정하고 있어 제도적으로 개인정보 보호 책임자의 전문성을 확보하기가 어려웠습니다. 이에 개정 개인정보 보호법 제31조제9항은 개인정보

본 내용은 일반적인 정보의 제공만을 목적으로 발행되므로 이에 수록된 내용은 저희 법인의 공식적인 견해나 구체적 사안에 관한 법률의견이 아님을 밝혀드립니다.

보호 책임자의 자격요건을 대통령령으로 위임하였고, 개인정보위는 그 세부내용을 규정하기 위해 동법 시행령 개정을 추진하고 있습니다. 개인정보위는 개인정보 보호책임자가 갖춰야 할 학력 및 개인정보 보호 경력(유관경력 포함) 등을 자격요건으로 도입할 계획입니다.

2. 대규모 의료기관에 대한 개인정보 보호책임자 제도개선 사항

개인정보위는 2023. 10. 12. 20여 개의 상급종합병원의 개인정보 보호책임자(CPO, Chief Privacy Officer)들과 함께 '의료기관 개인정보 보호책임자 간담회'를 개최하여 의료분야에서의 개인정보 보호 강화를 위한 다양한 방안을 논의하였습니다.

개인정보위가 이때 밝힌 의료분야 개인정보보호를 위한 협력·지원체계의 방향은 아래와 같습니다.

첫째, 개인정보 보호책임자가 갖춰야 할 학력 및 개인정보 보호 경력 등 자격요건을 도입하고, 독립성 보장 방안 마련을 추진할 계획입니다.

둘째, 개인정보 보호 전문성을 갖춘 의료인 개인정보 보호책임자가 양성될 수 있도록 의료분야의 특수성을 고려한 경력인정 체계 도입을 검토하고, 그에 따른 맞춤형 교육과 컨설팅을 제공하는 등 다양한 방식으로 지원할 예정입니다.

셋째, 대한병원협회와 같은 의료분야의 자율규제단체를 통해 연말까지 자율점검을 적극적으로 추진하며, 우수기관에 대한 과태료 및 과징금 감면 등의 인센티브를 제공하여, 의료기관의 개인정보 보호 자율규제 활동을 적극 지원할 예정입니다.

그 외에 개인정보 보호법 개정 이후 과징금 상한액 기준이 '전체 매출액'으로 변경됨에 따라 개인정보 침해사고 발생 시 처벌 규정이 강화되었다는 점도 잊지 말 것을 강조하였습니다.

3. 시사점

과거에도 의료기관을 포함한 개인정보처리자는 개인정보 보호책임자를 지정하였지만, 법률과 시행령은 개인정보 보호책임자의 요건을 대표자 또는 임원 등으로 단순 직위 요건만 정하였고, 그 결과 개인정보 분야에 대한 경험과 이해가 부족한 행정인력이 개인정보 보호책임자를 겸임하는 등 전문성 확보에 한계가 있어 왔습니다. 하지만 개정법 시행을 앞두고 개인정보위는 45개의 대규모 의료기관을 포함하여 전문 CPO 제도를 도입하려 하는 것입니다.

이에 의료기관을 포함한 개인정보처리자는 전문 CPO제도에 맞게끔 전문성을 확보한 개인정보 보호책임자를 지정하고 그에 따른 실질적인 개인정보 보호체계를 운영할 수 있어야 합니다.

화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 제공하고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다

본 내용은 일반적인 정보의 제공만을 목적으로 발행되므로 이에 수록된 내용은 저희 법인의 공식적인 견해나 구체적 사안에 관한 법률의견이 아님을 밝혀드립니다.

Contacts

이광욱
파트너변호사
T. (+82) 2 6003 7535
E. kwlee@yoonyang.com

이근우
파트너변호사
T. (+82) 2 6003 7558
E. klee@yoonyang.com

이수경
파트너변호사
T. (+82) 2 6182 8132
E. sgyi@yoonyang.com

유현상
변호사
T. (+82) 2 6182 8716
E. hsryu@yoonyang.com

백재환
전문위원
T. (+82) 2 6182 8366
E. jhb@yoonyang.com

지재원
연구위원
T. (+82) 2 6003 7568
E. jwji@yoonyang.com