WISENET

White paper

영상감시 시스템을 위한 GDPR 백서

2018. 5. 8.

Hanwha Techwin

Contents

면책 조항 (Disclaimer Clause)

한화테크윈 주식회사는 본 GDPR 백서를 통해 GDPR 관련 당사의 최신 정보를 전달하기 위해 노력하고 있습니다. 그러나 한화테크윈 주식회사는 본 백서 내 기술된 정보의 정확성 또는 사업 적합성 등에 대해서는 일체의 보증을 하지 않습니다. 정확한 법령 상 권리 및 의무사항의 확인 및 대응을 위해서는 전문 자문 기관 또는 변호사 등의 상담을 받으셔야 하는 점을 유의하시기 바랍니다. 그러한 상담 없이 본 백서에 기술된 내용만을 믿고 적용한 결과에 대해 한화테크윈 주식회사는 어떠한 책임도 부담하지 않습니다.

현재 CCTV 업계는 사회 안전 및 보안 강화와 같은 긍정적인 측면에도 불구하고 운영의 신뢰성이 결여된 감시의 확산 및 개인 프라이버시의 침해 우려와 같은 부정적인 이미지가 사회 전반에 자리잡고 있습니다. 특히, 사물인터넷(IoT), 클라우드, 빅데이터, 인공지능(AI)과 같은 새로운 기술이 IP 기반 CCTV 시스템에 적용되고 융합되면서 새로운 가능성이 창출되는 만큼, 네트워크 CCTV 시스템으로 인한 네트워크 보안 취약점(예를 들면, 무허가 접근 및 개인정보 취득)에 대한 위험성 및 그로 인한 법적 리스크도 고조되고 있는 현실입니다.

이러한 상황에 대응하기 위해 유럽연합(EU)은 EU내 디지털 경제의 활성화를 위해 EU 회원국간 개인정보의 자유로운 이동을 보장하는 한편 정보주체(사람)의 개인정보 보호 권리를 강화하기 위해 GDPR(General Data Protection Regulation)이 2016. 5. 25 발효되었으며, 2018. 5. 25부터 전격 시행됩니다.

GDPR은 개인 정보주체의 권리를 크게 강화하고 개인정보의 컨트롤러 및 프로세서에 대한 의무 및 책임성을 강화하고 있습니다. 그러한 점에서, CCTV 시스템의 관리자나 서비스 제공자는 자신이 관리하거나 고객에게 서비스를 제공하는 네트워크 CCTV 시스템과 관련하여 발생할 수 있는 개인정보 보안 취약점에 대한 법적 책임이 있음을 유념해야 합니다.

따라서, 신규 CCTV 시스템의 설치나 기존 시스템 업그레이드를 하고자 할 때는 물론 개인정보 영향평가를 수행하지 않았던 기존 CCTV 시스템에 대해서도, 개인정보의 처리 이전에 개인정보 영향평가를 수행하여 프라이버시 및 개인정보 보호를 위한 보안 리스크의 파악 및 안전 조치를 마련해야 할 것입니다. 예를 들면, 초기 설정 비밀번호와 같은 심각한 보안 이슈의 해결, 기술과 장비에 대한 주기적인 취약점 분석, 수용가능한 표준(중대 버그 수정 및 소프트웨어 업데이트) 유지, 최선의 행동 강령의 인식, 임직원에 대한 컴플라이언스 및 침해 사실 위반 통지 교육이 수행되어야 합니다.

또한, 클라우드 기반 CCTV 영상 저장 또는 분석 서비스를 제3자에게 위탁하는 경우, 정보처리의 위탁에 따른 프로세서에 대한 관리 의무가 강화되며 위반 시의 법적 책임도 함께 증가하였습니다.

하지만 유럽의 GDPR의 제정 배경을 보면 강화된 규제에 대한 소극적, 형식적인 준수(compliance)보다는 개인정보 영향평가 또는 Privacy by design/default과 같은 주도적, 선제적인 책임성(accountability) 강화를 권장하는데 초점을 맞추고 있습니다. 즉, 컨트롤러나 프로세서의 GDPR 컴플라이언스를 위한 혁신적 노력에 대한 보상을 제공함과 동시에 행동 강령 시행 및 인증 획득과 같은 적절한 매커니즘의 채택함으로써 자연스럽게 GDPR 컴플라이언스 프로세스에 대한 인식 개선이 이뤄지도록 권장하고 있습니다.

CCTV 시스템 사용자나 서비스 제공자가 주도, 선제적인 책임성을 갖고 적절한 기술적, 조직적 조치를 수행하여 GDPR 컴플라이언스라는 목적을 달성한다면, CCTV 영상 감시에 대한 신뢰성과 투명성 회복으로 인한 CCTV 산업의 활성화, 더 나아가 빅데이터 활용과 같은 디지털 경제의 활성화에 촉매제 역할을 할 것으로 전망됩니다. 또한, 유럽 개인의 정보를 처리하는 기업이라면 기업의 EU내 소재 여부를 불문하고 적용이 되고 막대한 과징금으로 인하여 GDPR의 준수를 사실상 강제하고 있으므로 GDPR은 유럽 이외의 국가들에도 상당한 영향을 미칠 것으로 예상됩니다.

GDPR은 회원국에 대한 입법지침 가이드라인 역할을 했던 기존의 지침과는 달리 EU의 모든 회원국들에게 직접적인 법적 구속력을 가집니다. EU 거주민에게 재화나 용역을 제공하거나 EU 거주민의 개인정보를 처리하는 EU에 소재하지 않은 외국의 기관에도 적용되며, GDPR의 중대 위반시 전세계 연 매출액의 4% 또는 2천만 유로 중 높은 금액까지 과징금이 부과될 수 있으며, 이와 별도로 집단소송 및 개인 민사소송도 가능하므로 EU에 진출하였거나 진출을 희망하는 기업들의 각별한 주의가 필요합니다.

GDPR에서는 이름, 전화번호 등과 같은 일반적 개인정보 외에 IP 주소, 쿠키와 같은 온라인 식별자와 위치 정보, 그리고 유전 정보와 바이오 정보 등의 생체 정보도 모두 개인정보의 범위에 폭넓게 포함시키고 있습니다. 특히, CCTV 시스템을 이용한 공공장소에서 대규모의 체계적인 모니터링은 개인 프라이버시 침해의 고위험을 초래할 가능성이 있는 개인정보 처리로 분류하고 있습니다.

이하에서는 CCTV 시스템(감시카메라, 저장장치 및 관제 소프트웨어)을 이용한 모니터링 및 개인정보를 처리하는 컨트롤러 및 프로세서(CCTV 관제 위탁 기관 및 수행 기관)가 꼭 유념해야 할 내용들에 대해 소개합니다.

2.1. GDPR의 주요 내용

2.1.1. 개인정보 처리원칙

적법성, 공정성, 투명성의 원칙

개인정보는 정보주체와 관련하여 적법하고, 공정하며 투명한 방식으로 처리되어야 합니다.

목적 제한의 원칙

구체적이고 명시적이며 적법한 목적으로만 개인정보를 수집해야 하며, 해당 목적과 부합하지 않는 방식으로 추가 처리를 할 수 없습니다.

최소화의 원칙

개인정보의 처리는 적절하며 관련성이 있고, 그 처리 목적을 위해 필요한 범위로 한정되어야 합니다.

보관기간 제한의 원칙

처리 목적을 위해 필요한 기간이 경과한 후에는 삭제하거나 정보주체를 식별할 수 없는 형태로 보관해야 합니다.

무결성 및 기밀성의 원칙

개인정보는 적절한 기술적, 조직적 조치를 통해 권한 없는 처리, 불법적 처리 및 우발적 멸실, 파괴 또는 손상에 대비한 보호 등 적절한 보안을 보장하는 방식으로 처리되어야 합니다.

정확성의 원칙

개인정보의 처리는 정확해야 하며, 최신으로 유지하기 위한 합리적 조치가 취해져야 합니다. 마지막으로 컨트롤러는 앞서 소개한 6가지 원칙을 준수할 책임을 지며 이를 입증할 수 있어야 합니다.

2.1.2. 정보주체의 권리보장

GDPR에서는 기존 지침에는 없던 삭제권('잊힐 권리'), 개인정보 이동권, 자동화된 결정(프로파일링)이 새로 도입되어 기존보다 정보주체의 권리를 강화하고 있습니다.

정보를 제공받을 권리

컨트롤러는 간결하고 명료하게 이해하기 쉬운 형태로 정보주체에게 개인정보 처리와 관련된 정보를 알려야 합니다.

열람권

정보주체는 (1) 본인의 정보가 처리되고 있다는 사실의 확인, (2) 본인의 개인정보에 대한 접근 등을 요구할 수 있습니다.

정정권

정보주체는 개인정보가 부정확하거나 불완전하다면 정정을 요구할 수 있습니다.

잊힐 권리

정보주체는 본인에 관한 개인정보의 삭제를 컨트롤러에게 요구할 수 있습니다.

처리 제한권

정보주체는 자신에 관한 개인정보의 처리를 차단하거나 제한할 수 있습니다.

개인정보 이동권

정보주체는 개인정보를 다른 서비스에 걸쳐 재사용할 수 있도록 개인정보의 이동을 요구할 수 있습니다.

반대권

정보주체는 본인의 특정 상황을 근거로 프로파일링 등 본인과 관련한 개인정보의 처리에 대해 언제든지 반대할 수 있습니다.

자동화된 결정 및 프로파일링 관련 권리

정보주체는 법적 효력을 초래하거나 이와 유사하게 본인에게 중대한 영향을 미치는 사항에 대하여 프로파일링 등 자동화된 처리에만 근거한 결정의 적용을 받지 않을 권리가 있습니다.

2.1.3. 컨트롤러 및 프로세서의 책임성 강화

컨트롤러는 개인정보의 처리 목적 및 수단을 결정하는 자연인, 법인, 공공기관, 또는 에이전시로서, 개인정보 처리의 성격, 범위, 목적, 위험성 등을 고려하여 개인정보의 처리가 GDPR을 준수하여 수행되는 것을 보장하고, 이를 입증할 수 있는 적절한 기술적, 조직적 조치를 이행할 의무가 있습니다.

프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 자연인, 법인, 공공기관, 또는 에이전시로서, 컨트롤러의 지시에 의건하여 개인정보를 처리해야 합니다.

처리활동의 기록

컨트롤러와 프로세서는 GDPR 준수를 입증하기 위하여 본인의 책임하에 개인정보 처리활동의 기록을 문서로 유지해야 합니다. 종업원이 250명 미만인 기업에는 처리활동의 기록 의무가 적용되지 않으나, 개인정보 처리가 (1) 정보주체의 권리와 자유에 위험을 초래할 가능성이 있거나, (2) 민감 정보 처리 등에 관한 경우 종업원 수에 무관하게 기록 의무가 있습니다.

따라서, CCTV 시스템을 활용한 공공 장소에서 대규모의 체계적인 모니터링을 하는 경우는 개인정보영향평가를 수행하고, 그 결과 정보주체의 권리와 자유에 위험을 초래할 가능성이 있다고 평가될 경우 종업원 수와 무관하게 기록을 남길 필요가 있겠습니다.

설계단계부터 프라이버시 보호의 고려

컨트롤러는 IT 시스템 및 프로세스의 설계 및 개발 과정에서 개인정보 보호를 검토하고 이를 개인정보 처리활동에 반영하였음을 입증하기 위하여 적절한 기술적, 조직적 조치를 반영해야 합니다. (Data protection by default)

적절한 기술적, 조직적 조치로는 가능한 빠른 시점의 개인정보 가명화, 비식별화, 개인정보 처리의 최소화 등이 있으며, GDPR 준수를 위해 개인정보 처리 과정 내의 필수적 보안조치도 적용되어야 합니다.

또한, 컨트롤러는 개인정보가 처리되는 제품, 서비스, 어플리케이션의 기본 설정이 프라이버시 친화적인지 검토하고 보완하여야 합니다. (Data protection by default) 특히, 대중교통시스템에서 사용되는 영상감시 카메라는 이러한 검토가 필요한 주요 어플리케이션 영역의 하나입니다. 그리고 예를 들면 (1) 수집되는 개인정보의 양, (2) 개인정보 처리의 범위, (3) 보유기간, (4) 접근 가능성(기본 설정이 개인정보 처리 시, 목적에 해당하는 특정 개인정보만 처리되는 것)을 보장하기 위해 적절한 기술적, 조직적 조치를 이행해야 합니다.

개인정보 영향평가(DPIA)

개인의 자유와 권리를 침해할 높은 위험이 있는 경우, 예를 들면 공개적으로 접근 가능한 장소에 대한 대규모의 체계적인 모니터링을 수행하는 CCTV 시스템에 대해서는 개인정보 영향평가를 사전에 수행하도록 명시하고 있습니다. 특히, CCTV 시스템의 경우 누가 자신의 정보를 수집하는지, 그 정보가 어떻게 이용될지를 모를 수 있는 상황에서 개인정보가 수집되고, 또한 개인이 공공 이용 장소에서 그런 처리의 대상이 되는 것을 피하기 어렵기 때문입니다.

개인정보 영향평가는 프라이버시 침해 및 개인정보 보호 위반 소지가 있는 리스크를 사전에 파악하고 이를 최소화하기 위한 목적이며, 개인정보 “처리가 이루어지기 전”에 수행되어야 합니다.

개인정보 영향평가는 (1) 예정 처리작업 및 처리목적, (2) 개인정보 처리의 필요성 및 형평성의 원칙에 대한 평가, (3) 정보주체의 권리 및 자유에 대한 위험평가, (4) 위험을 완화하기 위한 안전 조치를 포함하게 되어 있습니다. 개인정보 영향평가는 영향을 받는 정보주체나 그 대표자의 의견도 포함시켜야 하는데, CCTV 시스템의 경우 모니터링 대상인 종업원 또는 일반 공중이 그 대상이 될 수 있습니다.

개인정보보호관(DPO: Data Protection Officer)의 임명

공공 기관, 또는 핵심활동이 정보주체에 대한 대규모의 정기적이고 체계적인 모니터링을 요구하는 기관의 경우에는 DPO를 반드시 지정해야 합니다.

EU 29조 작업반의 지침에 따르면, 예를 들면 쇼핑 센터를 감시하는 보안회사와 같이, 공공 장소에서 CCTV 감시 서비스(SaaS)를 제공하는 회사도 이에 해당합니다. 반면, 자사 건물 내 또는 주변을 감시하는 목적으로 CCTV 시스템을 사용하는 민간 회사는 이에 해당하지 않을 수 있습니다. 이와 같이 DPO 지정 요건에 해당하지 않는 것으로 판단하여 지정하지 않는 경우, 관련 사항을 문서화하여야 합니다.

DPO는 DPIA를 수행할지 여부의 결정, 수행 방법론, 수행 주체(내부 또는 아웃소싱), 위험 완화를 위한 안전 조치, 사후 평가에 대한 조언을 제시하도록 권고됩니다.

DPO는 자신의 책무를 수행하는데 컨트롤러나 프로세서로부터 어떠한 지시를 받지 않도록 독립성이 보장되어야 하며, DPIA에 대한 최종 책임은 컨트롤러에게 있습니다.

프로세서 및 하청 프로세서에 대한 책임

컨트롤러는 GDPR 준수, 적절한 기술적 · 관리적 보호조치 보증이 제공되는 것을 조건으로 자신을 대신하여 프로세서에게 개인정보를 처리하게 할 수 있습니다. 컨트롤러는 프로세서의 행위로 인한 책임을 지게 되며, 프로세서 역시 정보주체의 권리 요청에 대응할 의무와 책임을 집니다. 따라서 컨트롤러는 프로세서와의 개인정보 처리업무 위탁 계약서에 프로세서가 처리할 범위 및 그에 따른 책임 관계를 명시하는 것이 필수적으로 요구됩니다.

프로세서가 개인정보의 처리 업무를 하청 주는 경우 컨트롤러로부터 사전 서면 동의를 받아야 하며, 컨트롤러와의 계약 의무 사항을 하청 계약서에 동일하게 포함시켜야 합니다. 그럼으로써 컨트롤러는 하청 프로세서의 행위로 인한 책임을 지게 됩니다.

CCTV 감시 서비스를 위탁하거나 하도급 주는 기관은 이러한 점을 유념해야 합니다. 또한, CCTV 감시 영상에 대한 클라우드 기반의 처리를 수행하는 프로세서를 고용하고자 하는 기관은 상기한 컨트롤러로서의 책임을 유념해야 합니다.

적절한 보안을 보장하는 사이버 보안 조치

컨트롤러는 무결성 및 기밀성의 원칙, 즉 적절한 기술적, 조직적 조치를 통하여 비인가/불법적 처리, 우발적 멸실/파괴나 손상에 대비한 적절한 보안 조치를 보장하여야 하는 원칙을 준수할 책임 및 입증할 책임이 있습니다.

또한, Data protection by design에 의해 IT 시스템의 설계 및 개발 과정에서부터 GDPR 준수를 위한 개인정보 처리 과정 내의 필수적 보안 조치를 적용해야 하며, 개인정보가 처리되는 제품, 서비스, 어플리케이션의 기본 설정이 특정한 개인정보의 처리 목적에 필요한 최소한의 범위 내에서 개인정보가 처리(접근, 전송, 저장, 반출, 이용, 파기 등)되는 것을 보장하기 위해 기술적, 조직적 (Data protection by default) 조치를 이행해야 합니다.

특히, CCTV 시스템도 IP 기반의 네트워크 카메라, 네트워크 저장장치 및 VMS로 구성되는 경우가 증가하면서 해커나 악의적 내부자로 인한 개인정보 유출, 위변조, 멸실, 오남용이 발생하고, 이는 곧 프라이버시의 침해 및 개인정보 보호 위반으로 이어지게 됩니다. 따라서, 컨트롤러는 GDPR 준수를 위해서는 네트워크 보안이 강화되고 내부 사용자 통제 및 오남용 방지가 가능한 CCTV 시스템으로 구축하거나 업그레이드할 필요가 있습니다.

개인정보 침해 발생시 조치

개인정보의 침해 발생시 프로세서는 이를 인지한 때로부터 컨트롤러에게 지체 없이 알려야 하며, 컨트롤러는 이를 인지한 때로부터 지체 없이 그리고 72시간 내에 감독기구에게 알려야 합니다. 또한, (1) 개인정보가 암호화 등에 의해 적절히 보호되고 있거나, (2) 침해로 인한 정보주체의 권리에 큰 영향이 없거나, (3) 정보주체에게 통지하는 것이 과도한 노력을 수반하는 상황에 해당하지 않는 한, 컨트롤러는 정보주체에게도 지체 없이 통지해야 합니다.

2.2. GDPR 위반시 제재 및 파급 효과

개인정보 처리 원칙, 수집시 동의 요건, 정보주체의 권리 보장, 국외 이전 제한 등에 대한 중대한 위반의 경우, 전세계 연간 매출액의 최대 4% 또는 최대 2천만 유로 중 더 높은 금액의 과징금이 부과됩니다. 그 외의 일반적 위반의 경우, 예를 들면 통지의무 위반시 전세계 매출액의 최대 2% 또는 최대 1천만 유로 중 더 높은 금액의 과징금이 부과됩니다.

만약 이러한 과징금이 부과되지 않는 침해에 대해서는 형사 처벌과 같은 다른 제재를 가하도록 규정하고 있으며, 이와 별도로 침해를 입은 개인 정보주체는 민사적인 손해배상도 청구할 수 있습니다. 이러한 이유로, GDPR을 준수하지 못한 기업은 브랜드 평판 추락, 더 나아가 비즈니스 생존이 위태로울 수 있으며, 개인의 입장에서는 일자리 감소에 영향을 미칠 수도 있을 것입니다.

GDPR은 유럽에 이미 진출한 기업뿐만 아니라 진출 예정인 기업은 반드시 숙지하고 철저한 대비를 해야 합니다. 뿐만 아니라, GDPR이 개인정보 보호의 글로벌 표준으로 자리매김할 가능성이 크기 때문에 글로벌 시장에서 비즈니스를 하고자 하는 기업에게는 장기적으로는 관심을 기울일 필요가 있습니다.

한편, 개인정보 보호 및 프라이버시가 필요한 공공용 CCTV, 영상 클라우드 서비스는 고위험군에 속해 위반 시에 많은 과징금이 부과될 가능성이 있다는 점에 유의해서 유럽 내에서 또는 유럽 외에서 유럽 거주민에 대한 영상 감시 서비스를 하는 컨트롤러 또는 프로세서는 철저한 준비를 하여야 할 것입니다.

3.1. 개인정보 처리원칙 및 Privacy by Design and Default

3.1.1. 보관기간 제한 및 파기 안전성

보관기간 제한의 원칙에 따라 보관기간이 경과한 개인이 촬영된 영상은 삭제하거나 사람의 신원이 확인되지 않도록 비식별화 처리를 하여야 합니다.

이를 위해서는 (1) 영상이 무기한 보관되지 않도록 법률 또는 개인정보 수집 동의서에 정해진 보관기간을 영상의 보관기한으로 반드시 설정하도록 의무화하고, (2) 설정된 보관기한이 경과하면 영상이 자동 삭제되는 기능을 제공하는 것이 바람직합니다. 또한, (3) 설정한 보관기간, 삭제된 영상파일명, 삭제 일시, 및 보관기간 설정자를 기록하고 관리함으로써 개인정보 처리의 투명성을 보장할 수 있을 것입니다.

개인정보 처리의 적법성 및 투명성을 보장하기 위해서 설정된 보관기간을 변경하거나 설정 해제하는 권한은 관리자에게만 부여하고, 보관기간 관련 처리 이력, 예를 들면 변경된 보관기간, 변경이나 설정 해제 일시 및 주체에 대해 기록하고 관리하는 것이 바람직합니다.

한화테크윈은 관련 법 내지 가이드라인에 규정된 보관기간을 초과해 영상이 수집, 보관되지 않도록 제품 내 관련 기능을 제공합니다. 예를 들어, 네트워크 비디오 저장장치의 경우 녹화일 수(1~400일)를 기준으로 영상정보의 보관기간을 설정할 수 있으며, 설정된 보관기간 이후의 영상정보는 순차적으로 자동삭제가 진행됩니다.

3.1.2. 음성녹음 제한

개인정보 처리의 최소화 원칙에 따라 일반적으로 영상감시 시스템을 이용해 음성 녹음을 해서는 안 됩니다. 특히, 개인간의 대화는 프라이버시 침해 우려가 크므로 음성 녹음이 허용되지 않습니다. 하지만, 공공 안전 등의 사유로 음성 정보 기록이 허용된 영상감시 시스템에서는 영상 저장뿐 아니라 음성 녹음이 필요합니다.

따라서, 음성 녹음 기능의 초기 설정은 비활성화로 하되, 영상 녹화와는 별개로 사용 여부를 제어할 수 있어야 하고, 예외적으로 음성 녹음이 필요한 경우, 기능 활성화 권한은 인증된 관리자에게만 부여하는 것이 바람직합니다.

아울러 녹음의 정당성이 인정되는 경우에만 설정을 변경 가능하게 하고 녹음 가능 여부에 대한 경고 문구와 함께 설정 변경 이력, 변경 일시 및 변경 주체에 대해 기록하고 관리하는 것이 바람직합니다.

한화테크윈의 제품은 Privacy by default에 의거하여 기본적으로 음성 녹음 기능이 비활성화되어 있습니다. 하지만, 오디오 정보는 CCTV 시스템에 있어 사용자에게 유용한 정보를 제공해 줄 수 있는 중요한 정보원임을 간과할 수 없기 때문에 오디오 검출(Audio Detection), 음원 분류(Sound Classification), 오디오 잔향 제거(Audio Echo Cancelation), 오디오 잡음 감쇄(Audio Noise Reduction) 등의 기능을 기본적으로 제공합니다.

이 중 오디오 검출과 음원 분류 기능은 음성 녹음을 하지 않고 카메라에서 자체 처리하여 제공되며, 향후 멀티채널 마이크 기반 음원 위치 추적 등 지능화된 오디오 분석 기술 개발을 통해 고객의 다양한 요구에 대응할 예정입니다. 물론, 이 경우에도 오디오 분석 목적 외 음성 녹음은 제한되며 개인 정보 처리의 최소화 원칙은 항상 유지됩니다.

3.1.3. PTZ 목적외 촬영 제한

개인정보 처리의 최소화 원칙에 따라 CCTV 영상감시 애플리케이션에서 영상의 촬영 및 수집에 관한 처리는 CCTV 영상감시 목적에 적절하고 관련성이 있으며 필요한 경우로 한정되어야 합니다.

영상감시 장비 중 PTZ 카메라는 고정 카메라와 달리 상하좌우 전방위 촬영이 가능할 뿐만 아니라 고배율 확대까지 가능하므로 경우에 따라 프라이버시 침해 소지가 있습니다. 따라서, 카메라의 설치 목적 및 프라이버시 침해 가능성을 고려하여 촬영 목적에 따른 패닝(좌우 회전) 및 틸팅(상하 회전) 가능 범위를 제한하는 기능을 제공할 필요가 있습니다.

PTZ 카메라에 의한 영상의 수집 및 저장과 같은 처리의 투명성 및 적법성을 보장하기 위하여, PTZ 카메라를 설치할 때 패닝 및 틸팅 허용 범위를 인증된 관리자로 하여금 설정하는 것을 권장합니다. 또한, 이미 설정되어 있는 패닝 및 틸팅 범위를 변경하거나 설정 해제하는 권한은 인증된 관리자에게만 부여하는 한편 설정 변경/해제 이력, 변경/해제 일시 및 변경 주체에 대해 기록하고 관리하는 것이 바람직합니다. 이와 함께, 인가된 관리자에 의해 설정된 패닝 및

틸팅 범위를 벗어나면 촬영이 되지 않도록 하거나 촬영 영상이 마스킹 처리되도록 하는 것도 고려해야 할 것입니다.

한화테크윈의 세계 최고 성능 PTZ 카메라에도 다른 자사 제품과 마찬가지로 개인정보 처리 최소화 원칙이 적용되어 있습니다. 한화테크윈의 PTZ 카메라는 최대 24개의 Privacy Mask를 설정할 수 있는 기능을 제공하며 패닝, 틸팅 및 줌 동작에 따라 Privacy Mask가 연동되어 높은 정확도로 유지되게 함으로써 영상감시 목적에 부합되지 않은 영상수집을 근본적으로 방지합니다. 아울러 패닝 및 틸팅 시 사용자가 설정해 놓은 영역 내에서만 이동이 가능하도록 PT Limit 기능을 기본으로 제공하며 이는 허가되지 않은 범위의 영상 촬영을 손쉽게 제한합니다.

3.1.4. 비식별화

CCTV 영상 내의 객체(사람 또는 자동차 번호판)에 대한 비식별화 처리(마스킹, 블러링, 모자이크 등)의 필요성은 영상의 수집 목적 및 처리 환경에 따라 달라집니다.

GDPR에서는 공익, 과학적, 역사적 연구 또는 통계의 목적으로 저장하는 경우로서 비식별화된 영상을 처리하여도 해당 목적을 달성할 수 있는 경우나, 수집된 원래 목적 외의 다른 목적으로 정보주체의 동의 없이 수행되는 경우에는 비식별화 처리를 수행할 것을 규정하고 있습니다.

한편, 후술할 열람권의 요청이 적법한 경우(예: 긴급 상황 또는 수사/사법기관 허락 등)로서 열람을 위한 영상의 제공시 영상내에 포함된 제3자의 프라이버시 보호가 침해된다고 판단되는 경우, 영상내 제3자의 비식별화가 필요할 수도 있습니다.

개인정보 처리의 최소화 및 프라이버시 보호를 극대화하기 위하여, 접근 권한에 따라, 예를 들면 관리자(Admin 계정)와는 달리 CCTV 관제요원(guest/user 계정)에게는 실시간 모니터링이나 녹화 영상 검색시 비식별화 처리된 영상을 제공하는 방안도 고려할 필요가 있습니다. 그럼으로써 (1) GDPR 개인정보 처리원칙을 적용받지 않게 되고, (2) 정보주체의 권리행사에 대한 리스크가 저감되고, (3) 최대한 빨리 비식별화를 함으로써 정보보호 의무의 준수 용이 및 입증에 도움이 되는 이점이 있습니다.

GDPR은 설계단계부터 프라이버시 보호의 고려(Privacy by design and by default)를 위해 가명화 또는 비식별화 조치와 같은 적절한 기술적 및 조직적 조치를 요구하고 있습니다. 또한, 개인정보 처리의 보안 수준을 보장하기 위한 기술적 및 조직적 조치를 요구합니다. 다만, 컨트롤러는 최신 기술, 실행 비용, 개인정보 처리의 성격과 범위, 상황, 목적, 개인정보 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성, 중대성 및 위험성을 고려하여 적절한 기술적, 조직적 조치를 이행하면 됩니다.

CCTV 영상감시 애플리케이션의 경우, 모든 프레임의 영상에 등장하는 개인을 구별하여 정확하게 비식별화하는데 상당한 기술적, 성능적, 비용적 어려움이 존재함을 고려할 때, 실제 CCTV시스템이 설치, 운용되는 목적이 상기한 비식별화 처리가 반드시 필요한 경우인지를 먼저 판단해 보고, 이에 해당하지 않는다면 비식별화 처리에 따른 이점 및 그에 수반되는 비용 간의 실익을 고려하여 비식별화 처리의 필요성을 결정하는 것이 바람직하겠습니다.

한화테크윈은 정보주체의 프라이버시 보호와 CCTV 영상을 통한 안전 및 보안 간의 균형을 도모하기 위하여, 파트너사와 함께 모니터링시 실시간 마스킹된 영상을 스트리밍하는 제품과 열람 제공을 위한 백업시 원하는 사람이나 구역을 마스킹할 수 있는 제품을 공급할 예정입니다.

3.2. 정보주체의 권리 보장

3.2.1. 열람권

백화점에 설치된 CCTV 카메라에 거부감을 느낀 고객이 귀가 후 백화점 홈페이지 고객센터를 통해 CCTV 영상 촬영이나 처리가 적법하게 이루어지고 있는지를 질의하면서 자신이 촬영되었는지 여부를 확인해 달라고 요청할 수 있습니다. 이에 대해 컨트롤러는 처리의 목적, 관련된 개인정보의 종류 등에 대해 전자적 형태로 제공할 수 있어야 합니다.

이를 위해서 컨트롤러는 정보 요청자에게 요청할 권한이 있는 정보주체인지 확인할 수 있는 정보를 제공하도록 요구하고, 해당 영상 정보를 찾기 위한 촬영 일시, 장소 등의 상세 정보를 제공하도록 요구할 수 있습니다.

열람권의 보장을 용이하게 달성하기 위해서는, (1) 저장장치(NVR/DVR 또는 VMS)의 사용자는 권한 인증을 거친 후 저장 영상에 접근하여야 할 것이며, (2) 신속 정확하게 해당 영상을 검색할 수 있는 사용자 인터페이스 및 스마트 검색 기능이 제공되어야 할 것이며, (3) 사용자는 화면에 표시된 검색 영상을 확인하여 그대로 제공을 해도 될 것인지 아니면 요청 정보주체를 제외한 제3자를 비식별화(마스킹, 블러링, 모자이크 등)해야 할 것인지를 판단하게 될 것입니다.

만약, 해당 영상에 요청 정보주체만 있다면 해당 영상을 그대로 제공해도 될 것이지만, 이와 달리 제3자가 존재한다면 영상을 그대로 제공하였을 때 제3자의 프라이버시에 대한 침해가 우려되는지 여부를 먼저 판단한 후 필요시 비식별화 조치가 필요할 것입니다.

또한, 개인정보의 처리가 적법하게 이루어지고 있다는 사실을 확인하는데 필요한 정보로서, 개인정보(촬영 영상)를 제공받았거나 제공받을 수령인, 및 보유 기간이 포함되어 있습니다. 따라서, 이러한 요구에 용이하게 대응하기 위해서는 (1) 저장장치는 영상에 접근 가능한 모든 사용자 목록, 각 영상에 대한 처리 이력, 예를 들면 각 영상의 복사, 반출 사실 및 해당 행위의 사용자, 발생 일시 등에 대한 로그, 및 영상의 보유 기간에 대한 정보를 생성하여 보관하여야 하며, (2) 권한 있는 사용자가 이를 용이하게 검색하고 전자 파일로 생성할 수 있는 사용자 인터페이스를 제공하는 것이 바람직합니다.

이러한 요청이 접수되고 영상 정보를 제공하는데 상당한 시일이 소요되는 경우에는 해당 영상 정보가 보관기간의 경과시 자동 삭제가 되지 않도록 조치하는 것이 바람직합니다.

3.2.2. 잊혀질 권리(삭제권)

CCTV 영상감시 애플리케이션 분야에서 열람권과 삭제권은 개인에 대한 영상을 검색해야 한다는 점에서는 유사하나, 열람권에 응하더라도 CCTV 영상의 원본이 그대로 남는 반면, 삭제권의 경우 CCTV 영상의 원본이 파기된다는 점에서 차이가 있습니다. 또한, 삭제권의 경우 CCTV 영상이 누군가에 의해 인터넷 등 외부로 유출되어 사생활 침해가 이미 발생한 경우에 통상 제기될 것이라는 점이 특징입니다.

잊혀질 권리에 대해 하나의 상황을 예로 들어 설명해보면 다음과 같습니다. 어느 고급빌라에 거주중인 유명인 A가 다른 유명인 B와 함께 출입하는 모습이 주차장에 설치된 CCTV 카메라를 통해 녹화되었고, 이 영상이 유출된 상황을 가정해보겠습니다. 이 경우, 사생활 침해를 이유로 A는 CCTV 관리자에게 자신이 촬영된 영상의 삭제를 요청할 수 있으며, 컨트롤러인 CCTV 관리자는 삭제 요구를 거부할 수 있는 5가지 경우*에 해당하지 않는 이상 A의 요청에 응해야 합니다.

· **삭제 요구를 거부할 수 있는 5가지 경우**

① 표현 및 정보(information)의 자유에 관한 권리 행사를 위한 경우
② 공익적 임무의 수행 및 직무권한 행사를 위한 법적 의무 이행을 위한 것인 경우
③ 공익을 위한 보건 목적을 위한 경우
④ 공익적 기론 보존(archiving purpose), 과학 및 역사적 연구 또는 통계 목적을 위한 것인 경우
⑤ 법적 청구권의 행사나 방어를 위한 것인 경우

다만, CCTV 영상이 적법한 목적(예, 범죄 예방 및 수사)에 따라 수집되고 적법한 절차에 따라 처리되는 경우 해당 목적의 달성을 위해 영상을 일정기간 보관할 것이 요구되는 바, CCTV 영상이 유출되지 않은 상태에서의 삭제 요청에 대해서는 삭제를 요구하는 정보주체의 이익(interest), 권리(rights) 및 자유(freedom)에 비해 처리(보관)을 계속할 적법한 이익(legitimate interest)이 중대한지의 여부에 따라 결론이 달라질 수 있습니다. 특히, 기술적 제약으로 인하여 함께 저장된 다른 시간대의 CCTV 영상이 삭제됨으로써 공익적 목적을 달성할 수 없게 되는 경우도 발생할 수 있다는 점이 고려될 필요가 있습니다.

그럼에도 불구하고 삭제권의 요구가 적법하고 필요하다고 판단된 경우, 삭제권의 보장을 용이하게 달성하기 위해서는 (1) 저장장치(NVR 또는 VMS)의 사용자는 권한 인증을 거친 후 저장 영상에 접근하여야 하고, (2) 신속 정확하게 해당 영상을 검색할 수 있는 사용자 인터페이스 및 스마트 검색 기능이 제공되는 것이 바람직합니다. 그리고 (3) 사용자는 화면에 표시된 검색 영상을 확인하여 삭제를 하여야 할 것인지 요청 정보주체만 마스킹하면 될 것인지를 판단하게 될 것입니다. 만약, 해당 영상에 요청 정보주체만 있다면 해당 영상의 삭제하면 될 것이지만, 제3자도 존재하고 원래의 수집, 처리 목적상 영상의 보유가 필요한 경우에는 요청 정보주체만 마스킹하는 것이 필요할 수도 있습니다.

다른 상황으로서, 유출된 영상의 사본이 인터넷에 유포된 경우 해당 정보주체는 사본 영상까지 삭제를 요청할 수 있으며, 컨트롤러는 인터넷 사이트의 관리자에게 요청 사실을 통지하여 사본 영상이 삭제될 수 있도록 해야 합니다.

이러한 요구에 용이하게 대응하기 위해서는 (1) 저장장치는 모든 영상에 대한 처리 이력, 예를 들면 영상의 복사, 반출, 삭제 사실 및 해당 행위의 사용자, 발생 일시 등에 대한 로그를 생성하여 보관하여야 하며, (2) 권한 있는 사용자가 이를 용이하게 검색할 수 있는 사용자 인터페이스를 제공하여야 할 것입니다. 이러한 시스템을 사용하면 사용자는 해당 영상을 누가 언제 어떤 경로로 유포하였는지 알 수 있어 통지 의무를 용이하게 달성할 수 있을 것입니다.

3.2.3. 한화테크윈 영상 분석 솔루션

컨트롤러는 정보주체의 권리를 보장하기 위해 먼저 해당 개인이 포함된 영상을 식별해야 합니다. 한화테크윈은 표준 제품 또는 기술 파트너를 통해 개별적으로 기록된 정보의 검색, 식별 및 수집을 용이하게 하는 일련의 도구를 제공합니다.

컨트롤러는 한화테크윈이 제공하는 안면 인식(Facial Recognition), 얼굴 검출(Face Detection), 움직임 검출(Motion Detection), 비디오 서머리(Video Summary) 및 스마트 검색(Smart Search) 기능을 이용하여 개인 정보주체의 열람권이나 삭제권 등의 요청에 대응할 수 있으며, 검색된 결과는 안전하게 암호화한 후 요청자에게 전달할 수 있습니다. 특히, 한화테크윈이 준비중인 차세대 영상처리 칩셋은 사람/차량/동물 등 확장된 객체를 대상으로 한 딥러닝 기반 영상분석 기술이 적용될 예정으로 좀 더 빠르고 정확하게 컨트롤러 및 프로세서의 요구에 대처할 수 있게 될 것입니다.

3.3. 사이버 보안 이슈 관리

3.3.1. 접근 권한의 관리

시스템의 최상위 권한을 갖는 관리자 계정만을 사용하면 계정이 유출될 경우 전체 시스템에 대한 보안이 취약해져 개인정보의 권한 없는 처리, 불법적 처리 및 우발적 멸실, 파괴 또는 손상으로 이어질 수 있습니다. 이를 방지하기 위해 사용자 계정을 추가하고 계정 별로 권한을 제한할 수 있는 기능이 반드시 필요합니다.

또한, 네트워크 기기에 비인가자가 침입을 시도하거나 침입하는 경우, 관리자 권한으로 로그인 후 허가되지 않은 사용자 계정을 추가 생성하거나 불필요한 권한을 부여하는 경우 같은 보안 사고가 발생할 수 있습니다.

한화테크윈은 카메라, 녹화 장치, VMS에 다양한 권한 및 수준별로 사용자 또는 사용자 그룹을 구분하여 생성할 수 있는 기능을 제공하고 있습니다. 해당 기능을 이용하여 관리자는 사용자에게 필요한 최소한의 기능만을 제공할 수 있으며, 이를 통해 필요 이상의 권한을 남용함으로써 발생할 수 있는 개인정보의 오남용을 예방하기 위한 적절한 보안을 보장하고 있습니다.

아울러 한화테크윈은 컨트롤러와 프로세서가 장비 로그를 통해 침입 경로를 분석하거나 사고의 경위를 파악할 수 있도록 권한 부여/변경/삭제에 대한 로그를 포함한 다양한 로그 저장 및 로그 확인 기능을 제공함으로써 개인정보 침해 리스크에 대한 적절한 보안 수준을 제공하고 있습니다.

3.3.2. 접근 통제

허가되지 않은 비인가자가 권한이 없는 장비에 접근하는 것을 막기 위한 다양한 장치가 필요합니다. 그중에는 지속적인 무작위 비밀번호 입력 공격에 대한 대책이 포함되어 있어야 하며, 특히, 사용자가 초기 비밀번호가 있는 장비를 구입하여 비밀번호를 변경하지 않고 그대로 사용하는 경우, 사용자 설명서 등 인터넷을 통해 쉽게 비밀번호가 노출되어 심각한 보안 사고가 발생할 가능성이 매우 높아짐을 명심해야 합니다.

영상감시 장비가 공용망에 연결되어 있는 경우, 제품 검색을 편리하게 해주는 자동 포워딩 기능 등이 개인정보 탈취의 주요 경로로 악용될 수 있으며, 비인가자가 자신의 침입을 감추기 위해 고의로 기기를 초기화시키거나 자신의 행위를 기록한 로그 정보 등을 삭제할 경우에 차후 침입 경로 분석이나 추적에 어려움이 발생할 수 있습니다. 따라서 접속기록의 보관 기능 등은 접근 통제에 있어 반드시 필요한 기능 중 하나입니다.

그 밖에 영상감시 장비용으로 제공되는 펌웨어에는 장비의 중요 정보가 들어 있으므로 기본적으로 외부에서 분석이 불가능해야 하며 제조사가 배포하는 펌웨어 임을 확인할 수 있는 장치가 포함되어야 할 것입니다.

비밀번호 정책

한화테크윈은 유추하기 쉬운 비밀번호를 사용하지 못하도록 비밀번호 설정 시 문자, 숫자 및 특수기호를 조합한 최소한의 복잡도와 반복(1111, aaaa 등)되거나 연속(1234, abcd 등)되는 문자를 사용하지 않도록 요구하고 있습니다. 이를 통해 비밀번호 유추 또는 무작위 입력을 통한 비인가자의 무단 접근을 예방하고 있습니다.

무허가 접근 제한

한화테크윈은 비인가자가 권한이 없는 장비에 접근하는 것을 막기 위해 한화테크윈의 카메라, 녹화 장치에서는 접속 가능하거나 불가능한 사용자의 네트워크 IP 대역을 IP 필터링이라는 기능을 통해 사전 설정할 수 있습니다.

또한, 5번 이상 연속되어 비밀번호가 잘못 입력되는 경우에는 일시적으로 비밀번호 입력을 제한함으로써 지속적인 무작위 비밀번호 입력 공격(Brute force attack)을 통한 인증 정보 탈취를 예방하고 있으며, 관리자 권한이 인증되지 않은 상태에서는 원격으로 비밀번호 초기화가 가능하지 않게 (로컬에서만 가능) 설계함으로써 비인가자의 장비 접근 로직을 일절 허용하지 않고 있습니다.

안전한 공용망 접속

한화테크윈은 카메라, 녹화 장치, VMS에서 Telnet, SSH, FTP 서버 등과 같은 쉘 접근이 가능한 임의의 원격 서비스 포트를 정책적으로 허용하지 않고 있으며, S/W 코드에 백도어가 존재하지 않도록 안전한 코드 개발(Secure Coding) 및 지속적인 테스트와 모니터링을 수행하고 있습니다. 또한, 공용망에서의 제품 검색은 편리하게 해주나 개인정보 탈취의 경로가 될 수 있는 UPNP Discovery의 자동 포트 포워딩(NAT Traversal) 기능 사용을 금지하고 있습니다. (단, 클라우드에 연결되는 홈카메라는 서비스를 위해 어쩔 수 없이 자동 포트 포워딩 기능을 허용하고 있으나 영상 스트리밍을 위한 포트를 랜덤하게 제공하여 보안을 향상시키고 있습니다.)

접속 기록의 보관 및 점검

한화테크윈은 카메라, 녹화 장치, VMS에 대한 모든 장치 설정 변경 사항을 기록하기 때문에 로그를 확인하여 어떤 내용이 변경되었으며 누가 변경했는지를 파악하는 것이 가능합니다. 또한, 대부분의 로그 항목에는 롤백이 용이하도록 이전 설정과 새로운 설정이 모두 포함되어 있습니다.

아울러 카메라, 녹화장치는 공장 초기화를 하는 경우에도 이러한 로그가 유지되도록 되어 있는데, 로그를 초기화하지 못하도록 하는 기능은 비인가자가 자신의 침입을 감추기 위해 고의로 기기를 초기화시키는 경우를 예방하고 침입 경로 분석 및 추적에 매우 유용하게 사용될 수 있습니다.

악성 프로그램 방지

한화테크윈의 카메라, 녹화 장치에서 사용하는 펌웨어가 암호화 되어 있으므로 펌웨어 안에 포함되어 있는 중요 정보가 임의로 분석되거나 위변조 될 수 없도록 설계되어 있습니다. 아울러 VMS, 모바일(iOS)에서 사용하는 어플리케이션은 신뢰할 만한 CA 기관에서 발급된 한화테크윈의 개인키로 전자 서명되어 있습니다. 이를 통해 해당 어플리케이션이 당사에서 배포되었다는 것을 보장할 수 있으며, 악성코드로부터 위변조되지 않았음을 보증할 수 있습니다. 또한, 한화테크윈의 홈카메라는 전용 서버를 통해 펌웨어가 최신 버전으로 자동 업데이트 되므로 손쉽게 보안 및 안정성을 향상시킬 수 있습니다.

3.3.3. 전송 안전성

CCTV 시스템(감시카메라, 저장장치 및 관제 소프트웨어)간의 공유되는 개인정보(사용자 인증정보, 영상 스트리밍)를 보호하기 위해서는 네트워크를 통해 전달되는 정보에 대한 안전한 보호장치가 마련되어야 합니다.

한화테크윈은 카메라, 녹화 장치, VMS에서 서버와 클라이언트간 HTTP 송수신 시 HTTP Digest 인증을 사용하여 사용자 비밀번호를 보호할 수 있으며, HTTPS를 사용하여 사용자 비밀번호 및 RTSP로 전송되는 사용자 영상을 보호할 수 있습니다. 다만, HTTPS 모드는 기본적으로 사용자 인증과 같이 HTTP 프로토콜로 전송되는 데이터만 보호되므로, RTSP 프로토콜로 전송되는 영상 스트리밍을 보호하기 위해서는 클라이언트 단에서 RTSP를 HTTPS로 터널링하는 추가적인 설정 작업을 필요로 합니다. 클라우드에 연결되는

홈카메라의 경우 RTP 기반의 미디어 통신용 보안 프로토콜인 SRTP를 사용하여 영상 스트리밍을 보호하고 있습니다.

3.3.4. 보관 안전성

감시카메라, 저장장치 및 관제 소프트웨어 내에 보관되는 시스템의 중요 정보(사용자 인증정보 포함)는 혹시라도 발생할 수 있는 보안 취약점이나 물리적 보안의 미흡으로 인하여 탈취되는 사고 발생 시 그 정보를 사용할 수 없도록 보호장치가 마련되어야 합니다. 한화테크윈은 카메라, 저장장치, VMS의 사용자 인증 정보(비밀번호)를 해시를 이용해 일방향 암호화를 하고 있으며, 필요에 따라서 양방향 암호화를 사용하여 안전하게 보관합니다.

3.3.5. 반출(백업) 안전성

CCTV 시스템(감시카메라, 저장장치 및 관제 소프트웨어)내에 보관되는 개인정보(비디오 파일)는 필요에 의해 해당 시스템에서 반출(백업)되더라도 권한 없는 사용자를 통해 임의로 재생 및 악용되지 못하도록 보호장치가 마련되어야 합니다.

한화테크윈은 저장장치, VMS에서 전용 백업 포맷인 SEC 파일 포맷으로 백업 시 비밀번호를 설정함으로써 비디오 파일에 대한 암호화를 적용할 수 있습니다. 추출된 해당 파일에 암호화가 적용되면 임의 열람이 불가능하므로 비디오 파일이 유출되더라도 개인정보를 보호할 수 있습니다. 아울러, 기본적으로 재생에 필요한 플레이어(백업 뷰어)가 SEC 파일에 자동으로 포함되어 있어 사용자가 SEC 파일을 더블 클릭만 하면 별도의 플레이어를 설치할 필요 없이 편리하게 비디오 파일을 재생할 수 있습니다.

3.3.6. 위변조 방지

CCTV 시스템(감시카메라, 저장장치 및 관제 소프트웨어)내에 보관되는 개인정보(비디오 파일)는 필요에 의해 해당 시스템에서 반출(백업)되더라도 권한 없는 사용자를 통해 임의로 위변조되지 못하도록 보호장치가 마련되어야 합니다.

한화테크윈은 저장장치, VMS에서 SEC 파일 포맷으로 백업 시 일반 편집용 소프트웨어로 파일 열기가 불가능하므로 파일의 위변조를 예방할 수 있으며, 위변조가 되더라도 비디오의 해쉬 정보를 프레임마다 같이 저장하는 워터마킹

기능이 적용되어 있어 해당 비디오의 특정 프레임이 변조되었는지 여부 확인이 가능합니다. 또한, 자사 VMS인 SSM에서 SEC 파일로 추출하는 경우, 전자 서명 기능이 추가 지원되어 해당 비디오가 한화테크윈의 SSM에서 추출되었다는 기술적 확인이 가능하며 비디오 파일이 위변조 되지 않았다는 증거로 활용할 수 있습니다. 해당 워터마킹과 전자서명에 대한 검증은 SEC 파일에 내장된 백업 뷰어 도구를 사용하여 확인이 가능합니다.

GDPR은 빅데이터와 같은 디지털 경제 활성화라는 시대적 요구에 대비하기 위하여 넓은 영토적 적용 범위, 개인정보 범위의 확대, 적법 처리 기준의 상향, 정보주체의 권리 확대, 개인정보 유출통지 의무, DPO 의무 지정, 기업의 책임성과 거버넌스의 강화 및 천문학적인 벌금으로 인하여 GDPR의 파급효과는 상당할 것으로 예상됩니다. 또한, GDPR의 영향으로 향후 세계 각국의 개인정보 보호도 더욱 강화될 것으로 예상됩니다.

CCTV 영상감시 애플리케이션의 경우 공공 장소에서 촬영된 대규모의 개인영상정보를 체계적으로 모니터링하는 고위험성이 있는 개인정보 처리에 해당하므로 개인정보 영향 평가(DPIA)의 수행뿐만 아니라 개인정보보호관(DPO)도 지정해야 합니다. CCTV 영상감시 애플리케이션을 운영 및 관리하는 CCTV 사용자나 CCTV 영상감시 서비스 제공자가 GDPR을 준수하기 위해서는 GDPR에 대한 바른 인식을 바탕으로 개인정보 처리의 6대 원칙을 준수하였음을 의미하는 책임성 원칙을 증명할 수 있는 방안을 마련해야 합니다.

유의해야 할 점은 GDPR은 개인정보의 컨트롤러 및 프로세서가 책임성 원칙을 입증하기 위해 적절한 기술적·조직적 조치를 취하기만 하면 개인정보의 침해가 절대 발생하지 않을 것을 요구하는 것은 아니라는 점입니다. 다시 말하면, 개인정보 침해의 일차적 책임은 컨트롤러나 프로세서에게 있지만, 그 책임성을 다했다는 것이 입증되고 그럼에도 불구하고 개인정보의 침해로 인한 벌금 등의 제재를 받는 경우, 그 책임은 CCTV 영상감시 시스템을 제공한 측에 전가될 수도 있다는 점입니다. 특히, 그 시스템이나 기술이 안전하다고 보증을 하였으나 실제로 그렇지 않은 것으로 판명된 경우가 이에 해당할 것입니다.

이와 같이 CCTV 영상감시 애플리케이션 관점에서의 GDPR 준수는, 특히 사이버보안 같은 문제로 인한 개인정보 침해나 유출에 효과적으로 대비하기 위해, CCTV 영상감시 시스템의 최종 사용자만이 아니라, 시스템 통합 업체(SI) 및 CCTV 제조업체들도 함께 협력하는 자세가 필요할 것입니다.

저희 한화테크윈은 GDPR(General Data Protection Regulation)에 대한 이해와 올바른 준수를 바탕으로, 개인정보 보호에 친화적인 제품을 제공하고 사용자와 시스템 관련 정보 및 기록되는 중요한 영상정보가 안전하게 처리될 수 있도록 최선을 다하겠습니다.

WISENET

Hanwha Techwin Co.,Ltd.

13488 경기도 성남시 분당구 판교로 319번길 6 한화테크윈 R&D센터

TEL 070.7147.8771-8

FAX 031.8018.3715

http://hanwha-security.com

Hanwha Techwin