

## 유럽 개인 정보 보호 규정 (GDPR)

영상 감시에 주는 영향

# 목차

서론	3
1. GDPR이란 무엇인가?	4
2. GDPR은 영상 감시에 어떤 영향을 주는가?	5
2.1 GDPR 준수를 위한 단계	5
3. 결론	7

유럽 개인 정보 보호 규정(GDPR, General Data Protection Regulation)이 2018년 5월 25일에 발효됩니다. 이는 개인에 대한 데이터가 수집, 처리, 공유되는 방식에 대해 더 많은 통제 권한을 개인에게 제공하기 위한 것으로, 영상 감시 기술의 설치업체, 시스템 통합업체 및 사용자에게 영향을 줍니다.

GDPR은 기업의 역할과 책임을 보다 명확하게 하는 데 도움이 되는 구조를 제공하고, 개인에게도 자신의 개인 데이터가 사용되는 방식을 관리할 수 있는 더 큰 기회를 제공합니다.

이 규정은 유럽연합(EU) 내에 있는 조직, 그리고 조직의 위치와 상관없이 EU에 거주하는 데이터 주체의 개인 데이터를 처리 및 보관하는 조직에 모두 적용됩니다.

하나의 조직으로서 Axis는 언제나 개인의 프라이버시를 존중하고 보호하기 위해 최선을 다하고 있습니다. 따라서 Axis는 GDPR의 도입을 전적으로 지지하고, Axis 자체가 완전한 준수를 위해 노력할 것이며, 고객들이 가능한 최상의 방식으로 이를 준수할 수 있도록 지원을 제공할 것입니다.

Axis는 GDPR을 준수하기 위한 모델을 수립할 수 있도록 조치를 취했습니다. 이러한 전략에는 데이터 처리와 관련하여 Axis가 실시하는 활동이 보안성을 유지할 수 있도록 하기 위한 지속적 테스트 및 검토가 포함되어 있습니다.

여러 조직이 GDPR과 관련하여 의문점을 가지고 있습니다. 지금 우리는 왜 이러한 새 규정이 필요한가? 이 규정으로 인해 무엇이 발생하는가? 이는 영상 감시에 어떻게 영향을 미치는가? 준수를 보장하려면 어떤 조치를 취해야 하는가? 등입니다.

이 백서는 GDPR의 영향을 살펴보고, 영상 감시 분야의 시장 참여자들이 GDPR로 인해 발생하는 도전과제와 기회를 모색할 수 있도록 도움을 주기 위한 것입니다.



**Simon Ottosson**  
법무 책임자  
Axis Communications



**Edwin Roobol**  
중유럽 지역 디렉터  
Axis Communications

## 1. GDPR이란 무엇인가?

개인 정보 보호 규정(GDPR)은 조직이 보유하고 있는 각종 형태의 개인 데이터에 적용되는 규칙의 조합입니다. GDPR은 모든 개인에게 자신의 개인 데이터에 대한 소유권을 제공하며, 조직에게는 데이터 처리 및 저장의 모든 단계에서 책임을 부여합니다. GDPR은 개인에게 여러 권한을 제공하고, 개인 데이터를 처리하는 조직에게는 상응하는 책임을 부여함으로써 그 목적을 달성합니다.

### 개인 데이터란 무엇인가?

GDPR을 이해하는 데 있어서 중요한 점은 개인 데이터에 대한 법률적 정의를 명확하게 하는 것입니다. 법률적 정의에 따르면 개인 데이터는 식별된 또는 식별 가능한 개인과 관련된 모든 정보입니다. 식별 가능한 개인이란 직접적 또는 간접적으로 식별할 수 있는 사람으로, 구체적으로는 이름, ID 번호, 위치 데이터, 온라인 식별자(IP 주소 또는 쿠키 식별자) 등과 같은 식별자, 또는 해당 개인의 물리적, 생리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특정한 하나 이상의 요소를 가리키는 맥락에서 사용하는 말입니다.

### GDPR의 지리적 범위

GDPR은 기업이 EU 내에 설립된 경우, 항상 이 기업의 개인 데이터 처리에 적용됩니다. 해당 기업이 EU 내에 설립되지 않은 경우에는 처리된 데이터가 EU에 있는 개인과 관련된 경우, 데이터 처리가 해당 개인이 EU 내에 있을 때 이들에 대한 재화 또는 용역의 제공과 관련이 있는 경우, 또는 이들 개인이 EU 내에 있을 때 이들의 행동을 모니터링하는 경우, GDPR이 적용됩니다. 따라서 이 유럽 규정은 세계적으로 영향을 미친다는 점이 명확합니다.

### 조직의 서로 다른 책임

개인 데이터를 처리 또는 저장하는 모든 조직은 GDPR을 준수하는 방식으로 이를 실시해야 할 책임이 있습니다.

GDPR은 조직을 *데이터 관리자* 와 *데이터 처리자* 두 범주로 분류하며, 각각 다음과 같은 법률적 의무가 있습니다.

*데이터 관리자*: 데이터 관리자는 개인 데이터 처리의 목적과 수단을 결정하는 사람으로, 감시 목적으로 CCTV 시스템을 사용하는 매장 소유자를 예로 들 수 있습니다.

*데이터 처리자*: 데이터 처리자는 데이터 관리자를 대신하여 데이터 관리자가 제공하는 지침에 따라 개인 데이터를 처리하는 사람입니다. 처리자는 예를 들어 매장 소유자와 같이 감시 목적으로 CCTV 시스템을 가지고 있는 사람을 대신해서, 그 사람이 제공하는 지침에 따라 CCTV 시스템에서 수집한 데이터를 관리하는 회사일 수 있습니다.

### 설계 프라이버시와 기본 설정 프라이버시

GDPR에 따르면 개인 데이터 관리자는 이러한 데이터를 처리할 때 GDPR에 규정된 데이터 보호 원칙을 구현할 수 있도록 설계된 기술적 또는 조직적 조치를 실행할 의무가 있습니다. GDPR은 이를 *설계 프라이버시(privacy by design)*라 합니다. 펌웨어가 포함된 카메라의 맥락에서 봤을 때 설계 프라이버시의 적절한 예는 사용자가 이미지 포착을 특정 경계 구역으로 제한할 수 있도록 디지털적으로 허용함으로써 그렇지 않은 경우 포착될 이러한 경계 구역 외부의 이미지를 카메라가 포착하는 것을 방지하는 기능일 것입니다.

또한 관리자는 해당 개인 데이터의 처리가 프라이버시 침해로 최소화하도록 기본 설정되어 있는 기술적 또는 조직적 조치를 구현할 책임이 있으며, GDPR은 이를 *기본 설정 프라이버시(privacy by default)*라 합니다. 펌웨어가 포함된 카메라의 맥락에서 봤을 때 기본 설정 프라이버시의 적절한 예는 사용자가 위의 예에 따라 정확한 이미지 포착 경계 구역을 설정하도록 자동으로 메시지를 표시하는 기능일 수 있습니다.

### 개인의 권한

GDPR을 제정한 주요 동인 중 하나는 개인 데이터의 관리와 관련하여 보다 큰 보호와 권한을 개인에게 제공해야 한다는 필요성입니다. 이 규정의 조건에는 일부 매우 구체적인 요건이 있으며, 이들 모두는 개인 데이터를 처리 또는 저장하는 당사자가 이러한 데이터의 프라이버시를 유지해야 할 책임이 있다는 것을 의미합니다.

또한 이 규정은 포착점에서 개인 데이터가 수집되는 시점과 이러한 데이터가 어떻게 사용되는지에

대해 알 수 있는 권한을 제공합니다. 예를 들어 영상 감시의 경우, 이는 영상 감시가 사용되고 있는 구역과 주변의 적절한 표시를 의미합니다.

## 2. GDPR은 영상 감시에 어떤 영향을 주는가?

GDPR과 관련된 대부분의 논의는 스프레드시트 또는 데이터베이스에 저장된 이름 및 이메일 주소의 목록과 같은 보다 전통적인 데이터의 안전한 저장과 처리에 중점을 두고 있습니다. 동영상에 대해서는 관심이 훨씬 적지만 이는 기업이 동일하게 인식해야 하는 영역입니다.

개인 데이터가 감시 영상에 포함된 정도에 따라 GDPR 조항이 적용됩니다.

### 카메라 제품 및 솔루션과 같은 감시 장비의 사용에 대한 GDPR의 영향

Axis가 판매하는 제품 및 솔루션의 경우, 개인 데이터를 처리하기 위한 제품 또는 솔루션의 이와 같은 사용이 GDPR을 준수하도록 해야 할 주된 책임은, 제품 또는 솔루션의 관리자인 사용자에게 있습니다. 이는 크게 봤을 때 제품 및 솔루션의 맥락에서 GDPR 준수 또는 위반의 발생은 고객이 제품 또는 솔루션을 사용하는 방식에 달려 있다는 것을 의미합니다.

### 특정 호스팅 서비스의 사용에 영향을 미치는 GDPR

서비스의 경우, GDPR 준수 여부는 일정 부분 이러한 서비스가 제공되는 방식에 따라 달라지며, 이는 Axis의 책임입니다. 그러나 GDPR 준수 또는 위반의 발생은 대부분 고객이 서비스를 사용하는 방식에 따라 달라집니다. 어떤 유형의 GDPR 책임이 발생하고 누가 이런 책임을 지는지는 용도별로 검토해야 합니다.

호스팅 서비스인 AXIS Guardian을 예로 들어 보겠습니다. GDPR이 일반적으로 어떻게 적용되며 누가 어떤 책임이 있는지는 다음과 같습니다.

- > *알람 운영사의 고객*: 사용자의 카메라 감시 시스템이 포착하여 AXIS Guardian으로 업로드한 비디오 자료에 포함된 개인 데이터의 관리자.
- > *알람 운영사*: 사용자가 AXIS Guardian으로 업로드한 개인 데이터(예: 사용자 직원 정보 및 포착한 비디오)의 사용자를 대신하는 데이터 처리자.
- > *Axis*: 알람 운영사가 AXIS Guardian으로 업로드한 개인 데이터(예: 알람 운영사 직원 정보)에 대해 알람 운영사를 대신하는 데이터 처리자, 그리고 알람 운영사의 고객이 AXIS Guardian으로 업로드한 개인 데이터(포착한 비디오)에 대해 알람 운영사를 대신하는 개인 데이터 하위 처리자.
- > *Amazon Web Services*: 알람 운영사 및 알람 운영사의 고객(사용자)이 AXIS Guardian으로 업로드한 개인 데이터에 대해 Axis를 대신하는 데이터 하위 처리자.

### 2.1 GDPR 준수를 위한 단계

GDPR은 미래에 조직이 비디오 데이터를 포함하여 데이터를 취급하는 방식에 영향을 미치는 규정입니다.

개인 데이터를 처리하는 각 조직은 적어도 해당 조직이 GDPR 및 회사 정책에 맞게 개인 데이터를 취급하도록 할 책임이 있는 한 명 이상의 담당 인원이 필요합니다(물론 여기에 할당되는 공수는 조직의 규모와 수집 및 처리되는 개인 데이터의 양에 따라 달라집니다). 또한 일부 조직의 경우, 이러한 작업을 실시하기 위한 공식적인 데이터 보호 책임자(Data Protection Officer: DPO)가 필요합니다.

또한 관리 프로세스에도 변화가 있을 것입니다. GDPR이 적용되는 가운데 조직은 데이터 처리 활동의 구체적이고 정확한 기록을 유지해야 합니다. 기록해야 하는 다양한 디테일이 있으며, 여기에는 다음과 같은 사항도 포함됩니다.

- > 처리한 개인 데이터와 관련된 개인의 범주(예: 고객, 직원, 매장 방문객 등)
- > 개인 데이터가 사용되는 목적
- > 개인 데이터가 다른 기업 및/또는 EU 밖으로 전송될 것인지 여부
- > 개인 데이터가 저장되는 기간
- > 각 개별 데이터 처리 활동과 관련하여 GDPR 준수를 보장하기 위해 해당 조직이 취하는 조치

저장된 감시 영상의 경우, 이 모든 것이 관련되어 있습니다.

조직은 비디오 카메라가 특정 장소에 있는 이유, 그리고 무엇을 왜 촬영하는지를 설명해야 할 의무가 있습니다. 영상 감시의 경우, 영상 감시를 사용하는 구역과 그 주변에 적절한 표시를 사용하여 이에 대한 정보를 제공해야 합니다.

공공 장소에 카메라를 설치하는 경우, 데이터 관리자는 데이터 보호 영향 평가(Data Protection Impact Assessment: DPIA)를 실시해야 할 수 있습니다. DPIA에는 다음과 같은 사항이 포함되어야 합니다(DPIA의 정확한 특징은 사례별로 결정해야 함).

- > 의도한 처리 작업 및 처리 목적의 체계적인 설명
- > 목적 면에서 처리 작업의 필요성 및 비례성 평가
- > 개인의 권한 및 자유에 대한 위험 평가
- > 개인 데이터의 보호 및 GDPR 준수를 보장하기 위한 보호 조치 및 메커니즘을 포함하여 이러한 위험을 해결하기 위해 계획한 조치(이는 개인 및 영향을 받는 다른 사람의 권한과 정당한 이익을 고려해야 함)

새로운 규정의 중요한 특징 중 하나는 모니터링 대상이 되는 사람에게 이들에 대한 어떤 데이터가 보관되고 있으며 어떻게 사용되고 있는지에 대해 완전히 알려야 한다는 점입니다.

이 규정은 암호화 및 데이터 보호 방법에 대한 일부 명확한 기본 규칙을 규정하고 있습니다. 데이터가 비디오 형식라는 사실은 이러한 요건에 영향을 주지 않습니다.

따라서 비디오를 저장하는 기업은 개인 데이터의 저장에 관한 한 명확한 책임이 있으며, 무단 접근을 방지할 수 있도록 확실한 조치를 취해야 합니다. 이는 누가 카메라와 기록에 접근할 것인지를 서면으로 규정해야 한다는 것을 의미합니다.

또한 조직은 개인이 개인 데이터에 대한 접근 권한을 행사하고 그 삭제를 요청하는 경우에 대비한 절차를 가지고 있어야 합니다. 이는 GDPR이 적용되는 가운데 이러한 요청을 충족시켜야 하는 것으로 설정된 한 달간의 기간을 벗어나지 않도록 하기 위한 것입니다. 이러한 요청을 할 때 요청자는 이러한 데이터를 찾을 수 있도록 적절한 정보(예: 영상이 포착된 대략적인 시간대 및 위치)를 제공할 것으로 기대할 수 있습니다.

또한 기업은 보관하고 있는 개인 데이터에 대한 무단 접근을 방지할 수 있도록 강력한 조치를 사용해야 합니다. 각 기업이 사용하는 전략은 해당 기업이 직면하는 도전과제에 따라 고유한 것입니다. 그러나 어떠한 경우에도 기업은 견실한 보안 관리를 적용하고, 최신 사이버 보안 모범 관행을 유지해야 하며, 안전한 하드웨어, 소프트웨어 및 철저한 사후 관리를 제공하는 신뢰성 높은 파트너와 함께해야 합니다.

### 3. 결론

GDPR을 준수하고 사용자가 처리하는 개인 데이터 주체의 권한을 보호할 책임은 궁극적으로 감시 장비, 감시 솔루션 및 감시 서비스의 사용자에게 있습니다. 이와 관련하여 아무런 조치도 취하지 않았거나 미흡한 조치를 취한 조직은 적절한 대책을 세워야 합니다. 해야 할 일을 완료하고 이 규정에 명시된 책임에 주의를 기울인 기업은 별로 걱정할 것이 없습니다.

따라서 감시 장비, 감시 솔루션 및 감시 서비스 사용자의 경우, 개인의 프라이버시를 존중하고 지키며 개인 데이터를 보호하는 데 최선을 다하는 공급사 및 벤더와 파트너 관계를 맺는 것이 좋습니다. 또한 감시 장비, 감시 솔루션 및 감시 서비스 사용자는 GDPR 준수를 쉽게 실시할 수 있도록 공급사 및 벤더로부터 받는 도움과 기술 지원에 의지할 수 있어야 합니다.

#### **추가적인 자료:**

[GDPR 전체 상세 정보](#)

[유럽 데이터 보호 감독 기구\(EDPS\) 웹사이트](#)

[중소기업 데이터 보호 가이드 웹사이트](#)

# Axis Communications

Axis는 보안성을 강화하고 비즈니스를 수행하는 새로운 방식에 대한 통찰력을 제공하는 네트워크 솔루션 창출을 통해 더욱 스마트하고 안전한 세상을 만듭니다. 네트워크 비디오 분야의 업계 리더인 Axis는 영상 감시, 접근 제어 및 오디오 시스템, 비디오 분석용 제품 및 서비스를 제공합니다.

Axis는 세계 50여 개국에 2,800여 명의 헌신적인 직원을 두고 있으며, 전 세계 파트너와의 협력을 통해 고객 솔루션을 제공합니다. 1984년에 설립된 Axis는 스웨덴에 본사를 두고 있으며 현재 NASDAQ Stockholm에 상장 (AXIS)되어 있습니다.

Axis에 대한 보다 자세한 내용은 [www.axis.com](http://www.axis.com)에서 확인하실 수 있습니다.