GDPR
(Regulamento Europeu Geral de Proteção de Dados)

Implicações para a área de vigilância por vídeo

Índice

O GDPR (Regulamento Europeu Geral de Proteção de Dados) entra em vigor no dia 25 de maio de 2018. O objetivo é proporcionar às pessoas mais controle sobre a forma como os dados mantidos sobre elas são coletados, processados e compartilhados, o que tem implicações para instaladores, integradores de sistemas e usuários de tecnologias de vigilância por vídeo.

O GDPR fornece uma estrutura que ajuda a tornar as funções e responsabilidades das empresas mais claras, além de proporcionar às pessoas mais oportunidades para controlar como seus dados pessoais são usados.

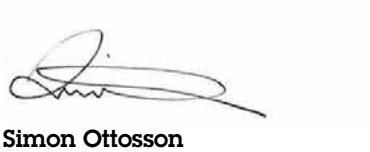
O regulamento rege empresas sediadas na UE (União Europeia) e aquelas que processam e mantêm dados pessoais de titulares de dados que residem na UE, independentemente da localização da empresa.

Como empresa, a Axis sempre esteve comprometida em respeitar e proteger a privacidade individual. Assim, a Axis está totalmente comprometida com a introdução do GDPR e, ao mesmo tempo que trabalha para estar em plena conformidade, também fornecerá suporte para facilitar a conformidade de seus clientes da melhor maneira possível.

A Axis tomou medidas para implementar um modelo de conformidade com o GDPR. Parte dessa estratégia inclui testes e análises contínuos, para garantir que as atividades da Axis relacionadas ao processamento de dados permaneçam seguras.

Muitas empresas têm dúvidas sobre o GDPR. Por que precisamos desse novo regulamento agora? O que o regulamento implica? Como ele afeta a vigilância por vídeo? E quais medidas devem ser tomadas para garantir a conformidade?

Este relatório técnico explora as implicações do GDPR e visa ajudar os agentes do setor de vigilância por vídeo a encarar os desafios e oportunidades do GDPR.



Simon Ottosson
Assessor jurídico
Axis Communications

Edwin Roobol
Diretor regional da Europa Central
Axis Communications

1. O que é o GDPR?

O GDPR (Regulamento Europeu Geral de Proteção de Dados) é um conjunto de regras que rege todos os tipos de dados pessoais mantidos por uma empresa. O GDPR proporciona a cada indivíduo o domínio sobre seus dados pessoais e, no lado da empresa, introduz a responsabilização por todas as etapas do processamento e armazenamento dos dados. O GDPR alcança esse objetivo concedendo uma série de direitos às pessoas e introduzindo obrigações correspondentes às empresas que processam dados pessoais.

O que são dados pessoais?
Para compreender o GDPR, é importante esclarecer a definição legal de dados pessoais. A legislação define dados pessoais como qualquer informação relativa a uma pessoa identificada ou identificável. Uma pessoa identificável é alguém que pode ser identificado direta ou indiretamente, especificamente por referência a um identificador como nome, número de identificação, dados de localização, identificador on-line, como endereços IP ou identificador de cookie, ou a um ou mais fatores específicos à identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

Alcance geográfico do GDPR
O GDPR sempre será aplicável ao processamento de dados pessoais de uma empresa se a empresa for estabelecida na UE. Se a empresa não tiver um estabelecimento dentro da UE, o GDPR será aplicável se os dados processados envolverem pessoas que estejam na UE, se o processamento dos dados estiver relacionado à oferta de bens ou serviços a essas pessoas quando estiverem na UE ou ao monitoramento do comportamento dessas pessoas quando estiverem na UE. Então, obviamente, esse regulamento europeu tem impacto mundial.

Diferentes responsabilidades para as empresas
Todas as empresas que processam ou armazenam dados pessoais devem assumir a responsabilidade de garantir que o façam em conformidade com o GDPR.

O GDPR classifica as empresas em duas categorias: *controladoras de dados* e *processadoras de dados*, cada uma com suas próprias obrigações legais:

Controladora de dados: uma controladora de dados determina a finalidade e os meios de processamento dos dados pessoais, por exemplo, um proprietário de loja que usa um sistema de CFTV para fins de vigilância.

Processadora de dados: uma processadora de dados processa os dados pessoais em nome da controladora de dados e de acordo com as instruções fornecidas por ela. Uma processadora pode ser uma empresa que gerencia os dados reunidos em nome de uma empresa que tenha um sistema de CFTV para fins de vigilância, e de acordo com as instruções fornecidas pela empresa, como por exemplo, o proprietário de uma loja.

Privacidade por concepção e privacidade por padrão
De acordo com o GDPR, ao processar esses dados, a controladora de dados pessoais tem a obrigação de implementar medidas técnicas e organizacionais concebidas para implantar os princípios de proteção de dados definidos no GDPR. O GDPR designa essas medidas como *privacidade por concepção*. No contexto de uma câmera que inclua firmware, um exemplo relevante de privacidade por concepção seria um recurso que permitisse ao usuário restringir digitalmente a captura de imagens a um determinado perímetro, impedindo que a câmera capturasse qualquer imagem fora desse perímetro que, de outra maneira, seria capturada.

A controladora também tem a obrigação de implementar medidas técnicas ou organizacionais que, por padrão, garantam o processamento menos invasivo possível da privacidade dos dados pessoais em questão; o GDPR designa isso como *privacidade por padrão*. No contexto de uma câmera que inclua firmware, um exemplo relevante de privacidade por padrão poderia ser um recurso que solicitasse automaticamente que o usuário definisse o perímetro exato de captura da imagem, de acordo com o exemplo anterior.

Direitos individuais
Uma das principais forças motivadoras por trás do GDPR é a necessidade de oferecer às pessoas maior proteção e um conjunto de direitos que rejam seus dados pessoais. Existem alguns requisitos muito específicos sob os termos do regulamento, o que significa que a parte que processa ou armazena dados pessoais tem a responsabilidade de manter esses dados privados.

O regulamento também dá às pessoas o direito de serem informadas quando seus dados pessoais forem coletados no ponto da captura, e como eles serão usados. No caso da vigilância por vídeo, por exemplo, isso significará uma sinalização adequada dentro e ao redor da área onde a vigilância por vídeo for usada.

2. Como o GDPR afeta a vigilância por vídeo?

Grande parte do debate sobre o GDPR foi concentrado no armazenamento e no processamento seguros dos dados mais tradicionais, como uma lista de nomes e endereços de e-mail armazenada em uma planilha ou banco de dados. Atenção muito menor vem sendo dada à imagem em movimento, mas essa é uma área com a qual as empresas precisam ficar igualmente atentas.

Na medida em que o vídeo de vigilância contiver dados pessoais, ele estará sujeito às disposições do GDPR.

O impacto do GDPR sobre o uso de equipamentos de vigilância, como produtos e soluções de câmeras
Com relação aos produtos e soluções vendidos pela Axis, é o usuário, como controlador do produto ou solução, o principal responsável por garantir que qualquer uso de um produto ou solução para processar dados pessoais seja compatível com o GDPR. Isso significa que, no contexto de produtos e soluções, a conformidade com o GDPR ou casos de violação em geral dependem de como o cliente usa o produto ou solução.

O GDPR afeta o uso de serviços hospedados específicos
No caso dos serviços, a conformidade com o GDPR depende, em parte, da forma como o serviço é fornecido, o que é uma responsabilidade da Axis. Porém, ainda assim, a conformidade com o GDPR ou casos de violação dependem, em grande parte, da forma como o serviço é usado pelos clientes. Os tipos de obrigações que surgem a partir do GDPR, e quem tem essas obrigações, é algo deve ser examinado de acordo com a aplicação específica.

Vamos tomar como exemplo um serviço hospedado, o AXIS Guardian. Veja a seguir como será uma aplicação típica do GDPR, e quem serão os responsáveis:

> *Clientes de operadores de alarme:* controlador de dados dos dados pessoais contidos no material de vídeo capturado pelo sistema de vigilância por câmera do usuário e transferido para o AXIS Guardian.
> *Operador de alarme:* processador dos dados, em nome dos usuários, dos dados pessoais transferidos para o AXIS Guardian pelo usuário (por exemplo, informações de funcionários e vídeos capturados do usuário).
> *Axis:* processador de dados, em nome do operador de alarme, dos dados pessoais transferidos para o AXIS Guardian pelo operador de alarme (por exemplo, informações dos funcionários do operador de alarme) e subprocessador de dados pessoais, em nome do operador de alarme, dos dados pessoais transferidos para o AXIS Guardian pelos clientes do operador de alarme (vídeo capturado).
> *Amazon Web Services:* subprocessador de dados, em nome da Axis, dos dados pessoais transferidos para o AXIS Guardian por um operador de alarme e pelos clientes do operador de alarme (usuários).

2.1 Avanços em direção à conformidade com o GDPR

O GDPR é um regulamento que influenciará a forma como as empresas lidam com os dados, incluindo dados de vídeo, no futuro.

No mínimo, todas as empresas que processam dados pessoais precisarão ter um ou mais funcionários designados responsáveis por garantir que a empresa lide com os dados pessoais de acordo com o GDPR e com a política da empresa (o número de horas de trabalho alocadas para isso dependerá do tamanho da empresa e do volume de dados pessoais coletados e processados). Além disso, para algumas empresas, o GDPR exigirá a nomeação de um DPO (Responsável pela Proteção de Dados) formal para executar essas tarefas.

Além disso, haverá mudanças nos processos administrativos. Sob o GDPR, as empresas deverão manter registros detalhados e precisos de suas atividades de processamento de dados. Há uma série de detalhes que devem ser registrados, incluindo, entre outros:

> À qual categoria de indivíduos os dados pessoais processados estão relacionados (por exemplo, clientes, funcionários, visitantes da loja etc.)
> Para quais fins os dados pessoais são usados
> Se os dados pessoais serão transferidos — para outras empresas e/ou fora da UE
> Por quanto tempo os dados pessoais serão armazenados
> As medidas tomadas pela empresa, em relação a cada atividade individual de processamento de dados, para garantir a conformidade com o GDPR

Tudo isso é relevante quando se trata de vídeos de vigilância armazenados.

As empresas são obrigadas a explicar a razão pela qual uma câmera de vídeo está em um lugar específico, o que está sendo filmado e o motivo. No caso da vigilância por vídeo, a sinalização apropriada dentro e ao redor da área onde a vigilância por vídeo está sendo aplicada deve ser usada para fornecer informações sobre isso.

O controlador de dados pode ser obrigado a realizar uma DPIA (Avaliação de Impacto sobre a Proteção de Dados) relativa à configuração de uma câmera em um local público. Uma DPIA deve incluir (as características precisas da DPIA devem ser decididas caso a caso):

> Uma descrição sistemática das operações de processamento e fins de processamento pretendidos
> Uma avaliação da necessidade e proporcionalidade das operações de processamento em termos de finalidade
> Avaliação de risco dos direitos e liberdades individuais
> As medidas planejadas para abordar esses riscos, incluindo garantias e mecanismos para garantir a proteção dos dados pessoais e a conformidade com o GDPR (isso deve levar em conta os direitos e interesses legítimos individuais e outras pessoas afetadas)

Uma das principais características do novo regulamento é que as pessoas sendo monitoradas precisam estar plenamente informadas sobre quais dados são mantidos sobre elas e como eles são usados.

O regulamento estabelece algumas regras básicas claras sobre criptografia e como os dados devem ser protegidos. O fato de os dados estarem em formato de vídeo não altera essa exigência.

As empresas que armazenam vídeos, portanto, têm responsabilidades claras quanto ao armazenamento de dados pessoais e devem implementar medidas sólidas para impedir o acesso não autorizado. Isso significa que é importante definir, por escrito, quem terá acesso às câmeras e gravações.

As empresas também devem ter procedimentos implementados para o caso de uma pessoa optar por exercer seu direito de acesso a seus dados pessoais ou solicitar sua exclusão. Essa medida deve permitir que a empresa respeite a janela de um mês durante a qual deve atender a essas solicitações sob o GDPR. Ao fazer tal solicitação, é razoável esperar que o solicitante forneça informações adequadas para a localização desses dados, como por exemplo, um período de tempo aproximado e o local onde a gravação foi capturada.

As empresas devem aplicar medidas sólidas para impedir o acesso não autorizado aos dados pessoais que armazenam. As táticas usadas por cada empresa serão exclusivas, de acordo com os desafios que enfrentam. Entretanto, em todo caso, as empresas devem empregar controles de segurança sólidos, ficar atualizadas sobre as práticas recomendadas de segurança cibernética e garantir que estejam trabalhando com parceiros confiáveis, que forneçam hardware, software e acompanhamento posterior minucioso.

3. Conclusão

Em última análise, o usuário dos equipamentos de vigilância, soluções de vigilância e serviços de vigilância é o responsável pela conformidade com o GDPR e pela proteção dos direitos das pessoas cujos dados pessoais o usuário processa. Empresas que tenham feito pouco ou nada nesse sentido precisarão se organizar. As empresas que cumpriram com seus deveres e ficaram atentas a suas responsabilidades sob o regulamento terão menos com o que se preocupar.

Como usuário de equipamentos de vigilância, soluções de vigilância e serviços de vigilância, é importante estabelecer parcerias com fornecedores comprometidos em respeitar e proteger a privacidade individual e os dados pessoais. Como usuário de equipamentos de vigilância, soluções de vigilância e serviços de vigilância, você também deverá ser capaz de contar com o suporte e a assistência técnica de seus fornecedores, para facilitar sua conformidade com o GDPR.

Fontes adicionais:

Todos os detalhes do GDPR

Site da Autoridade Europeia para a Proteção de Dados

Site de orientação sobre a proteção de dados para pequenas e médias empresas

72051/BR/R1/1807

Axis Communications em perspectiva

A Axis viabiliza um mundo mais inteligente e seguro, criando soluções de rede que fornecem insights para melhorar a segurança e apresentar novas formas de fazer negócios. Como líder do setor de vídeo em rede, a Axis oferece produtos e serviços para vigilância por vídeo, controle de acesso e sistemas de áudio, além de dados analíticos de vídeo.

A Axis conta com mais de 2.800 funcionários dedicados, em mais de 50 países, e colabora com parceiros em todo o mundo para oferecer soluções aos clientes. Fundada em 1984, a Axis é uma empresa com sede na Suécia e listada na NASDAQ de Estocolmo como AXIS.

Para obter mais informações, visite nosso site www.axis.com.

AXIS COMMUNICATIONS