Algemene verordening gegevensbescherming (AVG)

Implicaties voor videobewaking

Inhoudsopgave

De Algemene verordening gegevensbescherming (AVG) is op 25 mei 2018 in werking getreden. Het doel van de verordening is dat mensen meer controle krijgen over de manier waarop hun persoonsgegevens verzameld, verwerkt en gedeeld worden. De AVG heeft gevolgen voor installateurs, system integrators en gebruikers van videobewakingstechnologie.

Met de AVG wordt het duidelijker wat de verschillende rollen en verantwoordelijkheden zijn van elk specifiek bedrijf. Ook krijgen individuen meer zeggenschap over de manier waarop hun persoonsgegevens worden gebruikt.

De verordening geldt zowel voor organisaties die gevestigd zijn in de Europese Unie (EU) als voor organisaties die persoonsgegevens verwerken en bewaren van betrokkenen die in de EU wonen, ongeacht de locatie van de organisatie zelf.

Als organisatie heeft Axis zich altijd ingezet om de privacy te respecteren en te waarborgen. Axis staat dan ook vierkant achter de introductie van de AVG. Niet alleen werken we er hard aan om als bedrijf zelf de verordening volledig na te leven, ook helpen we onze klanten om er zo goed mogelijk aan te voldoen.

Axis heeft stappen gezet om een model voor AVG-compliance in te voeren. Onderdeel van deze strategie is het voortdurend testen en beoordelen van onze gegevensverwerkingsactiviteiten om ervoor te zorgen dat deze veilig zijn.

Veel organisaties hebben vragen over de AVG. Waarom hebben we deze nieuwe verordening nodig? Wat houdt de verordening precies in? Welke invloed heeft de verordening op videobewaking? Wat moet ik doen om de verordening na te leven?

Deze white paper gaat in op de gevolgen van de AVG en probeert medewerkers en bedrijven die werkzaam zijn in de videobewakingssector te helpen met de uitdagingen en kansen van de nieuwe verordening.

Simon Ottosson
Legal counsel
Axis Communications

Edwin Roobol
Regional Director Middle Europe
Axis Communications

1. Wat is AVG?

De Algemene verordening gegevensbescherming (AVG) beschrijft de regels voor organisaties die in contact komen met persoonsgegevens. De AVG bepaalt dat elk individu eigenaar is van zijn/haar persoonsgegevens. Bovendien moeten organisaties op elk moment verantwoording af kunnen leggen over de verwerking en opslag van deze gegevens. De AVG beschrijft de rechten van individuen met betrekking tot hun persoonsgegevens en de plichten van organisaties die persoonsgegevens verwerken.

Wat zijn persoonsgegevens?
Om een goed begrip te krijgen van de AVG, moet u eerst weten wat de juridische definitie is van persoonsgegevens. De wet geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Een identificeerbare persoon is iemand die direct of indirect geïdentificeerd kan worden, bijvoorbeeld aan de hand van een identificatie zoals een naam, identificatienummer, locatie, online identificatie zoals een IP-adres of cookie, maar ook aan de hand van een of meerdere factoren die verwijzen naar de fysieke, psychologische, genetische, mentale, economische, culturele of sociale identiteit van de betreffende persoon.

Geografisch bereik van de AVG
De AVG is van toepassing op bedrijven die in de EU gevestigd zijn en persoonsgegevens verwerken. Als het bedrijf geen vestiging heeft in de EU, is de AVG van toepassing indien de verwerkte gegevens betrekking hebben op personen in de EU, de gegevensverwerking betrekking heeft op het aanbieden van goederen of diensten aan deze personen wanneer deze zich in de EU bevinden of het bijhouden van het gedrag van deze personen wanneer ze zich in de EU bevinden. Het is dus duidelijk dat deze Europese richtlijn wereldwijde implicaties heeft.

Verschillende verantwoordelijkheden voor bedrijven
Bedrijven die persoonsgegevens verwerken of opslaan, zijn er zelf verantwoordelijk voor dat ze dit doen op een manier die voldoet aan de AVG.

De AVG deelt organisaties in twee categorieën in: *verwerkingsverantwoordelijken* en *gegevensverwerkers*. Beide hebben hun eigen wettelijke plichten.

Verwerkingsverantwoordelijke: een verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. Denk bijvoorbeeld aan een winkeleigenaar die gebruikmaakt van bewakingscamera's.

Gegevensverwerker: een gegevensverwerker is degene die persoonsgegevens verwerkt namens en in overeenstemming met instructies van de verwerkingsverantwoordelijke. Een verwerker kan een bedrijf zijn dat gegevens beheert die afkomstig zijn van een bewakingscamera. Het beheer gebeurt namens en in overeenstemming met instructies van degene die de bewakingscamera's heeft, bijvoorbeeld een winkeleigenaar.

Ingebouwde privacy (privacy by design) en standaard privacy (privacy by default)
De AVG schrijft voor dat de verwerkingsverantwoordelijke van persoonsgegevens, tijdens het verwerken van dergelijke gegevens, verplicht is om specifieke technische en organisatorische maatregelen te nemen om de gegevensbeschermingsprincipes, zoals beschreven in de AVG, op de juiste manier te implementeren. In de AVG wordt dit beschreven als *ingebouwde privacy*. Laten we eens kijken naar een camera met firmware. Een relevant voorbeeld van ingebouwde privacy zou een functie zijn waarmee de gebruiker op digitale wijze de beeldopname tot een bepaalde perimeter kan beperken. Zo wordt voorkomen dat de camera beelden opneemt buiten deze perimeter.

De verwerkingsverantwoordelijke is ook verplicht om technische of organisatorische maatregelen te nemen waarmee de verwerking van de betreffende persoonsgegevens standaard zo min mogelijk inbreuk maakt op de privacy van personen. In de AVG wordt dit beschreven als *standaard privacy*. Laten we weer kijken naar een camera met firmware. Een relevant voorbeeld van standaard privacy kan een functie zijn die de gebruiker, overeenkomstig het bovenstaande voorbeeld, automatisch eraan herinnert om de exacte beeldopnameperimeter in te stellen.

Rechten van individuen
Een van de belangrijkste drijfveren voor de AVG is de wens om individuen beter te beschermen en bepaalde rechten te geven waarmee ze hun persoonsgegevens zelf kunnen beheren. Er staan zeer

specifieke vereisten in de verordening. De partij die de persoonsgegevens verwerkt of opslaat, is er verantwoordelijk voor om de privacy ervan te beschermen.

De verordening geeft ook aan dat het verplicht is om individuen op de hoogte te stellen op het moment dat hun persoonsgegevens worden verzameld en te informeren over de manier waarop ze gebruikt worden. In het geval van videobewaking betekent dit dat het te bewaken gebied en het gebied eromheen voorzien is van duidelijke bebording die aangeeft dat het gebied bewaakt wordt.

2. Welke invloed heeft de AVG op videobewaking?

De meeste discussies over de AVG richten zich op de veilige opslag en verwerking van traditionele gegevens, zoals namenlijsten en e-mailadressen in een spreadsheet of database. Er is weinig aandacht voor bewegend beeld, maar dat betekent niet dat bedrijven hier minder op hoeven te letten.

Als de beelden van een bewakingsvideo persoonsgegevens bevatten, vallen ze onder de AVG.

Impact van de AVG op het gebruik van bewakingsapparatuur, zoals cameraproducten en -oplossingen
Bij door Axis verkochte producten en oplossingen wordt de gebruiker beschouwd als de verwerkingsverantwoordelijke. Deze is er dus in eerste plaats verantwoordelijk voor dat elke verwerking van persoonsgegevens, die gerealiseerd wordt met het product of de oplossing van Axis, in overeenstemming is met de AVG. Dit betekent dat naleving van of inbreuk op de AVG grotendeels afhangt van de manier waarop de klant het product of de oplossing gebruikt.

De AVG heeft invloed op het gebruik van specifieke hosted services
In het geval van hosted services hangt de naleving van de AVG ook samen met de manier waarop de dienst wordt geleverd. Hier is Axis voor verantwoordelijk. Maar de grootste factor voor naleving van of inbreuk op de AVG is afhankelijk van de manier waarop klanten de dienst gebruiken. Per applicatie dienen we te onderzoeken wat voor soort verplichtingen er in verband met de AVG ontstaan en wie verantwoordelijk is.

Laten we bijvoorbeeld eens kijken naar een hosted service, AXIS Guardian. Hieronder geven we aan hoe de AVG doorgaans wordt toegepast en wie verantwoordelijk is voor wat:

> *Klanten van de alarmcentrale* zijn als gegevensverantwoordelijken verantwoordelijk voor persoonsgegevens in het beeldmateriaal dat is vastgelegd door het camerabewakingssysteem van de gebruiker en geüpload in AXIS Guardian.
> De *alarmcentrale* is als gegevensverwerker namens de gebruikers verantwoordelijk voor persoonsgegevens die door de gebruiker in AXIS Guardian zijn geüpload (m.a.w. medewerkersgegevens van de gebruiker en beeldopnames).
> *Axis* is als gegevensverwerker namens de alarmcentrale verantwoordelijk voor persoonsgegevens die door de alarmcentrale zijn geüpload in AXIS Guardian (m.a.w. medewerkersgegevens alarmcentrale) en als subgegevensverwerker namens de alarmcentrale verantwoordelijk voor persoonsgegevens die in AXIS Guardian geüpload zijn door klanten van de alarmcentrale (beeldopnames).
> *Amazon Web Services* is als subgegevensverwerker namens Axis verantwoordelijk voor persoonsgegevens die door de alarmcentrale en klanten van de alarmcentrale (gebruikers) geüpload worden in AXIS Guardian.

2.1 Stappen voor naleving AVG

De AVG is een verordening die invloed zal hebben op de manier waarop organisaties in de toekomst gegevens behandelen, waaronder ook videogegevens.

Elke organisatie die persoonsgegevens verwerkt zal in ieder geval één, maar misschien zelfs meerdere personen aanwijzen die ervoor moeten zorgen dat de organisatie de persoonsgegevens behandelt overeenkomstig de AVG en bedrijfsbeleid. Het aantal uren dat voor deze taak nodig is, hangt uiteraard af van de grootte van de organisatie en de hoeveelheid persoonsgegevens die worden verzameld of verwerkt. Sommige organisaties zullen een functionaris gegevensbescherming (FG) aan moeten stellen om deze taken uit te voeren.

Er zullen ook veranderingen zijn in het administratieve proces. Onder de AVG moeten organisaties hun gegevensverwerkingsactiviteiten gedetailleerd en nauwkeurig bijhouden. Onder meer de volgende gegevens moeten geregistreerd worden:

> De categorie waar de verwerkte persoonsgegevens toe behoren (bijv. klanten, medewerkers, winkelbezoekers, etc.).
> De doelen waar de persoonsgegevens voor gebruikt worden.
> Of de persoonsgegevens worden gedeeld met andere bedrijven binnen of buiten de EU.
> Hoelang de persoonsgegevens bewaard blijven.
> Maatregelen die de organisatie moet nemen in verband met elke afzonderlijke gegevensverwerkingsactiviteit om aan de AVG te voldoen.

Dit zijn allemaal relevante zaken voor de opslag van beelden van een bewakingsvideo.

Organisaties zijn verplicht uit te leggen waarom een videocamera op een bepaalde plek hangt, wat er gefilmd wordt en waarom. In geval van videobewaking is het belangrijk dat de ruimtes waar camera's hangen en de ruimtes er direct omheen, voorzien zijn van de juiste bebording met informatie over het toezicht.

De verwerkingsverantwoordelijke zal wellicht een zogeheten Data Protection Impact Assessment (DPIA), een instrument om de privacyrisico's van gegevensverwerking vooraf in kaart te brengen, uit moeten voeren wanneer een camera wordt opgehangen in een openbare ruimte. Hoewel de exacte inhoud van een DPIA per geval bepaald moet worden, dient deze in ieder geval de volgende informatie te bevatten:

> Een systematische beschrijving van de beoogde verwerkingsactiviteiten en verwerkingsdoelen.
> Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen met betrekking tot het doel.
> Een beoordeling van de privacyrisico's en rechten van de betrokkenen.
> De beoogde maatregelen om de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en aan te tonen dat persoonsgegevens worden beschermd en aan de AVG wordt voldaan. Bedrijven dienen hierbij rekening te houden met de rechten en de legitieme belangen van individuen en andere betrokkenen.

Een van de belangrijkste kenmerken van de nieuwe verordening is dat de personen die gevolgd worden volledig op de hoogte moeten zijn van de gegevens die van hen bewaard worden en waar ze voor gebruikt worden.

De verordening geeft duidelijke regels over encryptie en de manier waarop gegevens beschermd moeten worden. Het feit dat de gegevens in de vorm van videobeelden komen, doet niets af aan deze eisen.

Bedrijven die videobeelden opslaan, hebben daarom duidelijke verantwoordelijkheden wat betreft het opslaan van persoonsgegevens en moeten krachtige maatregelen nemen om ongeautoriseerde toegang te voorkomen. Daarom is het belangrijk om schriftelijk vast te stellen wie toegang heeft tot de camera's en de beelden.

Organisaties moeten een procedure hebben wanneer een persoon zijn/haar recht op inzage wil uitoefenen of een verzoek tot verwijdering van de persoonsgegevens doet. De AVG schrijft namelijk voor dat organisaties binnen één maand aan dit soort verzoeken tegemoet moeten komen. Met een vaste procedure is het makkelijker om aan deze eis te voldoen. Bij dit soort verzoeken mag redelijkerwijs verwacht worden dat de aanvrager voldoende informatie aandraagt om de gevraagde gegevens te vinden, bijvoorbeeld een globaal tijdstip/datum en de locatie waar de beelden zijn opgenomen.

Bedrijven moeten krachtige maatregelen nemen om ongeautoriseerde toegang tot de opgeslagen persoonsgegevens te voorkomen. De manier waarop verschilt per bedrijf en sluit aan op de uitdagingen van de desbetreffende organisatie. Wat alle bedrijven echter wel gemeen hebben, is de noodzaak om strenge beveiligingscontroles uit te voeren en op de hoogte te blijven van best practices in cybersecurity. Bovendien is het cruciaal dat ze samenwerken met vertrouwde partners die veilige hardware en software verkopen en een zorgvuldige nazorg bieden.

3. Conclusie

Uiteindelijk is het de gebruiker van bewakingsapparatuur, -oplossingen en -diensten die verantwoordelijk is voor het naleven van de AVG en het beschermen van de rechten van individuen waarvan de gebruiker persoonsgegevens verwerkt. Organisaties die op dit vlak nog niet veel gedaan hebben, moeten nu snel actie ondernemen. Bedrijven die zich hebben voorbereid en weten wat hun verantwoordelijkheden zijn onder de nieuwe verordening, hoeven zich minder zorgen te maken.

Gebruikers van bewakingsapparatuur, -oplossingen en -diensten zouden dan ook alleen samen moeten werken met aanbieders en leveranciers die de privacy van individuen respecteren en hun persoonsgegevens beschermen. Als een gebruiker van bewakingsapparatuur, -oplossingen en -diensten moet u ook kunnen rekenen op de hulp en technische ondersteuning van uw leveranciers en verkopers, zodat u aan de AVG kunt voldoen.

Additionele bronnen:

Volledige informatie over de AVG

Website van de Europese Toezichthouder voor gegevensbescherming

Website richtlijn gegevensbescherming voor kleine en middelgrote bedrijven

73058/NL/R1/1904

Over Axis Communications

Axis maakt een slimmere en veiligere wereld mogelijk, door netwerkoplossingen te ontwikkelen die inzicht bieden in het verbeteren van de veiligheid en nieuwe manieren van zakendoen. Als marktleider in netwerkvideo biedt Axis producten en diensten voor videobewaking en beeldanalyse, toegangscontrole en audiosystemen. Axis heeft ruim 3.000 toegewijde werknemers in meer dan 50 landen en werkt samen met een wereldwijd netwerk van partners om klantspecifieke oplossingen te leveren. Axis is opgericht in 1984 en heeft zijn hoofdkantoor in Lund, Zweden.

Ga naar onze website www.axis.com voor meer informatie over Axis.

AXIS COMMUNICATIONS