Whitepaper

O que o GDPR significa para Videomonitoramento

Regulamento Geral de Proteção de Dados (GDPR) para aplicações de videomonitoramento

Genetec™

Conteúdo

1

Visão geral do GDPR

O GDPR é um novo conjunto de regras para operações de processamento de dados pessoais realizadas por organizações com residentes da UE que começaram a ser aplicadas em 25 de maio de 2018. O GDPR é a maior mudança no cenário jurídico europeu para proteção de dados desde que a Diretiva de Proteção de Dados da UE foi estabelecida em 1995. Embora baseado na diretiva atual, o GDPR cria novas obrigações complexas para organizações dentro e fora da Europa, e é previsto pelo Gartner que, até o final de 2018, "mais de 50% das empresas afetadas pelo GDPR não estarão em pleno compliance com seus requisitos".

"Gartner diz que as organizações não estão preparadas para o Regulamento Europeu de Proteção de Dados de 2018". 3 de maio de 2017. http://www.gartner.com/newsroom/id/3701117.

O GDPR usa uma abordagem baseada em risco para proteção de dados que exigirá que as organizações avaliem o nível de risco que suas operações de processamento de dados representam para os direitos e liberdades fundamentais dos indivíduos, referidos no GDPR como 'indivíduos-alvo'. Essas regras regerão a coleta, uso e compartilhamento de dados pessoais por ambos os controladores de dados - organizações que coletam dados pessoais para uso próprio - e processadores de dados - organizações que processam dados (o que também inclui a retenção de dados) em nome dos controladores de dados, como provedores de serviços na nuvem. Os dados pessoais incluem nome, endereço residencial, foto, dados bancários, postagens em redes sociais, informações médicas, endereços IP, ID do dispositivo móvel e dados coletados da IoT.

Os direitos dos indivíduos em relação aos seus dados são fundamentais para o novo regulamento. De acordo com o GDPR, o indivíduo ainda é dono ou possui os dados coletados pelo controlador de dados.

De acordo com o regulamento, os controladores de dados são responsáveis por (1) avaliar o nível de risco representado por suas operações de processamento de dados contra os direitos e liberdades fundamentais dos indivíduos e, em seguida, (2) modular seu compliance de acordo com a proteção de dados.

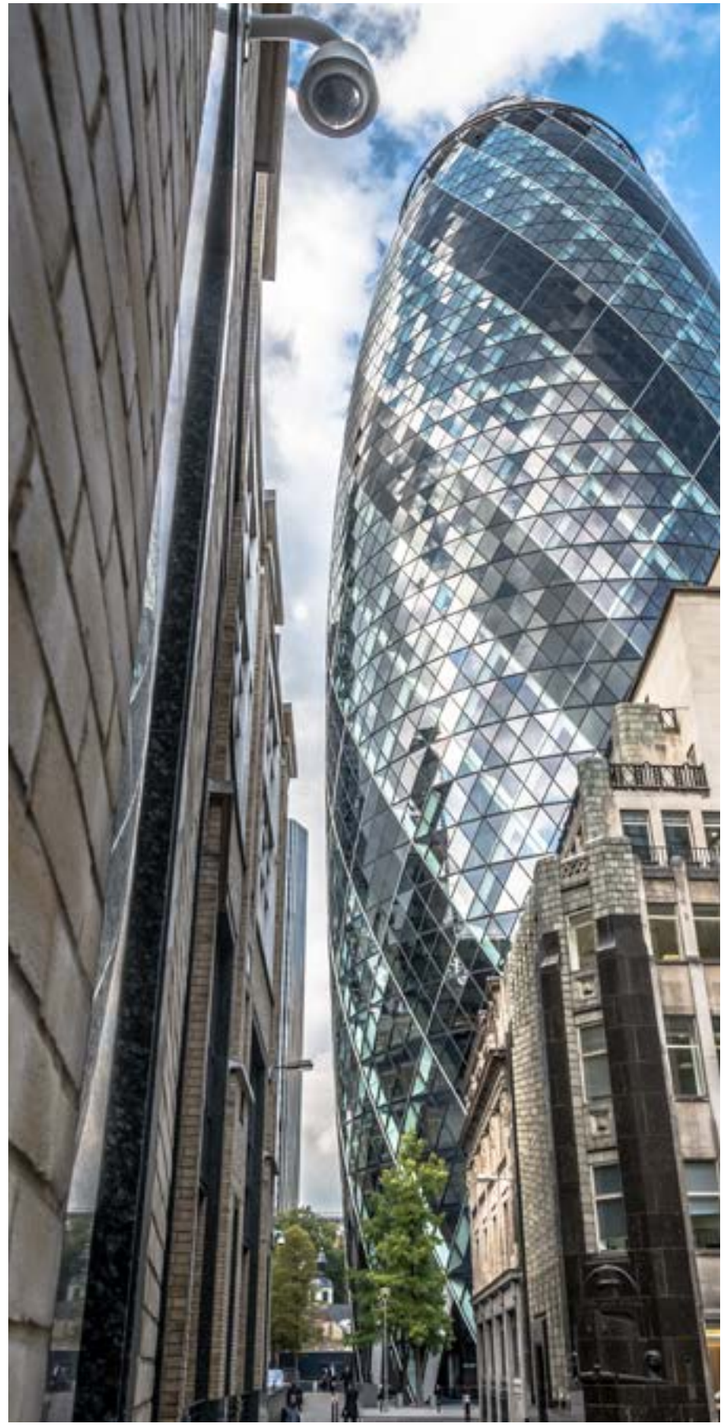
Um dos objetivos deste regulamento é proteger os dados dos indivíduos, obrigando os responsáveis pelo tratamento a gerir os dados de forma segura e a reagir adequadamente em caso de violação de privacidade ou de dados. Para isso, o GDPR exige que os controladores de dados incluam proteção de dados no design e na infraestrutura de seus sistemas; os controladores de dados que não cumprirem os requisitos enfrentarão grandes multas monetárias, ações coletivas e danos à sua reputação. Consequentemente, este novo paradigma na proteção de dados é uma oportunidade para os responsáveis pelo tratamento de dados introduzirem novos sistemas e promoverem a inovação em relação ao tratamento de dados pessoais, especialmente nas áreas de gestão, securitização, anonimização e entrega, com aqueles que estão à frente da curva potencialmente ganhando uma significativa vantagem competitiva.

1.1 O que o GDPR significa para videomonitoramento

Os controladores de dados que executam aplicações de videomonitoramento na UE, incluindo sistemas públicos de videomonitoramento, precisam prestar atenção especial às disposições do GDPR relacionadas à identificação, gerenciamento e mitigação de riscos. Embora o GDPR não faça referência específica a aplicações de videomonitoramento, os princípios gerais de proteção de dados

Whitepaper / O que o GDPR significa para videomonitoramento

O GDPR é a maior mudança no cenário jurídico europeu para proteção de dados desde que a Diretiva de Proteção de Dados da UE foi estabelecida em 1995.



2

As implicações para o videomonitoramento relativo a direitos e deveres no GDPR

do GDPR se aplicam a ele. As Agências Europeias de Proteção de Dados (DPA) classificam o videomonitoramento que envolve o monitoramento de áreas públicas em grande escala como uma 'operação de processamento de alto risco'. Como resultado, os controladores de dados que fazem uso de videomonitoramento na UE terão que realizar tarefas muito específicas, incluindo avaliações de risco, garantir a privacidade desde o design em seus sistemas e desenvolver sinalização adequada.

Ao determinar uma estratégia de compliance para seus sistemas, os controladores de dados têm a opção de (1) criar suas próprias soluções on-premises ou (2) terceirizar o processamento de dados. Em ambos os casos, os controladores de dados precisam encontrar uma solução que possa ajudá-los a cumprir suas obrigações do GDPR de entregar quaisquer dados coletados de um indivíduo a esse mesmo indivíduo mediante solicitação.

Um parceiro confiável que entende de videomonitoramento e questões de privacidade e proteção de dados pode ser vital para obter total compliance com o GDPR para aplicações de videomonitoramento. Os controladores de dados que desejam criar suas próprias aplicações de videomonitoramento compatíveis

on-premises precisarão considerar maneiras de fortalecer seus sistemas e encontrar soluções que ofereçam funcionalidades integradas como criptografia, autenticação e anonimização para assegurar o compliance. Aqueles que desejam terceirizar suas operações de processamento de dados para um processador de dados, precisarão fazer parceria com uma organização que ofereça soluções que possam ajudá-los a se ficarem totalmente em compliance com os requisitos do GDPR.

OGDPR é diferente da atual Diretiva Européia em vários aspectos importantes, especialmente no que se refere a 'operações de processamento de alto risco', como videomonitoramento. Primeiro, o GDPR amplia consideravelmente o escopo das atuais leis de proteção de dados da UE e concede aos indivíduos da UE uma variedade de novos direitos. Em segundo lugar, exige maior responsabilidade dos controladores de dados do que a lei atual em relação a questões importantes como avisos de privacidade e violações de dados e, em certas circunstâncias, exige que os coletores ou processadores de dados indiquem um Agente de Proteção de Dados (DPO). O GDPR também impõe obrigações específicas aos processadores de dados, incluindo provedores de serviços na nuvem, consagra o conceito de privacidade por design na legislação e exige penalidades severas por não compliance.

De acordo com o GDPR, o consentimento de um indivíduo, que é uma das inúmeras bases legais para o processamento, deve ser dado livremente, específico, informado e inequívoco.

2.1 Escopo expandido

A jurisdição estendida é uma das mudanças mais significativas introduzidas pelo GDPR. Em particular, o GDPR se aplica às operações de processamento de dados pessoais de indivíduos pelas seguintes organizações:

1. Controladores de dados e processadores de dados sediados na UE, independentemente do processamento ocorrer na UE ou não
2. Fornecedores de bens e serviços sediadas no exterior mas que operam na UE (independentemente de pagamento obrigatório)
3. Organizações sediadas no exterior que monitoram o comportamento dos residentes da UE

2.2 Novos direitos para indivíduos

Os indivíduos recebem direitos mais robustos e amplos sob o GDPR, que podem ser resumidos da seguinte forma:

2.2.1 Avisos de privacidade e consentimentos

Para tornar os controladores de dados mais transparentes sobre sua coleta e uso de dados, o GDPR exige que eles publiquem avisos de privacidade informando a identidade do controlador de dados e fornecendo informações sobre a natureza da operação de processamento de dados realizada. Os avisos de privacidade devem conter divulgações extensas e prescritas, incluindo

- detalhes de contato do controlador de dados
- finalidade do processamento
- com quem os dados serão compartilhados
- detalhes de qualquer transferência de dados fora da UE
- por quanto tempo os dados serão guardados
- quais são os direitos de um indivíduo
- como fazer uma reclamação

Os avisos devem ser claros e apresentados de forma fácil de ler; termos longos e ilegíveis em juridiquês serão proibidos.

Os avisos também devem ser concisos, o que claramente representa um desafio para os avisos sobre videomonitoramento. Os DPAs europeus favorecem avisos em camadas que fornecem informações básicas antecipadamente com links para informações mais completas para quem as deseja. Portanto, os provedores de videomonitoramento que desejam evitar um aviso grande exibindo todas as informações acima podem usar um aviso pequeno indicando quem são e por que estão capturando imagens junto com um URL ou número de telefone para indivíduos interessados em obter o aviso completo.

O regulamento também vale para aplicações de videomonitoramento em que um controlador de dados usa a plataforma de gerenciamento de vídeo de outro controlador de dados para obter maior consciência situacional. Por exemplo, os sistemas de vigilância da cidade estão sendo cada vez mais construídos usando uma abordagem colaborativa que integra sistemas e compartilha as informações desses sistemas com terceiros. Nesses casos, o coletor de dados que coleta os dados iniciais também precisará fornecer informações de contato para terceiros que tenham acesso aos dados. Além disso, esses terceiros também precisarão gerenciar e proteger adequadamente os dados coletados.

De acordo com o GDPR, o consentimento de um indivíduo, que é uma das inúmeras bases legais para o processamento, deve ser dado livremente, específico, informado e inequívoco. Como resultado, o silêncio ou as caixas pré-selecionadas para inferir o consentimento serão proibidos. De acordo com o GDPR, deve ser tão fácil para os indivíduos remover o consentimento quanto para eles.

2.2.2 Direito de acesso

O novo regulamento aumenta muito a transparência dos dados, ao mesmo tempo que dá maior poder aos indivíduos. De acordo com o GDPR, os indivíduos têm o direito de obter confirmação sobre se seus dados estão ou não sendo processados, onde estão sendo processados e para qual finalidade. Além disso, o controlador de dados deverá enviar, gratuitamente, uma cópia (inclusive em formato eletrônico) dos dados pessoais ao indivíduo mediante solicitação. O GDPR também apresenta uma nova recomendação de práticas recomendadas de que, sempre que possível, as organizações devem ser capazes de fornecer acesso remoto a um sistema de autoatendimento seguro que forneceria aos indivíduos acesso direto às suas informações.

No caso de videomonitoramento, os controladores de dados precisarão ter sistemas para reconhecer solicitações, avaliar sua validade e fornecer as informações dentro de um mês. Isso pode ser especialmente desafiador para sistemas de videomonitoramento nos casos em que um indivíduo solicita cópias de vídeo em que a identidade de outros indivíduos incluídos na filmagem precisa ser mascarada ou protegida de outra forma.

2.2.3 Direito ao apagamento (ou ao esquecimento)

Os indivíduos poderão solicitar que seus dados sejam apagados, opor-se ao processamento ou restringir o processamento de seus dados. As condições para o apagamento incluem (1) quando os dados não são mais relevantes em relação à intenção original das operações de processamento e (2) quando o processamento foi originalmente baseado em consentimento e, em seguida, os indivíduos retiram seu consentimento.

O GDPR também introduzirá um sistema escalonado de multas para controladores e processadores que podem chegar a 4% do faturamento anual ou €20 milhões, o que for maior.

Whitepaper / O que o GDPR significa para videomonitoramento

3

Migrando para um sistema de videomonitoramento em compliance com o GDPR

2.2.4 Direito à portabilidade de dados

Os indivíduos podem pedir para receber seus dados e transferi-los para um novo controlador de dados. Os controladores de dados devem fornecer os dados em um formato legível por máquina comumente usado. Os indivíduos também podem solicitar que seus dados sejam transferidos diretamente para um novo controlador de dados.

2.2.5 Notificação de violação

O GDPR impõe uma regra obrigatória de relatório de violação de dados aos controladores de dados. As violações devem ser relatadas aos DPAs da UE dentro de 72 horas após o controlador de dados tomar conhecimento da violação. Os processadores de dados também serão obrigados a notificar os controladores de dados - que são seus clientes - sobre violações de dados "sem atrasos indevidos".

Além disso, se um controlador de dados determinar que uma violação de dados provavelmente representa um alto risco para os direitos e liberdades dos indivíduos, o controlador de dados também deverá notificar os indivíduos afetados “sem demora injustificada”. No entanto, o GDPR contém uma exceção a esse requisito de

A Genetec pode fornecer aos controladores de dados informações valiosas sobre a extensão de suas obrigações com o GDPR

notificar os indivíduos afetados e se aplica a controladores de dados que tornam seus dados ininteligíveis para pessoas não autorizadas por meio da implementação de medidas de proteção técnica e organizacional apropriadas, incluindo criptografia e anonimização.

2.3. Responsabilidade e nomeação de DPOs

Atualmente, os controladores de dados devem se registrar no DPA local. Embora esse requisito irá desaparecer, o GDPR impõe novos requisitos de manutenção de registros aos controladores e processadores de dados. Os controladores de dados também serão obrigados a realizar uma Avaliação de Impacto na Proteção de Dados (DPIA) e consultar o DPA nos casos em que o processamento for de alto risco. As organizações também terão que nomear um DPO em casos de processamento de dados de alto risco, incluindo aplicações de videomonitoramento que envolvam o monitoramento sistemático de uma área pública em grande escala - por exemplo, no caso de sistemas de vigilância em toda a cidade ou um campus.

2.4 Privacidade por design

Sob o GDPR, a privacidade deve ser por design em vez de 'adicionada'. A obrigação de privacidade por design no GDPR exige uma abordagem de engenharia de sistemas em que os princípios de proteção de dados, como criptografia e anonimização de imagens de vídeo, por exemplo, sejam incluídos desde o início em qualquer design de sistema.

Além disso, os controladores de dados também serão responsáveis por garantir que, por padrão, a quantidade mínima de dados seja coletada. Os sistemas de videomonitoramento que gravam constantemente e armazenam imagens indefinidamente violarão esta disposição; como resultado, os controladores de dados precisarão adotar sistemas de videomonitoramento com uma interface rica em recursos que ofereça flexibilidade nas operações de gravação de vídeo que lhes permita controlar por quanto tempo as imagens ficarão retidas.

2.5 Obrigações específicas para processadores de dados

Conforme mencionado anteriormente, os controladores de dados podem decidir terceirizar suas operações de processamento de dados usando soluções de terceiros. Nesses casos, o GDPR exige que os controladores de dados estabeleçam certos termos com seus processadores de dados, incluindo

1. a obrigação de ajudar o controlador a cumprir suas obrigações relativas ao GDPR
2. a obrigação de processar apenas de acordo com as instruções do controlador
3. a obrigação de não contratar os serviços de um subprocessador sem permissão e fornecer ao controlador direitos de auditoria contratuais

2.6 Penalidades

O GDPR também introduzirá um sistema escalonado de multas para controladores e processadores que podem chegar a 4% do faturamento anual ou €20 milhões, o que for maior. O percentual da multa será medido em relação à receita bruta de todo o grupo e não em relação ao lucro líquido. O GDPR também permitirá que indivíduos prejudicados por uma violação ajuizem ações civis.

Esta seção (1) fornece aos controladores de dados uma série de considerações importantes destinadas a tornar a transição para um sistema de videomonitoramento compatível com GDPR o mais eficiente operacionalmente possível e (2) considera diferentes soluções ou funcionalidades para criar plataformas de vídeo de ponta a ponta mais resilientes.

No que diz respeito a compliance com o GDPR, os controladores de dados precisam prestar atenção especial ao videomonitoramento como uma operação de processamento de dados devido ao seu contexto e escala e à sua natureza intrusiva. Os sistemas de videomonitoramento em grande escala serão definidos como operações de processamento de alto risco sob o GDPR e exigirão tratamento especial.

Depois de avaliar o nível de risco envolvido em suas aplicações de videomonitoramento, os controladores de dados devem pensar em como proteger seus sistemas contra violações de dados e realizar uma avaliação completa do fluxo de dados através dos três estágios de suas operações de processamento de dados - desde a coleta e processamento até a restituição.

Os controladores de dados também devem revisar como processarão os direitos dos indivíduos, especialmente em relação aos direitos de solicitar imagens capturadas. Essas solicitações podem custar caro em termos de tempo necessário para coletar e anonimizar os dados. A tecnologia certa pode reduzir significativamente o impacto e o custo geral dessa obrigação.

E, finalmente, os controladores de dados devem considerar como um processador de dados pode ajudá-los a alcançar o compliance para suas aplicações de videomonitoramento, fornecendo a infraestrutura apropriada.

Como um parceiro de confiança, a Genetec pode fornecer aos controladores de dados informações valiosas sobre a extensão de suas obrigações com o GDPR e sobre a melhor forma de projetar e desenvolver seus sistemas de vídeo para atender a essas obrigações. A Genetec também oferece soluções de ponta a ponta on-premises e SaaS que podem ajudar os controladores de dados a obter compliance com GDPR com suas responsabilidades básicas e estendidas em relação às operações de processamento de dados de alto risco para videomonitoramento.

3.1 Nível de risco

Para os controladores de dados que usam aplicações de videomonitoramento para indivíduos da UE, o primeiro passo para garantir compliance com o GDPR é realizar um DPIA para determinar se o processamento “tem probabilidade de resultar em alto risco para os direitos e liberdade dos indivíduos”.

Os controladores de dados devem primeiro consultar o Artigo 35 para determinar o nível de risco associado às suas aplicações específicas de videomonitoramento. Os tipos de processamento que podem resultar em alto risco para os direitos e liberdade dos indivíduos são aqueles que envolvem

- uma avaliação sistemática e extensa de aspectos pessoais relacionados a assuntos naturais, que incluiria reconhecimento facial para fins de criação de perfil e Reconhecimento Automático de Placas de Veículos (ALPR)
- um monitoramento sistemático e em larga escala de uma área acessível ao público, incluindo cidades, aeroportos, lojas e hotéis.

Se os controladores de dados estiverem operando esses sistemas de alto risco, eles terão que nomear um DPO e podem exigir o consentimento do DPA antes de prosseguir.

3.2 Obrigações com violação de dados do GDPR

A mudança para compliance com o GDPR começa antes da implementação do próprio sistema de videomonitoramento, e os controladores de dados precisam começar pensando em como fortalecer seus sistemas contra violações de dados. Independentemente da sensibilidade dos dados coletados, uma violação de dados pode:

- afetar negativamente a reputação e prejudicar o reconhecimento da marca
- aumentar significativamente os custos operacionais à medida que os controladores de dados trabalham para reparar a violação e garantir que seus sistemas estejam limpos
- resultar em grandes multas monetárias

A capacidade dos controladores de dados de responder efetivamente a uma violação de dados intencional ou não intencional será uma parte importante do processo de avaliação de risco, pois o GDPR exige que os controladores de dados relatem violações dentro de 72 horas após a descoberta.

Dependendo da implementação de um sistema de videomonitoramento e de quem participa da sua gestão, será necessário implementar um processo de comunicação eficaz, bem como ferramentas apropriadas para reportar violações de dados em qualquer componente do sistema. A rastreabilidade de todas as operações por meio de registros e relatórios, bem como a cadeia de custódia quando uma série de vídeos se tornarem evidenciais, serão funcionalidades importantes para obter compliance. E, para ajudar a proteger os direitos e a privacidade dos indivíduos cujos dados estão sendo coletados, os controladores de dados também podem implementar medidas de proteção técnica e organizacional, incluindo criptografia e anonimização, que tornam os dados ininteligíveis para pessoas não autorizadas. Com esses processos, ferramentas e medidas de proteção de dados, os controladores de dados podem investigar efetivamente a causa de uma violação, bem como demonstrar seu compromisso com o gerenciamento de dados de forma responsável.

Soluções on-premises e SaaS da Genetec: A 'Segurança da Segurança' está no centro de nossa estratégia proativa para evitar violações de dados e acesso não autorizado a informações pessoais. Os produtos Genetec usam criptografia e autenticação baseada em reivindicações, fornecem uma funcionalidade de gerenciamento de autorização e oferecem anonimização dinâmica que torna

4

Conclusão

automaticamente anônimos os indivíduos em vídeo ao vivo e gravado ao monitorar ações e movimentos.

3.3 Compliance com GDPR e fluxo de dados

3.3.1 Coleta

A coleta refere-se ao registro real das informações e, nesta fase, os controladores de dados são responsáveis por garantir que seus sistemas conseguem manter a integridade dos dados. Se uma operação de processamento de dados for de alto risco, os controladores de dados devem considerar criptografar ou anonimizar o fluxo de vídeo.

Por exemplo, para proteger os direitos dos indivíduos consagrados no GDPR, os controladores de dados podem criptografar os dados que coletam. Quando os dados são criptografados, mesmo que uma pessoa ou entidade não autorizada obtenha acesso aos dados, eles não podem ser lidos sem a chave de descriptografia apropriada. Tanto quanto os dados estão armazenados ou em transferência de uma câmera, a criptografia protege os dados confidenciais e aprimora a comunicação entre clientes e servidores. Outras medidas eficazes que podem ajudar a tornar um sistema de videomonitoramento resiliente e seguro são autenticação, autorização e aplicação de senha.

Um sistema de videomonitoramento pode garantir que a identidade dos indivíduos permaneça anônima de três maneiras:

1. Mascaramento permanente, que envolve a anonimização permanente de indivíduos em imagens de vídeo e significa que o mascaramento não pode ser removido
2. Anonimização dinâmica, que é o processo pelo qual um software, monitorando ações e movimentos, anonimiza automaticamente os indivíduos em vídeo ao vivo e gravado.

3. Edição, que envolve ocultar a identidade apenas de pessoas selecionadas nas imagens de vídeo e que geralmente é feita após o fato quando uma organização deseja compartilhar o vídeo com as autoridades

Soluções on-premises da Genetec: O Genetec Security Center oferece métodos de criptografia e autenticação para garantir que apenas pessoal autorizado possa ter acesso ao sistema de segurança de um controlador de dados. Com o Security Center, os controladores de dados podem implementar novos níveis de comunicação criptografada entre todos os componentes do sistema e usar certificados digitais para garantir a confiança em seus sistemas. O Security Center também pode autenticar comunicações dentro do sistema, validando e garantindo que dados e vídeos não sejam trocados com fontes externas.

Oferecendo anonimização dinâmica que torna automaticamente anônimos indivíduos em vídeo ao vivo e gravado ao monitorar ações e movimentos, o Security Center também pode ajudar os controladores de dados a obter compliance ao realizar o videomonitoramento de espaços públicos. O KiwiVision™ Privacy Protector™ permite que o vídeo bruto seja criptografado e gravado em segundo plano e depois descriptografado por pessoal autorizado. Os controladores de dados podem aplicar o Privacy Protector apenas às câmeras envolvidas no processamento de alto risco e podem escolher o nível ideal de anonimização para cada situação. Com apenas alguns cliques, eles podem pixelizar, desfocar ou obscurecer completamente indivíduos e objetos no campo de visão de uma câmera.

Soluções SaaS Genetec: Os controladores de dados podem obter compliance com o GDPR em relação à integridade dos dados durante a coleta, implantando o Genetec Stratocast™. E, para obter compliance com a edição para exportações de vídeo, a solução Genetec Clearance™ Case Management as a Service fornece aos controladores de dados as ferramentas necessárias para realizar a tarefa de maneira eficiente e oportuna.

3.3.2 Processamento

Processamento refere-se à operação de processamento de dados real realizada pelo coletor de dados. Uma disposição fundamental no GDPR é que os controladores de dados serão responsáveis por vigiar o acesso aos dados coletados em seus sistemas. Isso é importante tanto para a privacidade quanto para o gerenciamento de possíveis violações de dados, pois o gerenciamento adequado dos direitos de acesso pode ajudar a reduzir as chances de uma violação de dados não intencional.

Autenticação e autorização são duas formas ideais para os controladores de dados controlarem quem pode acessar o vídeo e os dados

coletados em seus sistemas. Os controladores de dados podem proteger o acesso aos seus sistemas por meio de mecanismos de autenticação que garantem que os funcionários acessem o sistema correto quando fizerem login. A autenticação usa certificados, combinações de nome de usuário/senha e tokens para impedir que criminosos cibernéticos finjam ser um servidor de segurança para penetrar em um sistema de segurança e manipular, copiar ou assumir o controle dos dados. A autorização envolve controlar quem vê os dados em um sistema e o que eles podem fazer com esses dados. Com recursos de autorização, os controladores de dados podem restringir o escopo da atividade em seu sistema, concedendo direitos de acesso a grupos ou indivíduos para recursos, dados ou aplicações e definindo o que os usuários podem fazer com os recursos, garantindo assim a segurança dos dados transmitidos e armazenados em seus sistemas.

Soluções on-premises e SaaS da Genetec: As soluções da Genetec oferecem privilégios detalhados de acesso ao usuário para ajudar a proteger a privacidade, definindo claramente como o pessoal autorizado tem acesso a dados específicos e se podem modificar esses dados ou o comportamento do sistema.

3.3.3 Restituição

A restituição refere-se ao gerenciamento do ciclo de vida dos dados coletados e ao requisito do GDPR de que os controladores de dados devem, mediante solicitação, fornecer cópias digitais de dados pessoais a indivíduos. Esta é uma parte muito importante do GDPR, pois os indivíduos têm o direito de solicitar uma cópia de seus próprios dados.

Na maioria dos casos, os controladores de dados devem fornecer esse serviço gratuitamente e devem garantir que, ao atender tais solicitações, elas não afetem os direitos e a liberdade de terceiros. Uma maneira de obter compliance ao considerar a portabilidade de dados seria os controladores de dados fornecerem cópias digitais das informações por meio de um quiosque de autoatendimento. No entanto, como um problema comum com videomonitoramento é a presença de muitos indivíduos em qualquer parte da filmagem, a anonimização do vídeo que protege a liberdade e os direitos de privacidade de outros indivíduos será essencial. Além disso, como resultado do direito de um indivíduo ao apagamento, os controladores de dados precisam prestar muita atenção ao gerenciamento de seus arquivos, pois podem ser obrigados a isolar e apagar dados específicos.

Soluções on-premises e SaaS da Genetec: Para cumprir suas obrigações de restituição, os controladores de dados precisarão primeiro identificar as imagens nas quais o indivíduo está presente.

Seja por meio de suas ofertas padrão ou por meio de parceiros de tecnologia, a Genetec oferece uma série de ferramentas que podem facilitar muito a busca, identificação e coleta de informações registradas de um indivíduo.

Para a restituição em si, os controladores de dados podem implantar o Genetec Clearance em seus sistemas de videomonitoramento para reconhecer solicitações de dados de indivíduos, avaliar sua validade e fornecer as informações/serviços dentro de um mês. Essa solução de arquitetura aberta baseada na nuvem apresenta criptografia, coleta de vídeo centralizada e pesquisa avançada, essenciais para o gerenciamento eficiente e seguro de dados de vídeo de 'alto risco'. Com recursos de edição de vídeo integrados que mascaram a identidade de todos os indivíduos capturados por câmeras de vídeo, os controladores de dados também podem usar o Genetec Clearance para desenvolver um portal de autoatendimento de acesso remoto onde os indivíduos podem acessar diretamente seus dados pessoais.

3.3.4 Ferramentas para apoiar os Agentes de Proteção de Dados (DPOs)

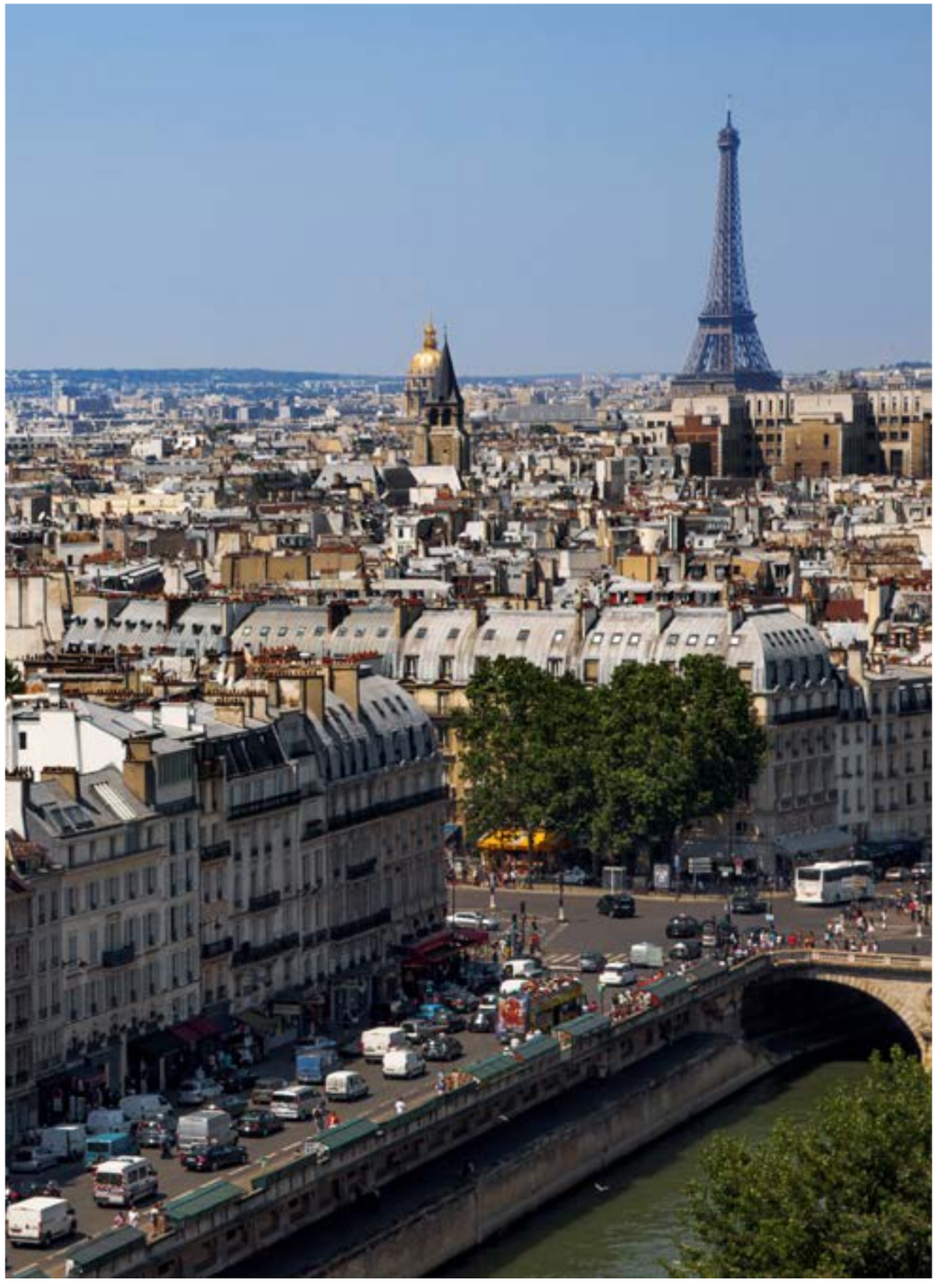
Os controladores de dados podem ter que nomear um DPO para monitorar seu compliance em relação às suas obrigações do GDPR. Será vital que os controladores de dados tenham acesso às informações corretas e, se nomeado, o DPO precisará mostrar as medidas tomadas pelo controlador de dados para proteger as informações coletadas.

Soluções on-premises e SaaS da Genetec: As soluções da Genetec oferecem vários registros e, mais importante, uma plataforma de relatórios robusta que pode ajudar os controladores de dados e DPOs a monitorar o estado de seus sistemas de videomonitoramento ou a realizar pesquisas sobre quem teve acesso e/ou baixou informações de seus sistemas.

O GDPR entrou em vigor em 25 de maio de 2018, e todas as organizações que fazem uso de aplicações de videomonitoramento para indivíduos-alvo na UE, especialmente em áreas públicas, precisarão garantir que seus sistemas atendam às obrigações de privacidade por design estabelecidas no regulamento. As organizações também terão que respeitar os direitos dos indivíduos conforme consagrados no GDPR, incluindo o direito de acesso às informações coletadas. Além disso, as organizações precisarão monitorar e manter a integridade dos dados coletados e precisarão informar os DPAs sobre uma violação dentro de 72 horas. O não cumprimento prejudicará a reputação de uma organização e resultará em elevadas multas monetárias.

A Genetec pode orientar as organizações para compliance com o GDPR com suas soluções locais ou, contratadas para atuar como processadora de dados, com seu portfólio de soluções SaaS. A Genetec também pode ajudar as organizações a reduzir os custos operacionais associados a suas aplicações de videomonitoramento, fornecendo ferramentas de pesquisa e edição.

Whitepaper / O que o GDPR significa para videomonitoramento



Fundada em 1997, a Genetec é líder global em plataformas de segurança unificadas, com uma ampla oferta para uma variedade de especialidades de segurança.

Videomonitoramento: Obtenha uma maior consciência situacional e aumente a segurança em sua cidade com a capacidade de compartilhar câmeras entre agências e organizações, fornecendo uma imagem operacional em comum e melhorando o tempo de resposta a incidentes.

Controle de acesso: Aumente a segurança da sua organização de forma eficaz responda às ameaças e tome
decisões mais claras e oportunas usando uma plataforma unificada e pronta para IP,
tanto na implantação de um novo sistema de controle de acesso ou para atualizar uma
instalação existente.

Reconhecimento automático de placas de veículos: Automatize a detecção de veículos de interesse, aumente a eficiência da fiscalização em estacionamentos e acelere as investigações de segurança pública por meio da capacidade de compartilhar informações de placas de veículos com agências selecionadas e organizações parceiras, sem violar propriedade e privacidade.**Suporte à decisão operacional:** Gere mais eficiência no tratamento de incidentes e tomada de decisões através de fluxos de trabalho avançados que
guiam os operadores durante alertas de situação por meio de procedimentos baseados em políticas para exportação de compilação detalhada de casos.

Gerenciamento de caso investigativo: Simplifique o gerenciamento de casos e acelere as investigações com uma plataforma que permite centralizar evidências digitais e colaborar de forma segura com investigadores, agências externas e o público.

Serviços na nuvem: Estenda os recursos do seu sistema de segurança on-premises e reduza os custos de TI com serviços na nuvem altamente escalável, on-demand que capacitam sua cidade a lidar facilmente com os requisitos de segurança em rápida mudança e operar com maior eficiência.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec