Whitepaper

Was die DSGVO für Videoüberwachung bedeutet

Schutz der Privatsphäre gemäß Datenschutz-Grundverordnung (DSGVO) für Anwendungen zur Videoüberwachung

Genetec™

Inhalt

1

DSGVO im Überblick

Die DSGVO enthält neue Regeln zur Verarbeitung personenbezogener Daten von EU-Bürgern durch Organisationen. Diese Verordnung tritt am 25. Mai 2018 in Kraft. Sie stellt die größte Veränderung im Bereich des EU-Datenschutzrechts seit Einführung der EU-Datenschutzrichtlinie im Jahr 1995 dar. Die DSGVO basiert zwar auf der aktuellen Richtlinie, bringt jedoch neue komplexe Verpflichtungen für Organisationen innerhalb und außerhalb Europas mit sich. Laut Gartner ist davon auszugehen, dass bis Ende 2018 „über 50 Prozent der von der DSGVO betroffenen Unternehmen die Anforderungen der Verordnung nicht vollständig erfüllt haben werden“.

„Gartner: Organisationen sind auf die Einführung der EU-Datenschutz-Grundverordnung im Jahr 2018 nicht vorbereitet“. 3. Mai 2017. http://www.gartner.com/newsroom/id/3701117.

Bei der DSGVO wird der Datenschutz unter dem Risikoaspekt betrachtet. Demnach müssen Organisationen beurteilen, wie hoch das Risiko ihrer Datenverarbeitungsprozesse im Hinblick auf die Grundrechte und -freiheiten von Personen - in der DSBVO als „betroffene Personen“ bezeichnet - ist. Darunter fallen die Erhebung, Nutzung und Weitergabe personenbezogener Daten durch Datenverantwortliche – Organisationen, die personenbezogene Daten zur eigenen Nutzung erheben – sowie Datenverarbeiter – Organisationen, die Daten im Auftrag von Datenverantwortlichen, zum Beispiel Anbieter von Clouddiensten, verarbeiten (einschließlich Datenbesitz). Personenbezogene Daten sind unter anderem Name, Anschrift, Foto, Bankinformationen, Beiträge in sozialen Netzwerken, medizinische Informationen, IP-Adressen, Mobilgeräte-ID sowie über das IoT erfasste Daten.

Die Rechte von Personen in Bezug auf ihre Daten sind ein wesentlicher Bestandteil der neuen Verordnung. Nach Maßgabe der DSGVO bleibt die betroffene Person Eigentümer der vom Datenverantwortlichen erhobenen Daten.

Laut der Verordnung müssen Datenverantwortliche (1) die Höhe des Risikos beurteilen, das ihre Datenverarbeitungsprozesse für die Grundrechte und -freiheiten der Personen darstellen und anschließend (2) die zur Einhaltung der Datenschutzbestimmungen erforderlichen Änderungen vornehmen.

Diese Verordnung zielt unter anderem darauf ab, Daten von Personen zu schützen, indem die Datenverantwortlichen zu einem sicheren Umgang mit den Daten sowie zu geeigneten Maßnahmen bei Verstößen gegen den Schutz oder die Sicherheit der Daten verpflichtet werden. Zu diesem Zweck sind Datenverantwortliche gemäß DSGVO verpflichtet, bei der Konzeption und Infrastruktur ihrer Systeme auf Datenschutz zu achten. Datenverantwortliche, die dagegen verstoßen, müssen mit hohen Geldstrafen, Sammelklagen und Rufschädigung rechnen. Folglich bietet dieses neue Datenschutzmodell den Datenverantwortlichen die Gelegenheit, neue Systeme einzuführen und innovative Lösungen im Hinblick auf den Umgang mit personenbezogenen Daten zu fördern, insbesondere in Bereichen wie Verwaltung, Sicherung, Anonymisierung und Bereitstellung. Wer dies zügig umsetzt, kann einen erheblichen Wettbewerbsvorteil erlangen.

1.1 Was die DSGVO für Videoüberwachung bedeutet

Datenverantwortliche, die Anwendungen zur Videoüberwachung in der EU nutzen, darunter auch öffentliche Videoüberwachungssysteme, müssen ganz besonders auf die DSGVO-Bestimmungen zu Erkennung, Management und Minderung von Risiken achten.

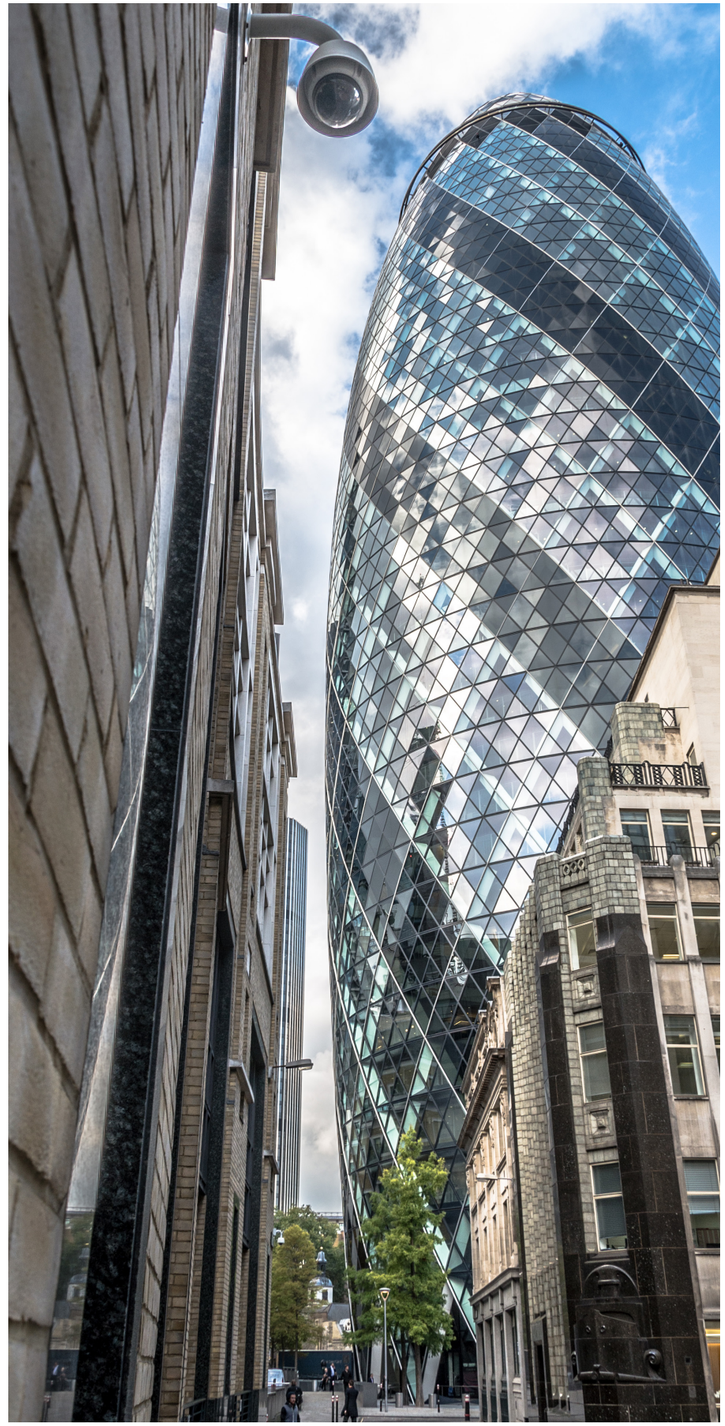
In der DSGVO wird zwar nicht konkret auf Anwendungen zur Videoüberwachung Bezug genommen, es gelten jedoch auch hier die allgemeinen Datenschutzgrundsätze der DSGVO. Die europäischen Datenschutzbehörden stufen die Form der Videoüberwachung, bei der öffentliche Bereiche überwacht werden, auf breiter Basis als „Verarbeitungsvorgang mit hohem Risiko“ ein. Dementsprechend müssen Datenverantwortliche, die in der EU von der Videoüberwachung Gebrauch machen, sehr spezifische Aufgaben – darunter Risikobeurteilungen – ausführen, um einen „eingebauten Datenschutz“ (Privacy by design) sicherzustellen und für geeignete Kennzeichnungen zu sorgen.

Bei der Ausarbeitung einer Compliance-Strategie für ihre Systeme müssen Datenverantwortliche die Möglichkeit haben, (1) eigene standortgebundene Lösungen zu entwickeln oder (2) einen externen Anbieter mit der Datenverarbeitung zu beauftragen. In beiden Fällen müssen die Datenverantwortlichen eine Lösung finden, die ihnen bei der Erfüllung ihrer Verpflichtungen laut DSGVO – wonach einer Person auf Anfrage sämtliche über diese Person erhobenen Daten bereitgestellt werden müssen – hilft.

Ein bewährter Partner, der sich mit Videoüberwachung und den Herausforderungen des Datenschutzes auskennt, kann entscheidend dazu beitragen, dass die DSGVO-Bestimmungen beim Einsatz von Videoüberwachungslösungen komplett eingehalten werden. Datenverantwortliche, die standorteigene, DSGVO-konforme Videoüberwachungsanwendungen entwickeln möchten, müssen überlegen, wie sie ihre Systeme härten können. Zudem müssen sie Lösungen finden, die über integrierte Funktionen wie Verschlüsselung, Authentifizierung und Anonymisierung verfügen, damit die Bestimmungen in jedem Fall eingehalten werden. Wer die Vergabe an einen externen Datenverarbeiter bevorzugt, muss mit einer Organisation zusammenarbeiten, deren Lösungen dazu beitragen, eine vollständige Compliance mit den DSGVO-Anforderungen herzustellen.

Whitepaper/Was die DSGVO für Videoüberwachung bedeutet

Die DSGVO stellt die größte Veränderung im Bereich des EU-Datenschutzrechts seit Einführung der EU-Datenschutz-richtlinie im Jahr 1995 dar.



2

Auswirkungen der Rechte und Pflichten aus der DSGVO auf Videoüberwachung

Die DSGVO unterscheidet sich in vielerlei Hinsicht von der aktuellen europäischen Richtlinie, vor allem aufgrund des Bezugs zu „Verarbeitungsvorgängen mit hohem Risiko“ wie Videoüberwachung. Erstens wird durch die DSGVO der Geltungsbereich der derzeitigen EU-Datenschutzgesetze in erheblichem Maße erweitert und EU-Bürgern wird eine Reihe neuer Rechte gewährt. Zweitens erfordert die neue Verordnung im Vergleich zum aktuellen Recht bei Kernaspekten wie Datenschutzhinweisen und -verstößen ein größeres Verantwortungsbewusstsein unter Datenverantwortlichen. Unter bestimmten Umständen müssen die Datenverantwortlichen oder -verarbeiter Datenschutzbeauftragte benennen. Die DSGVO legt außerdem Datenverarbeitern spezifische Verpflichtungen auf, darunter auch Anbietern von Clouddiensten, verankert das Konzept eines „eingebauten Datenschutzes“ im Gesetz und fordert harte Strafen bei Verstößen.

2.1 Größerer Geltungsbereich

Zu den wesentlichen Änderungen, die mit der DSGVO einhergehen, gehört der erweiterte Geltungsbereich. Insbesondere bezieht sich die DSGVO auf Prozesse zur Verarbeitung personenbezogener Daten durch folgende Organisationen:

1. In der EU ansässige Datenverantwortliche und Datenverarbeiter, unabhängig davon, ob die Daten in der EU verarbeitet werden oder nicht
2. Nicht in der EU ansässige Organisationen, die Güter und Dienstleistungen in der EU anbieten (unabhängig davon, ob eine Zahlung erforderlich ist)
3. Nicht in der EU ansässige Organisationen, die das Verhalten von EU-Bürgern überwachen

2.2 Neue Rechte für Personen

Personen werden unter der DSGVO stärkere und umfassendere Rechte gewährt, die wie folgt zusammengefasst werden können:

2.2.1 Datenschutzhinweise und Einverständniserklärungen

Für eine höhere Transparenz bei der Datenerhebung und -nutzung müssen Datenverantwortliche gemäß der DSGVO Datenschutzhinweise mit Angabe der Identität des Datenverantwortlichen veröffentlichen sowie Informationen zur Art des angewendeten Datenverarbeitungsprozesses bereitstellen. Datenschutzhinweise müssen umfassende, vorgeschriebene Angaben enthalten, unter anderem:

- Kontaktdaten des Datenverantwortlichen
- Zweck der Datenverarbeitung
- Personen/Organisationen, an welche diese Daten weitergegeben werden
- Informationen zu Datenübertragungen außerhalb der EU
- Dauer der Aufbewahrung der Daten
- Rechte von Personen
- Anleitung für die Einreichung von Beschwerden

Diese Hinweise müssen eindeutig sowie in leicht lesbarer und verständlicher Form angegeben werden; lange, schwer lesbare und im Juristenjargon formulierte Bestimmungen sind nicht zulässig.

Die Hinweise müssen zudem kurz und knapp dargestellt werden. Das ist bei der Videoüberwachung problematisch. Europäische Datenschutzbehörden bevorzugen „mehrschichtige“ Hinweise, d. h. die wichtigsten Informationen sind sofort sichtbar und für diejenigen, die Näheres wissen möchten, durch Links mit ausführlicheren

Informationen verknüpft. So könnten Nutzer von Videoüberwachungslösungen, die nicht alle oben aufgeführten Informationen auf einem großen Hinweisschild unterbringen möchten, ein kleineres Schild mit Angaben zu ihrer Identität und zum Zweck der Bilderfassung anfertigen – plus URL oder Telefonnummer für Personen, die den gesamten Hinweistext lesen möchten.

Die Verordnung gilt auch für Videoüberwachungslösungen, bei denen der Datenverantwortliche auf die Videomanagementplattform eines anderen Datenverantwortlichen zugreift, um Situationen besser einschätzen zu können. Städtische Überwachungssysteme basieren zunehmend auf einem kooperativen Konzept, das die Integration von Systemen und die Weitergabe von Informationen in diesen Systemen an Dritte vorsieht. In diesen Fällen muss der Datenverantwortliche, der die ursprünglichen Daten erhebt, auch die Kontaktinformationen der Dritten angeben, die auf diese Daten zugreifen können. Darüber hinaus müssen diese Dritten die gesammelten Daten ordnungsgemäß verwalten und schützen.

Laut DSGVO muss die zu den zahlreichen rechtlichen Datenverarbeitungsgrundlagen gehörende Einverständniserklärung einer Person freiwillig erteilt werden, einen konkreten Bezug haben, auf fundierten Informationen beruhen und eindeutig sein. Demnach dürfen das Schweigen der Person oder vorab aktivierte Kontrollkästchen nicht als Einverständnis ausgelegt werden. Gemäß der DSGVO müssen Personen ihr Einverständnis ebenso leicht widerrufen wie erteilen können.

Laut DSGVO muss die zu den zahlreichen rechtlichen Datenverarbeitungsgrundlagen gehörende Einverständniserklärung einer Person freiwillig erteilt werden, einen konkreten Bezug haben, auf fundierten Informationen beruhen und eindeutig sein.

2.2.2 Zugriffsrecht

Die neue Verordnung sorgt für deutlich höhere Datentransparenz und stärkt die Rechte der betroffenen Personen. Laut DSGVO können Personen Auskunft darüber verlangen, ob, wo und zu welchem Zweck ihre Daten verarbeitet werden. Zudem muss der Datenverantwortliche der betroffenen Person auf Anforderung kostenlos eine Kopie (auch als elektronische Version) der personenbezogenen Daten zusenden. Die DSGVO enthält außerdem eine neue Empfehlung, wonach Organisationen nach Möglichkeit den Fernzugriff auf ein sicheres Self-Service-System gewähren sollten, über das Personen direkt auf ihre Informationen zugreifen können.

Im Zusammenhang mit der Videoüberwachung müssen Datenverantwortliche über Systeme verfügen, mit denen innerhalb eines Monats Anfragen angenommen und überprüft sowie entsprechende Informationen herausgegeben werden können. Dies kann vor allem dann schwierig werden, wenn eine Person Kopien eines Videos anfordert und dabei die Identität anderer Personen, die auf den Aufnahmen zu sehen sind, unkenntlich gemacht oder anderweitig geschützt werden muss.

2.2.3 Recht auf Löschung (oder Vergessen)

Personen können den Wunsch äußern, dass ihre Daten gelöscht werden; zudem können sie der Verarbeitung ihrer Daten widersprechen oder die Verarbeitung einschränken. Für die Löschung der Daten gelten folgende Bedingungen: (1) Die Daten haben für den ursprünglichen Verarbeitungszweck keine Bedeutung mehr und (2) die Verarbeitung beruhte ursprünglich auf einem Einverständnis, das die Person danach jedoch widerrufen hat.

2.2.4 Recht auf Datenübertragbarkeit

Die betroffenen Personen können den Erhalt und die Übertragung ihrer Daten an einen neuen Datenverantwortlichen anfordern. Datenverantwortliche müssen die Daten in einem gängigen, maschinenlesbaren Format bereitstellen. Personen können auch die direkte Übertragung ihrer Daten an einen neuen Datenverantwortlichen verlangen.

2.2.5 Benachrichtigung über Verstöße

Die DSGVO sieht vor, dass Datenschutzverstöße von Datenverantwortlichen gemeldet werden müssen. Demnach sind Verstöße binnen 72 Stunden, nachdem der Datenverantwortliche erstmals von dem Verstoß Kenntnis erlangt hat, den EU-Datenschutzbehörden zu melden. Datenverarbeiter sind verpflichtet, die Datenverantwortlichen – also ihre Kunden – unverzüglich über Datenschutzverstöße zu benachrichtigen.

Stellt ein Datenverantwortlicher fest, dass durch einen Datenschutzverstoß wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten von Personen entsteht, muss er zudem die betroffenen Personen unverzüglich benachrichtigen. Allerdings sieht die DSGVO eine Ausnahme von dieser Verpflichtung zur Benachrichtigung der betroffenen Personen vor. Diese gilt für Datenverantwortliche, die durch die Umsetzung technischer und organisatorischer Maßnahmen wie Verschlüsselung und Anonymisierung dafür sorgen, dass die Daten von Unbefugten nicht zu erkennen oder verstehen sind.

2.3. Verantwortung und Benennung von Datenschutzbeauftragten

Zurzeit müssen sich Datenverantwortliche bei ihrer örtlichen Datenschutzbehörde registrieren lassen. Diese Anforderung wird in der DSGVO nicht mehr enthalten sein; stattdessen kommen neue Nachweisvorschriften auf Datenverantwortliche und -verarbeiter zu. Datenverantwortliche müssen außerdem eine Datenschutz-Folgenabschätzung vornehmen und die Datenschutzbehörde um Rat ersuchen, wenn die Verarbeitung mit einem hohen Risiko verbunden ist. Zudem

müssen Organisationen Datenschutzbeauftragte benennen, wenn durch die Datenverarbeitung ein hohes Risiko besteht, unter anderem bei Videoüberwachungslösungen mit systematischer, großräumig angelegter Überwachung eines öffentlichen Bereichs – etwa bei stadt- oder campusweiten Überwachungssystemen.

2.4 Eingebauter Datenschutz

Gemäß DSGVO muss der Datenschutz von vornherein durch technische Maßnahmen und nicht erst durch zusätzliche Maßnahmen sichergestellt werden. Die Verpflichtung zu einem „eingebauten" Datenschutz in der DSGVO erfordert ein Systemtechnikkonzept, bei dem Datenschutzgrundsätze wie die Verschlüsselung und Anonymisierung von Videoaufnahmen von Beginn an Teil des Systemdesigns sind.

Darüber hinaus müssen Datenverantwortliche sicherstellen, dass standardmäßig nur die Mindestmenge an Daten erhoben wird. Videoüberwachungssysteme, die ständig aufzeichnen und Bilder auf unbestimmte Zeit speichern, stellen einen Verstoß gegen diese Bestimmung dar. In diesem Fall müssen Datenverantwortliche auf Videoüberwachungssysteme mit einer funktionsreichen Benutzeroberfläche umstellen, die durch flexible Aufzeichnungsoptionen eine individuelle Festlegung der Aufbewahrungsdauer ermöglicht.

2.5 Besondere Verpflichtungen für Datenverarbeiter

Wie bereits erwähnt, können Datenverantwortliche die Durchführung ihrer Datenverarbeitungsprozesse an Drittanbieter auslagern. Für diese Fälle sieht die DSGVO vor, dass die Datenverantwortlichen den von ihnen beauftragten Datenverarbeitern Bedingungen auferlegen, darunter

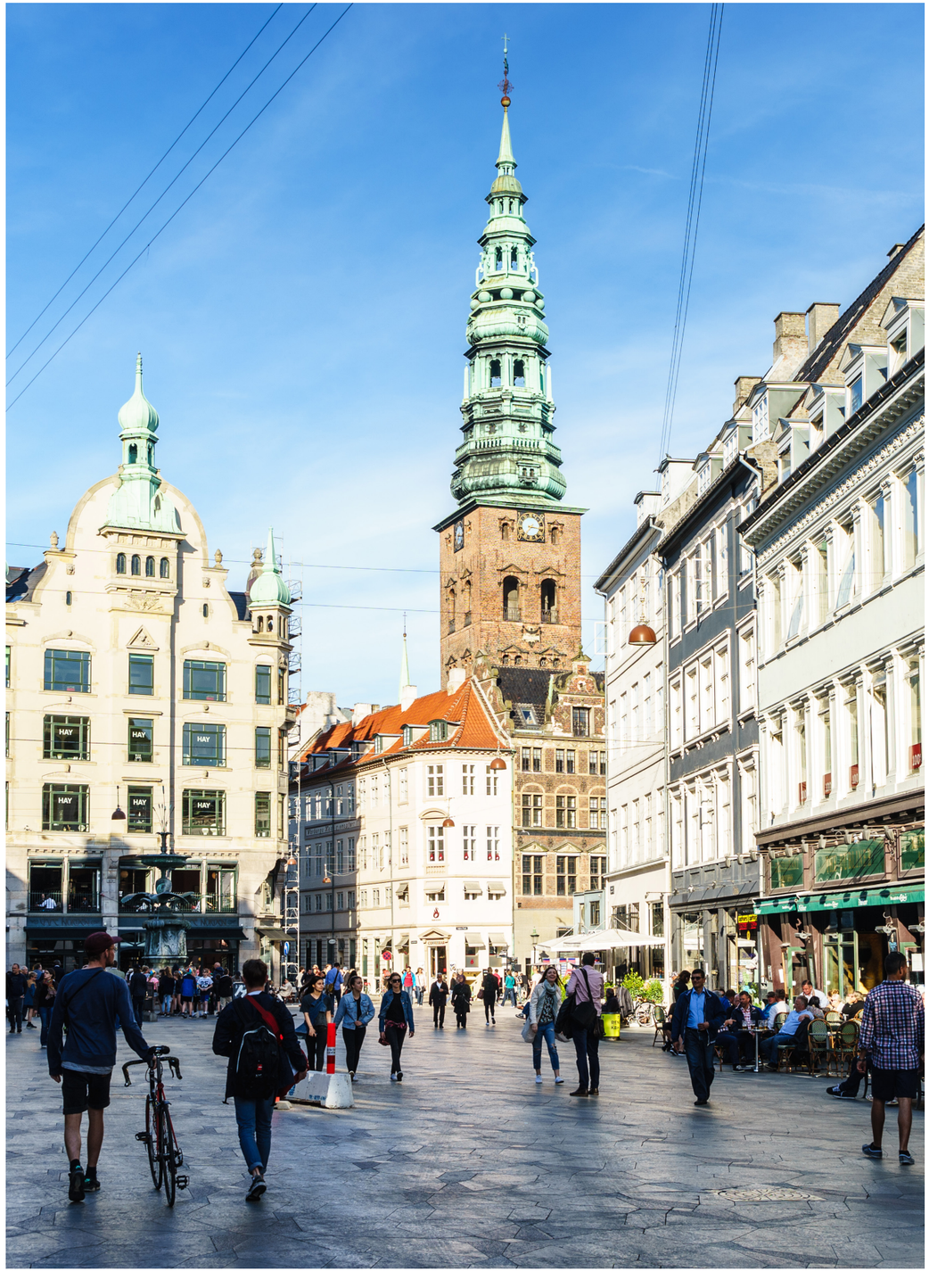
1. die Verpflichtung, die Datenverantwortlichen bei der Erfüllung ihrer Verpflichtungen aus der DSGVO zu unterstützen
2. die Verpflichtung, bei der Datenverarbeitung die Anweisungen der Datenverantwortlichen strikt zu befolgen
3. die Verpflichtung, nicht ohne Einverständnis der Datenverantwortlichen Unterauftragnehmer mit der Datenverarbeitung zu beauftragen, und die Verpflichtung, den Datenverantwortlichen Prüfrechte vertraglich zu gewähren.

2.6 Sanktionen

Die DSGVO sieht ein mehrstufiges System von Geldbußen für Datenverantwortliche und -verarbeiter vor, die sich auf 4 % des Jahresumsatzes oder 20 Millionen Euro belaufen können, wobei der jeweils höhere Wert maßgeblich ist. Der Prozentsatz der Geldbuße bezieht sich nicht auf den Nettogewinn, sondern auf den Bruttoumsatz des gesamten Unternehmens. Außerdem ermöglicht die DSGVO den von einem Verstoß betroffenen Personen das Einreichen einer Zivilklage.

Die DSGVO sieht ein mehrstufiges System von Geldbußen für Datenverantwortliche und -verarbeiter vor, die sich auf 4 % des Jahresumsatzes oder 20 Millionen Euro belaufen können, wobei der jeweils höhere Wert maßgeblich ist.

Whitepaper/Was die DSGVO für Videoüberwachung bedeutet



3

Der Weg zu einem DSGVO-konformen Videoüberwachungs-system

In diesem Abschnitt werden (1) Datenverantwortlichen eine Reihe wichtiger Überlegungen hinsichtlich der effizientesten Umstellung auf ein DSGVO-konformes Videoüberwachungssystem vorgestellt und (2) verschiedene Lösungen oder Funktionen für robustere End-to-End-Videoplattformen betrachtet.

Im Hinblick auf die DSGVO-Konformität müssen Datenverantwortliche aufgrund des Kontexts, des Ausmaßes und des invasiven Charakters besonderes Augenmerk auf Videoüberwachung als Vorgang der Datenverarbeitung legen. Systeme zur groß angelegten Videoüberwachung gelten gemäß DSGVO als Verarbeitungsvorgänge mit hohem Risiko und bedürfen eines besonderen Umgangs.

Genetec kann Datenverantwort-lichen wertvolle Einblicke in den Umfang ihrer DSGVO-Verpflich-tungen bieten.

Nachdem die Datenverantwortlichen das mit ihren Videoüber-wachungslösungen verbundene Risiko beurteilt haben, sollten sie überlegen, wie sie ihre Systeme vor Datenschutzverstößen schützen, und eine sorgfältige Einschätzung des Datenflusses durch die drei Phasen der Datenverarbeitung – Erhebung, Verarbeitung, Herausgabe – vornehmen.

Datenverantwortliche sollten außerdem prüfen, wie sie die Rechte der betroffenen Personen wahren, insbesondere das Recht auf Anforderung von Videoaufzeichnungen. Solche Anforderungen könnten sich aufgrund des zeitlichen Aufwands für die Erhebung und Anonymisierung der Daten als kostspielig herausstellen. Mit der passenden Technologie fallen die Auswirkungen und Gesamtkosten dieser Verpflichtung erheblich geringer aus.

Zu guter Letzt sollten Datenverantwortliche überlegen, wie sie mit der Unterstützung eines Datenverarbeiters und der geeigneten In-frastruktur die Konformität ihrer Videoüberwachungsanwendungen sicherstellen können.

Als zuverlässiger Partner kann Genetec Datenverantwortlichen wertvolle Einblicke in den Umfang ihrer DSGVO-Verpflichtungen bieten und ihnen aufzeigen, wie die Videosysteme zur Erfüllung dieser Verpflichtungen idealerweise konzipiert und entwickelt werden sollten. Genetec bietet auch standortgebundene und SaaS-basierte End-to-End-Lösungen, die Datenverantwortlichen bei der Einhaltung der DSGVO und bei den grundlegenden und erweiterten Verantwortlichkeiten im Hinblick auf die Hochrisiko-Verarbeitung von Videoüberwachungsdaten helfen.

3.1 Risikostufe

Datenverantwortliche, die EU-Bürger per Video überwachen, müssen zur Sicherstellung der DSGVO-Konformität als Erstes eine Datenschutz-Folgenabschätzung vornehmen, um festzustellen, ob durch die Verarbeitung „wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten von Personen entsteht“.

Zunächst müssen die Datenverantwortlichen anhand von Artikel 35 die Risikostufe im Zusammenhang mit ihren Videoüber-wachungslösungen bestimmen. Ein hohes Risiko für die Rechte und Freiheiten von Personen kann entstehen, wenn im Rahmen der Verarbeitung

- eine systematische und umfassende Bewertung personenbezogener Aspekte natürlicher Personen erfolgt, darunter Gesichtserkennung zu Profilingzwecken sowie automatische Nummernschilderkennung
- eine groß angelegte, systematische Überwachung eines öffentlich zugänglichen Bereichs erfolgt, darunter Städte, Flughäfen, Ladenlokale und Hotels

Betreiben Datenverantwortliche derartige Hochrisikosysteme, müssen sie Datenschutzbeauftragte benennen und unter Umstän-den das Einverständnis der Datenschutzbehörde einholen, ehe sie fortfahren können.

3.2 Verpflichtungen gemäß DSGVO bei Datenschutzverstößen

Der Schritt in Richtung DSGVO-Konformität beginnt bereits vor der Implementierung des Videoüberwachungssystems. Datenverantwortliche müssen sich überlegen, wie sie ihre Systeme gegen Datenschutzverstöße wappnen. Unabhängig von der Vertraulichkeit der erhobenen Daten kann ein Datenschutzverstoß

- negative Auswirkungen auf den Ruf haben und das Ansehen der Marke beschädigen
- beträchtlich höhere Betriebskosten nach sich ziehen, da Datenverantwortliche Abhilfe schaffen und dafür sorgen müssen, dass ihre Systeme bereinigt sind
- zu hohen Geldbußen führen

Die Möglichkeit von Datenverantwortlichen, auf einen vorsätzlichen oder versehentlichen Datenschutzverstoß wirksam zu reagieren, ist ein wesentlicher Bestandteil des Risikobeurteilungsverfahrens, denn laut DSGVO müssen die Datenverantwortlichen einen Verstoß binnen 72 Stunden nach seiner Feststellung melden.

Je nachdem, wie ein Videoüberwachungssystem implementiert wird und wer an dessen Management beteiligt ist, sind ein effektives Kommunikationsverfahren sowie geeignete Instrumente erforderlich, damit Datenschutzverstöße in einzelnen Komponenten des Systems gemeldet werden können. Die Rückverfolgbarkeit aller Vorgänge anhand von Protokollen und Berichten sowie eine lückenlose Nachweiskette, wenn Videodaten als Beweis weitergegeben werden, sind wichtige Funktionen für die Einhaltung der Verordnung. Zur Wahrung der Rechte und des Datenschutzes der Personen, deren Daten erhoben werden, können Datenverantwortliche zudem technische und organisatorische Schutzmaßnahmen wie Verschlüsselung und Anonymisierung treffen, sodass die Daten von Unbefugten nicht zu erkennen oder verstehen sind. Mit diesen Prozessen, Instrumenten und Datenschutzmaßnahmen können Datenverantwortliche die Ursache eines Verstoßes effektiv erforschen und ihr Engagement für ein verantwortungsvolles Datenmanagement unter Beweis stellen.

Standortgebundene und SaaS-basierte Lösungen von Genetec: „Sicherheit der Sicherheit“ bilden den Kern unserer proaktiven Strategie zur Vermeidung von Datenschutzverstößen und des unbefugten Zugriffs auf personenbezogene Informationen. Produkte von Genetec arbeiten mit Verschlüsselung und Claims-basierter Authentifizierung, verfügen über Autorisierungsmanagementfunktionen und bieten eine dynamische Anonymisierung, durch die Personen in Live-Videos und Videoaufzeichnungen beim Überwachen von Handlungen und Bewegungen automatisch anonymisiert werden.

3.3 DSGVO-Konformität und Datenfluss

3.3.1 Erhebung

Als „Erhebung“ gilt das Erfassen von Informationen. In dieser Phase müssen die Datenverantwortlichen sicherstellen, dass die Integrität der Daten in ihren Systemen gewahrt bleibt. Besteht bei der

Datenverarbeitung ein hohes Risiko, sollten Datenverantwortliche eine Verschlüsselung oder Anonymisierung des Videostreams in Betracht ziehen.

So können die Datenverantwortlichen die von ihnen erhobenen Daten verschlüsseln, um die in der DSGVO verankerten Rechte der Personen zu schützen. Verschlüsselte Daten können nur mit dem entsprechenden Entschlüsselungsschlüssel gelesen werden und sind somit auch dann geschützt, wenn sich eine unbefugte Person oder Entität Zugriff auf die Daten verschafft. Ganz gleich, ob es sich um stationäre oder um von einer Kamera übertragene Daten handelt – durch die Verschlüsselung werden vertrauliche Daten geschützt und die Kommunikation zwischen Clients und Servern verbessert. Weitere wirksame Maßnahmen, mit denen ein Videoüberwachungssystem robust und sicher gemacht werden kann, sind Authentifizierung, Autorisierung und Passwortanforderung.

Mit einem Videoüberwachungssystem kann auf dreierlei Weise sichergestellt werden, dass die Identität von Personen anonym bleibt:

1. Permanente Unkenntlichmachung – dabei werden Personen in Videoaufnahmen dauerhaft anonymisiert, d. h. die Unkenntlichmachung lässt sich nicht rückgängig machen.
2. Dynamische Anonymisierung – mithilfe einer Software, die Handlungen und Bewegungen überwacht, werden Personen in Live-Videos und Videoaufzeichnungen automatisch anonymisiert.
3. Bearbeitung – hierbei wird nur die Identität von ausgewählten Personen in Videoaufnahmen verborgen. Dies geschieht in der Regel nachträglich, wenn eine Organisation die Videoaufnahmen an Vollzugsbehörden weitergeben möchte.

Standortgebundene Lösungen von Genetec: Genetec Security Center bietet Verschlüsselungs- und Authentifizierungsverfahren, sodass nur befugte Personen Zugang zum Sicherheitssystem des Datenverantwortlichen haben. Mit Security Center können Datenverantwortliche neue Stufen der verschlüsselten Kommunikation zwischen allen Systemkomponenten einführen und durch digitale Zertifikate das Vertrauen innerhalb ihrer Systeme gewährleisten. Zudem kann Security Center die Kommunikation im System authentifizieren und auf diese Weise überprüfen und sicherstellen, dass Daten und Videos nicht mit externen Quellen ausgetauscht werden.

Durch dynamische Anonymisierung, bei der Personen in Live-Videos und Videoaufzeichnungen bei der Überwachung von Handlungen und Bewegungen automatisch anonymisiert werden, trägt Security Center außerdem dazu bei, dass Datenverantwortliche bei der Videoüberwachung öffentlicher Räume die Vorschriften einhalten. Mit KiwiVision™ Privacy Protector™ können unbearbeitete, unverschlüsselte Videos im Hintergrund kryptographisch verschlüsselt und aufgezeichnet werden. Anschließend werden sie von befugtem Personal entschlüsselt. Bei Bedarf können Datenverantwortliche den Einsatz von Privacy Protector auf die Kameras beschränken, die bei der Hochrisiko-Verarbeitung genutzt werden, und in jeder Situation den idealen Grad der Anonymisierung wählen. Mit wenigen Klicks können sie Personen und Gegenstände im Kamerasichtfeld verpixeln, deren Schärfe reduzieren oder vollkommen unkenntlich machen.

SaaS-basierte Lösungen von Genetec: Mit Genetec Stratocast™ können Datenverantwortliche dafür sorgen, dass die DSGVO-Bestimmungen zur Datenintegrität während der Erhebung eingehalten werden. Um die Anforderungen zur Bearbeitung von Videoexporten zu erfüllen, können Datenverantwortliche die SaaS-basierte Fallmanagementlösung Genetec Clearance™ nutzen. Die darin enthaltenen Tools tragen zu einer effizienten und zügigen Erledigung der Aufgabe bei.

3.3.2 Verarbeitung

„Verarbeitung“ bezieht sich auf den Vorgang der eigentlichen Datenverarbeitung durch Datenverantwortliche. Eine wichtige Bestimmung der DSGVO besteht darin, dass Datenverantwortliche für die Überwachung und Kontrolle des Zugriffs auf die in ihren Systemen gespeicherten Daten verantwortlich sind. Dies ist sowohl für den Datenschutz als auch für den Umgang mit möglichen Datenschutzverstößen von Bedeutung, da durch eine ordnungsgemäße Verwaltung der Zugriffsrechte die Wahrscheinlichkeit eines unbeabsichtigten Datenschutzverstoßes verringert werden kann.

Durch Authentifizierung und Autorisierung können Datenverantwortliche auf ideale Weise steuern, wer auf die in ihren Systemen erfassten Videos und Daten zugreift. Datenverantwortliche können den Zugang zu ihren Systemen durch Authentifizierungsmechanismen schützen, die dafür sorgen, dass Personen beim Anmelden auf das richtige System zugreifen. Bei der Authentifizierung wird mithilfe von Zertifikaten, Kombinationen aus Benutzername und Passwort sowie Token verhindert, dass Cyberkriminelle sich als Sicherheitsserver ausgeben, so in ein Sicherheitssystem eindringen und Daten manipulieren, kopieren oder kontrollieren können. Bei der Autorisierung wird gesteuert, wer Daten innerhalb eines Systems sehen kann und was diese Personen mit den Daten machen können. Mithilfe von Autorisierungsfunktionen können Datenverantwortliche den Umfang der Aktivitäten in ihrem System beschränken, indem sie nur bestimmten Gruppen oder Personen die Berechtigung zum Zugriff auf Ressourcen, Daten oder Anwendungen erteilen. Somit gewährleisten sie die Sicherheit der in ihren Systemen übertragenen und gespeicherten Daten.

Standortgebundene und SaaS-basierte Lösungen von Genetec: Mit Lösungen von Genetec können detaillierte Zugriffsrechte für Benutzer bestimmt werden. Datenschutz wird sichergestellt, indem eindeutig festgelegt wird, wie autorisierten Personen die Berechtigung zum Zugriff auf bestimmte Daten erteilt wird und ob sie diese Daten oder das Systemverhalten ändern können.

3.3.3 Herausgabe

„Herausgabe“ bezieht sich auf das Lebenszyklusmanagement der erfassten Daten und auf die DSGVO-Bestimmung, wonach Datenverantwortliche einer betroffenen Person auf deren Anforderung digitale Kopien personenbezogener Daten bereitstellen müssen. Dies ist ein überaus wichtiger Abschnitt der DSGVO, da Personen das Recht haben, eine Kopie ihrer eigenen Daten anzufordern.

In den meisten Fällen müssen Datenverantwortliche diese Daten kostenlos bereitstellen und dafür sorgen, dass sie die Rechte und

Freiheiten anderer nicht beeinträchtigen, wenn sie einer solchen Anforderung nachkommen. Wenn es um die Übertragbarkeit von Daten geht, können Datenverantwortliche die Einhaltung der DSGVO beispielsweise dadurch sicherstellen, dass sie digitale Kopien von Informationen über einen Self-Service-Kiosk bereitstellen. Allerdings besteht ein typisches Problem der Videoüberwachung darin, dass auf einer Aufnahme häufig viele Personen zu sehen sind. Daher spielt die Anonymisierung von Videos zur Gewährleistung der Freiheit und Datenschutzrechte anderer Personen eine entscheidende Rolle. Da betroffene Personen das Recht auf Löschung ihrer personenbezogenen Daten haben, müssen Datenverantwortliche zudem ein besonderes Augenmerk auf die Verwaltung ihrer Archive legen, denn möglicherweise müssen bestimmte Daten gesondert aufbewahrt und gelöscht werden.

Standortgebundene und SaaS-basierte Lösungen von Genetec: Um ihre Verpflichtungen im Zusammenhang mit der Herausgabe von Daten erfüllen zu können, müssen Verantwortliche zunächst feststellen, auf welchen Bildern die betroffene Person zu sehen ist. Im Rahmen der eigenen Standardangebote oder über Technologiepartner bietet Genetec eine Reihe von Tools, die das Auffinden, Identifizieren und Zusammentragen der aufgezeichneten Informationen einer Person erheblich erleichtern.

Für die Herausgabe der Daten können Datenverantwortliche innerhalb ihrer Videoüberwachungssysteme Genetec Clearance einsetzen und so innerhalb eines Monats Datenanforderungen von betroffenen Personen annehmen, auf ihre Gültigkeit überprüfen und Informationen herausgeben. Diese cloudbasierte Lösung mit offener Architektur bietet Funktionen, die für ein effizientes und sicheres Management von „Hochrisiko“-Videodaten unverzichtbar sind: Verschlüsselung, zentralisierte Videosammlung und erweiterte Suche. Zudem enthält Genetec Clearance integrierte Videobearbeitungsfunktionen zur Unkenntlichmachung aller von den Videokameras erfassten Personen. So können Datenverantwortliche ein Self-Service-Portal mit Fernzugriff entwickeln, in dem Personen direkt auf ihre personenbezogenen Daten zugreifen können.

3.3.4 Tools zur Unterstützung von Datenschutzbeauftragten

Datenverantwortliche müssen unter Umständen Datenschutzbeauftragte benennen, um die Einhaltung ihrer DSGVO-Verpflichtungen zu überwachen. Der Zugang zu den richtigen Informationen ist für die Datenverantwortlichen unverzichtbar. Datenschutzbeauftragte müssen ihrerseits nachverfolgen können, welche Schritte Datenverantwortliche zum Schutz der erhobenen Informationen unternommen haben.

Standortgebundene und SaaS-basierte Lösungen von Genetec: Lösungen von Genetec bieten zahlreiche Protokolloptionen und vor allem eine leistungsstarke Berichtsplattform, über die Datenverantwortliche und Datenschutzbeauftragte den Zustand ihrer Videoüberwachungssysteme überwachen oder nachforschen können, wer Zugang zu Informationen hatte und/oder Informationen aus ihren Systemen heruntergeladen hat.

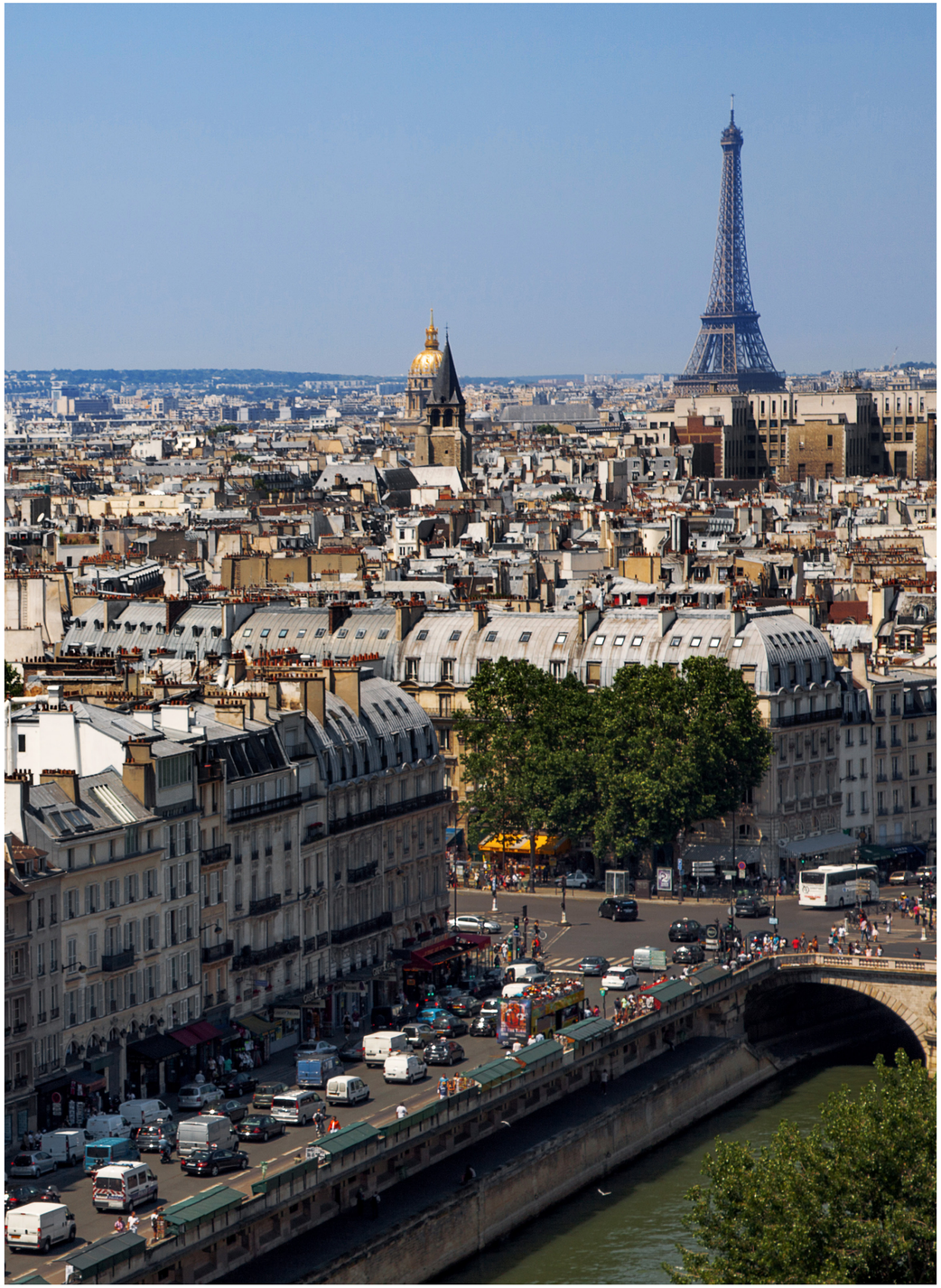
4

Fazit

Die DSGVO tritt am 25. Mai 2018 in Kraft. Spätestens dann müssen alle Organisationen, die Videoüberwachungslösungen in der EU einsetzen, insbesondere in öffentlichen Bereichen, sicherstellen, dass ihre Systeme die in der Verordnung dargelegten Anforderungen eines „eingebauten“ Datenschutzes (Privacy by design) erfüllen. Außerdem müssen Organisationen die in der DSGVO verankerten Rechte von Personen achten, darunter das Recht des Zugriffs auf personenbezogene Informationen, die von den Organisationen erhoben wurden. Darüber hinaus müssen Organisationen die Integrität der erfassten Daten überwachen und wahren sowie im Fall eines Datenschutzverstoßes die Datenschutzbehörden binnen 72 Stunden informieren. Die Nichteinhaltung dieser Bestimmungen führt zu einem Reputationsverlust der Organisation und zieht hohe Geldbußen nach sich.

Mit standortgebundenen Lösungen oder – als beauftragter Datenverarbeiter – mit einem Portfolio an SaaS-basierten Lösungen kann Genetec dazu beitragen, dass Organisationen die Bestimmungen der DSGVO einhalten. Zudem kann Genetec Organisationen helfen, durch Such- und Bearbeitungstools die Betriebskosten im Zusammenhang mit ihren Videoüberwachungsanwendungen zu reduzieren.

Whitepaper/Was die DSGVO für Videoüberwachung bedeutet



Genetec wurde 1997 gegründet und ist der weltweit führende Anbieter von einheitlichen Sicherheitsplattformen mit einem umfassenden, vielfältigen Angebot an Sicherheitskomponenten.

Videoüberwachung: Verbessern Sie die Situationseinschätzung und die Sicherheit in Ihrer Stadt dank der Möglichkeit, Kameras für verschiedene Behörden und Organisationen freizugeben. So erhalten Sie ein gemeinsames Bild der Situation und verkürzen die Reaktionszeit bei Vorfällen.

Zutrittskontrolle: Mit einer integrierten IP-fähigen Plattform können Sie die Sicherheit Ihrer Organisation erhöhen, effektiv auf Bedrohungen reagieren sowie schneller klare Entscheidungen treffen – ganz gleich, ob Sie ein neues Zutrittskontrollsystem installieren oder eine bestehende Installation aktualisieren.

Automatische Nummernschilderkennung: Automatisieren Sie die Erkennung gesuchter Fahrzeuge, setzen Sie Parkvorschriften effizienter durch und beschleunigen Sie Untersuchungen zum Schutz der Öffentlichkeit, indem Sie Nummernschilddaten an ausgewählte Behörden und Partnerorganisationen weitergeben, ohne Abstriche beim Eigentums- und Datenschutz.

Entscheidungsunterstützung: Gestalten Sie den Umgang mit Vorfällen sowie die Entscheidungsfindung effizienter – mit fortschrittlichen Workflows, die Sicherheitsverantwortliche durch das System führen - von der Warnmeldung über richtlinienbasierte Vorgehensweisen bis hin zum Export detaillierter Fallzusammenstellungen.

Investigative Fallverwaltung: Mit einer Plattform, auf der Sie digitale Beweise zentral ablegen und sicher mit Ermittlern, externen Stellen und der Öffentlichkeit zusammenarbeiten können, lässt sich die Fallverwaltung vereinfachen und Untersuchungen beschleunigen.

Cloud-Services: Erweitern Sie die Funktionen Ihres lokalen Sicherheitssystems und senken Sie die IT-Kosten – dank äußerst skalierbarer On-Demand-Cloud-Services, mit denen Ihre Stadt die sich rasch verändernden Sicherheitsanforderungen problemlos bewältigen und effizienter arbeiten kann.

Whitepaper/Was die DSGVO für Videoüberwachung bedeutet

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

GDPRWP_WPIEN