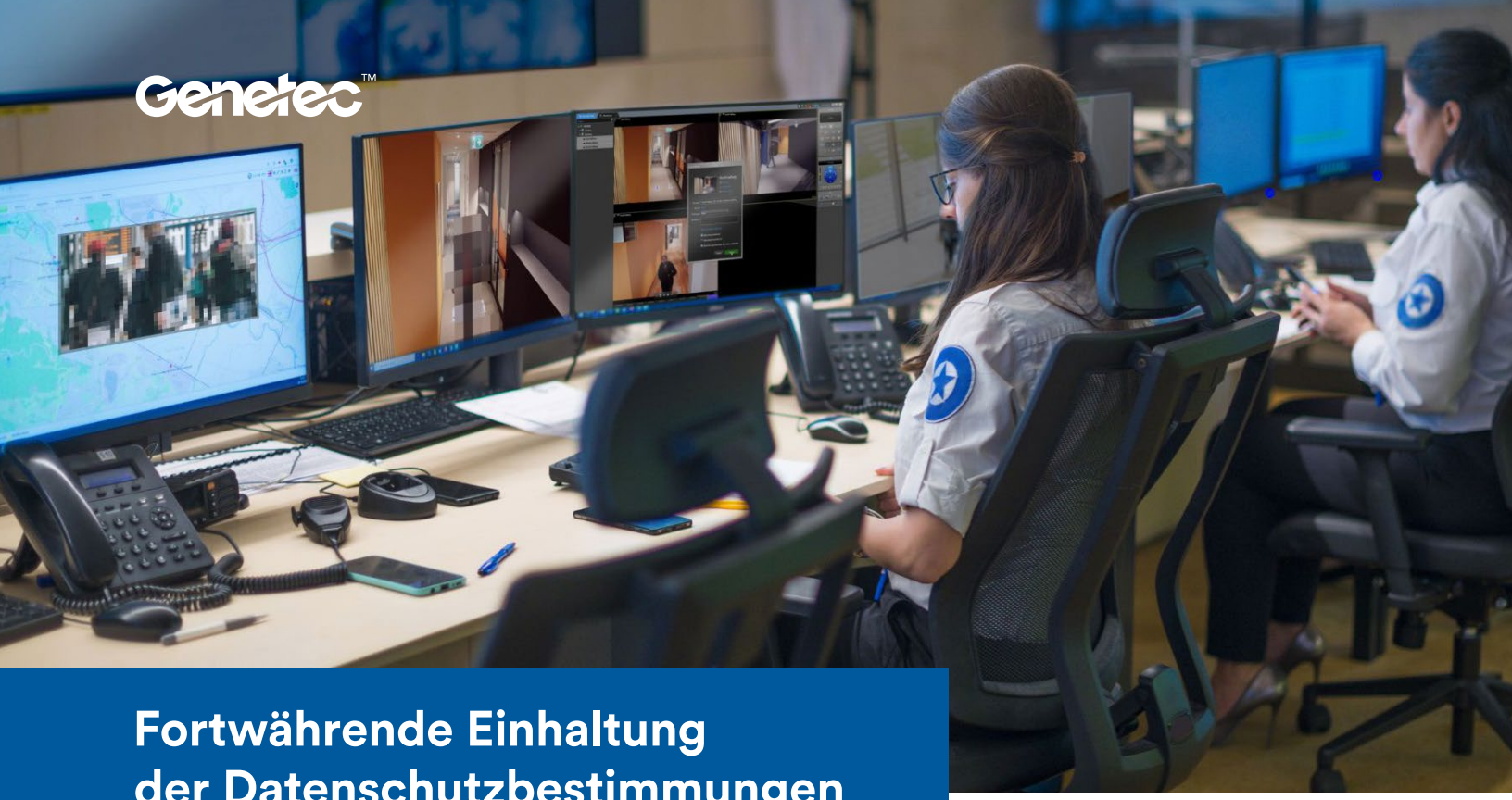

Fortwährende Einhaltung der Datenschutzbestimmungen in 2023

Teil 1

Bei der Weitergabe von Videoaufzeichnungen an Dritte müssen Sie sicherstellen, dass die Privatsphäre sensibler Daten geschützt ist. Das liegt daran, dass Regierungen weltweit Datenschutzgesetze erlassen haben, die Unternehmen für die Art und Weise, wie sie personenbezogene Daten erfassen, verwalten, speichern und weitergeben, zur Verantwortung ziehen.

In Europa beispielsweise unterliegen die meisten Organisationen den Bestimmungen der Datenschutz-Grundverordnung (DSGVO). Die DSGVO gilt schon seit fünf Jahren, aber immer noch suchen Unternehmen nach Möglichkeiten, den Richtlinien zu entsprechen und ihre Prozesse zu optimieren.

In dieser zweiteiligen Abhandlung erfahren Sie mehr über drei spezielle Bestimmungen innerhalb der DSGVO, die auch heute noch für Unternehmen eine Herausforderung darstellen. Zudem erfahren Sie, wie ein digitales Beweismanagementsystem (Digital Evidence Management System, DEMS) für Ihre Organisation die Lösung zur Einhaltung der DSGVO-Bestimmungen beim Einsatz von Videoüberwachungstechnologie sein könnte.

Erfahren Sie, wie Scotrail Zugriffsanfragen betroffener Personen schneller bearbeitet

Drei Datenschutzregelungen der DSGVO, mit deren Umsetzung sich Organisationen schwer tun

Die DSGVO trat im Jahr 2018 in Kraft. Seitdem haben viele Unternehmen zur Einhaltung dieser Datenschutzgesetze neue Mitarbeiter eingestellt, neue Prozesse eingeführt und unternehmensweite Richtlinien erstellt.

Bei der Weitergabe von Videomaterial und dem Schutz von Daten gibt es jedoch einige Bestimmungen, bei deren Einhaltung sich Organisationen schwer tun:

- Auskunftsrecht (Artikel 15) – Beantwortung von Anfragen der Öffentlichkeit zur Auskunft zu personenbezogenen Daten innerhalb von 30 Tagen.
- Keine Anwendung auf anonymisierte Daten (Erwägungsgrund 26) – Unkenntlichmachung irrelevanter betroffener Personen bei der Weitergabe von Videos an Strafverfolgungsbehörden oder andere Parteien.
- Recht auf Löschung (Artikel 17) – Automatisierung von Aufbewahrungsrichtlinien für gespeicherte Videos, um sicherzustellen, dass sie nicht länger als nötig aufbewahrt werden.

Viele Organisationen haben eine Lösung gefunden, wie sie mit diesen spezifischen Datenschutzanforderungen umgehen sollen. Aber sie nutzen dazu häufig manuelle, ressourcenintensive und fehleranfällige Prozesse.

Da schon ein einziger Fehler zu einem Verstoß gegen die Datenschutzbestimmungen, hohen Geldstrafen, Gerichtsverfahren und potenziell irreparablen Schäden für den Ruf einer Organisation führen kann, wurden wir gefragt: Gibt es eine bessere Möglichkeit, die Einhaltung der Datenschutzbestimmungen beim Einsatz von Videoüberwachungssystemen zu gewährleisten?

Und an dieser Stelle kommt ein digitales Beweismanagementsystem ins Spiel, das Ihnen hilft, genau diese DSGVO-Bestimmungen zu erfüllen.

Worum genau geht es beim Auskunftsrecht der DSGVO?

Wenn Sie über Videoüberwachungstechnologie verfügen, ist es nicht ungewöhnlich, dass Ihr Team nach Aufzeichnungen gefragt wird. Dazu können Anfragen von Behörden zählen, die um ein Video zu einem Verfall bitten, der sich in der direkten Umgebung Ihres Unternehmens zugetragen hat, oder von Ihrem Versicherer, der Beweise für einen Haftungsanspruch benötigt.

Doch damit ist Ihre Verpflichtung zur Weitergabe von Videomaterial mittlerweile noch nicht zu Ende. Gemäß Artikel 15 der DSGVO, dem Auskunftsrecht, haben Personen das Recht, Zugang zu allen personenbezogenen Daten zu verlangen, die Ihre Organisation über sie gespeichert hat, einschließlich Videoaufzeichnungen.

Und Sie müssen diesen Anfragen nicht nur innerhalb von 30 Tagen nachkommen. Gemäß Erwägungsgrund 26, der nicht für anonyme Daten gilt, müssen Sie zudem die Identität aller anderen Personen in der Videoaufnahme unkenntlich machen. Wie können Sie also sicherstellen, dass Ihr Team diese Videoanfragen schnell bearbeiten und gleichzeitig die Datenschutzbestimmungen einhalten kann? Indem Sie ein digitales Beweismanagementsystem verwenden.

Bearbeitung von Videoanfragen mit einem digitalen Beweismanagementsystem

Wie sieht Ihr Erfüllungsprozess aus, wenn Sie eine Anfrage zu einem Video von einer Strafverfolgungsbehörde oder einer Einzelperson erhalten?

Bei vielen Organisationen muss hierbei in der Regel ein Anfrageformular in Papierform ausgefüllt werden. Ein Mitarbeiter Ihres Teams überprüft und genehmigt diese Anfrage dann und weist den Auftrag dem Sicherheitsteam zu. Anschließend sucht ein Sicherheitsmitarbeiter nach dem gewünschten Video, exportiert es auf einen USB-Stick oder eine DVD und sorgt dafür, dass es der anfordernden Person direkt übergeben wird.

Dieser Prozess ist sehr zeit- und ressourcenintensiv. Es gibt zudem keine Garantie dafür, dass der USB-Stick nach der Übergabe nicht verlegt wird oder verloren geht, was zu einer Datenschutzverletzung führen könnte.

Mit einem digitalen Beweismanagementsystem (DEMS) wird die Weitergabe von Videoaufzeichnungen sicherer und einfacher. Sie können das DEMS verwenden, um individualisierte Antragsformulare zu erstellen, die online eingereicht werden können.

Nachdem die Anfrage genehmigt wurde, kann Ihr Team Videoaufzeichnungen problemlos in die Beweismanagementlösung exportieren und der anfordernden Person per E-Mail einen sicheren Link zu den Dateien senden.

Der Empfänger kann die Dateien dann gemäß den ihm zugewiesenen Berechtigungen anzeigen oder herunterladen.

Alle Benutzeraktivitäten werden automatisch im DEMS protokolliert. Dies bedeutet, dass Sie zu jeder Zeit überprüfen können, wann und wie Benutzer auf die Dateien zugreifen. Bei öffentlichen Anfragen, die offiziell auch als Zugriffsanfragen betroffener Personen bezeichnet werden, können Sie damit nachweisen, dass Sie jede Anfrage fristgerecht bearbeitet haben und die Vorschriften einhalten. Bei Strafverfolgungsfällen können Sie so die Beweismittelverwahrung nachverfolgen und Datenverletzungen minimieren.

Schutz der Identität von Personen bei der Weitergabe von Videoaufzeichnungen

Die einfache Weitergabe von Videobeweisen ist jedoch nur ein Teil der Herausforderung. Gemäß den DSGVO-Bestimmungen, insbesondere Erwägungsgrund 26, ist Ihr Team für den Schutz von Identitäten von Personen verantwortlich, die in von Ihnen weitergegebenen Videoaufzeichnungen auftauchen.

Vor der Einführung von DEMS nutzten viele Organisationen eine separate Lösung für die Videobearbeitung für diese Aufgabe. Nach dem Export des Videos musste das entsprechende Team das Video in die Anwendung zur Videobearbeitung laden und die Identitäten entsprechend unkenntlich machen.

In Fällen, in denen täglich Dutzende solcher Anfragen eingehen können, ist dies eine enorme Belastung für die entsprechenden Ressourcen. Gehen hingegen nur selten solche Anfragen ein, stellt sich die vertraute Frage: Rechtfertigt dies wirklich die Investition in eine weitere Lösung?

Eine bessere Option zum Schutz von Identitäten in Videos ist die Verwendung eines DEMS mit integriertem Unkenntlichmachungstool.

Genetec Clearance™ bietet beispielsweise ein solches integriertes Tool. Damit können Sie die Identität von Personen in Ihren Videos automatisch maskieren. Unabhängig davon, für wen Sie das Video freigeben, können Sie sicherstellen, dass die Privatsphäre anderer Personen geschützt bleibt.

Wie ein Technologiecampus die Weitergabe von Beweisen und Compliance mithilfe von Clearance optimiert

Mit der Verabschiedung der DSGVO begannen viele Unternehmen, ihre Prozesse zur Weitergabe von Videomaterial zu überdenken. Auch Here East, ein Technologiecampus in London, gehörte dazu.

Wenn das Sicherheitsteam von Here East in der Vergangenheit eine Beweisanforderung erhielt, brannte das Sicherheitspersonal das entsprechende Videomaterial auf CDs oder USB-Sticks. Dieser Prozess war nicht nur zeitaufwändig, sondern Here East hatte zudem keinerlei Kontrolle darüber, wie das Material von anderen Personen gespeichert und weitergeben wurde.

„Das war keine angenehme Situation für uns“, so Leighton Jones, Head of Security bei Here East. „Wir müssen immer wieder mal Material innerhalb und außerhalb der Organisation weitergeben. Dabei müssen wir die Kontrolle über unsere Daten behalten.“

Seit Here East Clearance nutzt, werden alle digitalen Beweise über das DEMS erfasst, weitergeben und verteilt. Das Team hat außerdem geeignete Sicherheitsvorkehrungen getroffen, um das Risiko einer unzulässigen Weitergabe oder eines Verlusts des Videomaterials zu minimieren. So können sie beispielsweise Zugriffsrechte für bestimmte Benutzer festlegen, Zeitlimits setzen und den Zugriff auf zuvor freigegebenes Videomaterial widerrufen.

Mit Clearance müssen Nutzer keinerlei Zeit mehr darauf verwenden, die Identitäten unschuldiger Parteien im Material manuell unkenntlich zu machen. Die Aufgabe wird sofort und automatisiert im DEMS durchgeführt.

Erfahren Sie im nächsten Teil, wie Sie durch Auswahl der richtigen Beweismanagementlösung Ihre Datenschutzstrategie weiter stärken können. Im dem Artikel wird erläutert, wie Ihr Team mit einem DEMS die Videoaufbewahrung automatisieren kann, sodass Sie Videos nie länger als nötig aufbewahren.

Erfahren Sie, wie mit Privacy by Design Prozesse für digitale Beweismittel beschleunigt werden können – E-Book herunterladen