White Paper

RGPD (Reglamento General de Protección de Datos) para el Sistema de Videovigilancia

8 de mayo de 2018

Índice

Declaración de Responsabilidad

Hanwha Techwin Co., Ltd. Tiene como objetivo suministrar las informaciones más recientes sobre la LDPR por medio de este white paper. Sin embargo, Hanwha Techwin Co., Ltd. no ofrece ninguna garantía con respecto a la precisión o adecuación comercial de las informaciones descritas en este white paper. Observe que usted debe consultar un órgano consultivo profesional o abogado para confirmar y entender sus derechos y obligaciones bajo los estatutos aplicables. Hanwha Techwin Co., Ltd. no será responsable de cualesquiera consecuencias de aplicar el contenido de este white paper sin tal consulta.

A pesar de los aspectos positivos, como seguridad social y seguridad mejorada, la industria de CCTV sufre de una imagen negativa en toda la sociedad debido a la diseminación de la vigilancia sin confiabilidad operativa y preocupaciones de violaciones de privacidad personal. A medida que nuevas tecnologías, como Internet (IoT), nube, Big Data y IA, son aplicadas y convergen con sistemas de CCTV basados en IP y nuevas posibilidades son creadas, los riesgos de vulnerabilidades de seguridad de red (por ejemplo, acceso no autorizado y adquisición de datos personales) y riesgos legales relacionados a los sistemas de CCTV de red también están aumentando.

En un esfuerzo para tratar con esta situación, la Unión Europea (UE) promulgó el RGPD (Reglamento General de Protección de Datos), que garantiza la libre circulación de datos personales entre los estados miembros de la UE, al mismo tiempo en que fortalece los derechos de protección de privacidad del titular de los datos (persona). Este reglamento fue introducido el 25 de mayo de 2016 para vitalizar la economía digital en la UE y pasó a ser aplicado a partir del 25 de mayo de 2018.

El RGPD refuerza significativamente los derechos de los titulares de los datos personales, así como las obligaciones y responsabilidades de los controladores y procesadores de datos personales. En este sentido, usuarios de sistemas de CCTV y prestadores de servicios deben tener en mente que son legalmente responsables de las vulnerabilidades de seguridad causadas por el sistema de CCTV de red que administran o que sirven al cliente.

Por tanto, al instalar nuevos sistemas de CCTV o actualizar los sistemas existentes, una Evaluación de Impacto en la Privacidad (PIA - Privacy Impact Assessment) debe ser realizada antes de procesar cualesquiera datos personales para determinar riesgos de seguridad y establecer las medidas de seguridad necesarias para proteger la privacidad y los datos personales, incluso en sistemas de CCTV existentes en los cuales el PIA nunca fue realizado. Por ejemplo, problemas graves de seguridad, como configuraciones iniciales de contraseña, análisis periódico de vulnerabilidades en tecnología y equipos, mantenimiento de estándares aceptables (correcciones de errores críticos y actualizaciones de software), concientización sobre el Código de Conducta y entrenamiento de conformidad y notificación de violación para funcionarios deben ser incluidos en el PIA y deben ser corregidos.

Además de esto, al consignar un servicio de almacenamiento o análisis de imágenes de CCTV basado en nube para terceros, las responsabilidades de gestión del procesador de consignar el procesamiento de informaciones fueron reforzadas y las responsabilidades legales por violaciones aumentaron.

Sin embargo, la base de la legislación RGPD de Europa se concentra en incentivar la iniciativa y la responsabilidad preventiva, instituyendo requisitos como la

Evaluación de Impacto en la Privacidad o Privacidad por Diseño/Defecto, en vez de conformidad formal pasiva con reglamentos reforzados. En otras palabras, incentiva la mejoría natural en la concientización de los procesos de conformidad con el RGPD, recompensando los esfuerzos innovadores del controlador o de los procesadores para la conformidad con el RGPD, adoptando mecanismos apropiados, como la aplicación del Código de Conducta y certificaciones.

Si la conformidad con el RGPD es alcanzada a través de la implementación de medidas técnicas y organizativas apropiadas con responsabilidad preventiva bajo el liderazgo del usuario o proveedor de servicios del sistema de CCTV, esto llevaría a la restauración de la confiabilidad y transparencia de la vigilancia por vídeo con CCTV. Esto resultaría en el crecimiento del sector de CCTV y, en último análisis, serviría como un catalizador para promover la economía digital, incluyendo la utilización de big data. Además de esto, las empresas que tratan con datos personales de europeos están sujetas a la conformidad con el RGPD y a multas enormes, independientemente de que la empresa esté localizada en la UE. Esto prácticamente impone la conformidad con el RGPD y tiene un impacto significativo en las empresas de países fuera de la UE.

Al contrario de la directriz legislativa existente para los estados miembros de la UE, el RGPD establece una vinculación legal directa sobre todos los estados miembros de la UE. El reglamento también se aplica a entidades extranjeras no localizadas en la UE, pero que suministran bienes o servicios a residentes de la UE o procesan datos personales de residentes de la UE. Una violación grave del RGPD está sujeta a una multa de hasta 4% de los ingresos globales anuales o € 20 millones, lo que sea mayor. Además de esto, una violación del RGPD puede estar sujeta a acciones colectivas o acciones civiles contra individuos. Como resultado, es necesario extrema cautela de las empresas que operan o se expanden para la UE.

Además de los datos personales generales, como nombres y números de teléfono, el RGPD considera un alcance más amplio de datos personales, como identificadores online (direcciones IP y cookies), así como informaciones genéticas e informaciones biométricas. El monitoreo sistematizado en larga escala de espacios públicos usando sistemas de CCTV es categorizado como procesamiento de datos personales con altos riesgos potenciales de invasión de privacidad.

A continuación están los elementos-clave que los controladores y procesadores (órgano de consignación de monitoreo de CCTV y cuerpo ejecutor) deben tener en mente al monitorear o procesar datos personales usando sistemas de CCTV (cámaras de vigilancia, dispositivos de almacenamiento y software de monitoreo).

2.1. Principales detalles del RGPD

2.1.1. Principios relacionados al tratamiento de datos personales

Principios de legalidad, equidad y transparencia

Los datos personales deben ser tratados de forma lícita, justa y transparente en relación al titular de los datos.

Principio de la limitación de la finalidad

Los datos personales deben ser recolectados para fines especificados, explícitos y legítimos y no tratados de forma incompatible con estos fines.

Principio de la minimización

El tratamiento de datos personales debe ser adecuado, relevante y limitado a lo necesario con relación a las finalidades para las cuales son procesados.

Principio de la limitación del almacenamiento

Los datos personales deben ser conservados de una forma que permita la identificación de los titulares de los datos por un período no superior al necesario para las finalidades para las cuales los datos personales son procesados.

Principios de integridad y confidencialidad

Los datos personales deben ser procesados para garantizar la seguridad adecuada, incluyendo protección contra procesamiento no autorizado o ilegal, pérdida accidental, destrucción o daños por medio de medidas técnicas y organizativas apropiadas.

Principio de la precisión

El procesamiento de datos personales debe ser preciso y deben ser tomadas medidas razonables para mantenerlos actualizados. Por fin, el controlador es responsable de cumplir y probar la conformidad con los seis principios anteriores.

2.1.2. Protección de los derechos de los titulares de los datos

El RGPD refuerza los derechos del titular de los datos con la adición del derecho a la eliminación ("derecho al olvido"), portabilidad de datos y toma de decisión individual automatizada (creación de perfiles).

Derecho a la prestación de informaciones

El responsable del tratamiento debe suministrar al titular de los datos informaciones relacionadas con el tratamiento de datos de forma concisa, clara y comprensible.

Derecho de acceso

El titular de los datos tiene el derecho de solicitar

i. confirmación del tratamiento de sus datos personales y
ii. acceso a sus datos personales.

Derecho de rectificación

El titular de los datos tiene el derecho de solicitar la rectificación de cualesquiera datos personales inexactos o incorrectos.

Derecho al olvido

El titular de los datos tiene el derecho de solicitar al responsable del tratamiento que excluya sus datos personales.

Derecho a la restricción de procesamiento

El titular de los datos tendrá el derecho de restringir o limitar el tratamiento de sus datos personales.

Derecho a la portabilidad de datos

El titular de los datos tendrá el derecho de solicitar la transferencia de datos personales para que puedan ser reutilizados en otros servicios.

Derecho de objeción

El titular de los datos tendrá el derecho de objeción en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de sus datos personales.

Derechos relacionados con la toma de decisiones individuales automatizadas, incluyendo la definición de perfiles

El titular de los datos tiene el derecho de no estar sujeto a una decisión basada exclusivamente en el tratamiento automatizado, incluyendo la definición de perfiles, que produzca efectos jurídicos que le conciernan o que lo afecten significativamente de forma semejante.

2.1.3. Aumento de la responsabilidad del controlador y del procesador

Como persona física, corporación, organización pública o agencia que determina la finalidad y los medios de procesamiento de datos personales, el controlador será responsable de implementar medidas técnicas y organizativas apropiadas para garantizar y ser capaz de demostrar que el procesamiento es realizado de acuerdo con el RGPD, teniendo en cuenta la naturaleza, alcance, contexto, finalidades y riesgos del procesamiento de datos personales.

Como persona física, corporación, organización pública o agencia que procesa datos personales en nombre del controlador, el procesador debe procesar datos personales de acuerdo con las instrucciones del controlador.

Registros de actividades de procesamiento

Para demostrar la conformidad con el RGPD, el controlador y el procesador deben mantener un registro de las actividades de procesamiento de datos personales realizadas bajo su responsabilidad. La obligación de mantener registros de las actividades de procesamiento no se aplica a corporaciones con menos de 250 funcionarios. Sin embargo, tales obligaciones se aplican independientemente del número de trabajadores, si

i. el tratamiento de datos personales presenta riesgos de violación de los derechos o libertades del titular de los datos o
ii. procesar datos sensibles.

Una Evaluación de Impacto en la Privacidad debe ser realizada en casos de monitoreo sistematizado en larga escala de espacios públicos. Si la Evaluación de Impacto en la Privacidad concluye que existe un riesgo de violación de los derechos y de la libertad de un titular de datos, las actividades de tratamiento deben ser registradas independientemente del número de trabajadores.

Protección de datos por defecto

El responsable del tratamiento debe revisar la protección de datos personales en la ingeniería y en el desarrollo de sistemas y procesos informáticos y aplicar medidas técnicas y organizativas adecuadas para demostrar que la protección de datos personales fue implementada en las actividades de tratamiento de datos personales.

Medidas técnicas y organizativas apropiadas incluyen seudonimización de datos personales, desidentificación y minimización del procesamiento de datos personales. Las protecciones necesarias también deben ser implementadas en el procesamiento de datos personales para cumplir el RGPD.

Además de esto, el responsable del tratamiento debe revisar y garantizar que las predefiniciones de los productos, servicios o aplicaciones que procesan datos personales respeten la privacidad. Cámaras de videomonitoreo usadas en sistemas de transporte público están entre las aplicaciones que exigen esta revisión. Por ejemplo, las medidas técnicas y organizativas necesarias deben ser implementadas para garantizar la conformidad en relación

i. a la cantidad de datos personales recogidos,
ii. a la extensión del tratamiento de datos personales,
iii. al período de almacenaje,
iv. a la rendición de cuentas

Evaluación de Impacto sobre la Protección de Datos (AIPD)

Si la recogida o el tratamiento de datos, bajo cualquier forma, es susceptible de resultar en elevado riesgo para los derechos y libertades de los individuos, como en el caso de sistemas de CCTV que efectúan monitorización sistematizada y en larga escala de espacios públicos, es necesario realizar una evaluación de impacto sobre la protección de datos. Esto ocurre porque los sistemas de CCTV recolectan datos personales mientras el titular de los datos no sabe quién está recolectando sus datos personales y cómo estos datos serán usados. Es difícil para los individuos evitar tornarse sujetos a tal procesamiento en áreas públicas.

El objetivo de una Evaluación de Impacto sobre la Protección de Datos es identificar y minimizar riesgos de violación de privacidad y violación de la protección de datos personales, y debe ser realizada antes que el procesamiento de datos personales ocurra.

La evaluación de impacto sobre la protección de datos debe incluir

i. una evaluación del tratamiento programado y de la finalidad del tratamiento
ii. la necesidad del tratamiento de datos personales y el principio de la equidad

iii. riesgos para los derechos y la libertad del titular de los datos

iv. protecciones para mitigar estos riesgos

La evaluación de impacto sobre la protección de datos debe también incluir la opinión del titular de los datos afectado o de sus representantes. Para los sistemas de CCTV, se aplica a los funcionarios o al público en general, que son objeto de monitoreo.

Cargo de Director de protección de datos (DPD)

Organizaciones públicas u organizaciones que exigen monitoreo en larga escala, periódico y sistematizado de titulares de datos deben nombrar un DPD. De acuerdo con el grupo de trabajo del artículo 29 de la UE, esto también se aplica a empresas que suministran vigilancia de CCTV como servicio (SaaS) en áreas públicas, como shopping centers. Por otro lado, puede no aplicarse a corporaciones privadas que usan sistemas de CCTV para monitorear el interior o las cercanías de sus edificios. Si un DPD no es designado por no ser necesario, las razones para esta decisión deben ser documentadas.

Se recomienda que el DPD preste orientación sobre la realización o no de AIPD, metodologías de ejecución, órganos ejecutores (internos o subcontratados), medidas de seguridad para mitigar riesgos y evaluaciones de seguimiento.

La independencia del DPD en relación al responsable del tratamiento o al subcontratante en el ejercicio de sus funciones debe ser garantizada y el responsable del tratamiento es, en última instancia, responsable de la AIPD.

Responsabilidades de procesadores y procesadores subcontratados

El controlador puede hacer que el procesador procese datos personales en nombre del controlador, siempre que la conformidad con el RGPD y las protecciones técnicas y administrativas adecuadas sean garantizadas. El controlador será responsabilizado por las acciones del procesador, y el procesador asume las obligaciones y responsabilidades de responder a solicitudes relativas a los derechos del titular de los datos. Por tanto, es esencial que el controlador especifique el alcance de tareas y responsabilidades del procesador en el contrato de consignación de procesamiento de datos personales celebrado con el controlador.

Si el procesador subcontrata el tratamiento de datos personales para un procesador secundario, el procesador original deberá obtener el consentimiento por escrito del controlador. Las obligaciones derivadas del contrato con el controlador deben ser incluidas en el contrato de subcontratación. Esto también garantiza que el controlador asuma responsabilidades por las acciones de los procesadores subcontratados.

Las organizaciones que consignan o subcontratan su servicio de vigilancia por CCTV deben observar este hecho. Además de esto, las organizaciones que buscan

emplear procesadores que realizan procesamiento basado en nube de vídeos de vigilancia por CCTV también deben observar las responsabilidades del controlador mencionadas anteriormente.

Medidas de seguridad cibernética para garantizar la seguridad adecuada

El controlador es responsable de cumplir y demostrar el cumplimiento de los principios de integridad y confidencialidad, o sea, garantizar medidas de seguridad adecuadas contra el procesamiento no autorizado/ilegal, pérdida/destrucción accidental o daños.

Además de esto, el controlador debe implementar las medidas de seguridad necesarias dentro del proceso de procesamiento de datos personales para garantizar la conformidad con el RGPD en el proceso de ingeniería y desarrollo de sistemas de TI. El controlador también debe implementar medidas técnicas y organizativas para garantizar que las configuraciones estándar de productos, servicios, procesos de aplicaciones (acceso, transferencia, almacenamiento, liberación, uso, destrucción, etc.) y el propio procesamiento de datos personales estén dentro del alcance mínimo para el propósito específico del procesamiento de datos personales.

A medida que más configuraciones de sistema de CCTV utilizan cámaras de red basadas en IP, dispositivos de almacenamiento de red y VMS, la fuga, la falsificación, la adulteración, la pérdida y el abuso de datos personales por hackers o infiltrados malintencionados está aumentando. Este aumento resultará naturalmente en un riesgo más alto de violaciones de la privacidad y violaciones de la protección de datos personales. Por tanto, para estar en conformidad con el RGPD, el controlador debe establecer sistemas de CCTV o actualizar los existentes para que ofrezcan mejor seguridad de red, control de usuarios internos y recursos antiabuso.

Acciones tomadas en el caso de violación de datos personales

Al tomar conocimiento de una violación de datos personales, el procesador debe notificar al controlador sin demora. El controlador debe, entonces, notificar a la autoridad de control sin demora injustificada y, ciertamente, en el plazo de 72 horas. El controlador debe también notificar sin demora al titular de los datos, excluyendo cuando

i. los datos personales estén adecuadamente protegidos por medidas de seguridad, como criptografía,
ii. la violación no afecte significativamente los derechos del titular de los datos, o
iii. notificar al titular de los datos implique un esfuerzo no proporcional.

2.2. Penas para violaciones del RGPD y efectos en cascada

En el caso de violación importante de los principios relacionados con el tratamiento de datos personales, consentimiento para la recogida de datos personales, protección de los derechos de los titulares de los datos o restricciones a transferencias para países terceros, el mayor valor entre 4% de los ingresos globales anuales o € 20 millones será impuesto como penalidad.

Para violaciones menos graves, como la violación de las responsabilidades de notificación, el mayor valor entre 2% de los ingresos globales anuales y € 10 millones será impuesto como penalidad.

Para violaciones a las cuales tales penalidades no son impuestas, otras sanciones, como acusaciones penales, pueden ser impuestas. Además de esto, los titulares de datos cuyos datos personales hayan sido violados pueden pedir una indemnización por daños. Por tanto, las empresas que no cumplan el RGPD pueden enfrentar caídas significativas en la reputación de la marca e incluso el posible cierre de las operaciones. El incumplimiento del RGPD también puede llevar a la pérdida de empleos en nivel individual.

Es por eso que todas las empresas, incluyendo aquellas que ya operan en Europa, así como aquellas que planifican expandirse para Europa, deben estar completamente preparadas para la conformidad con el RGPD. Como existe una fuerte posibilidad de que el RGPD se torne el estándar global de protección de datos personales, cualquier empresa que busque operar en el mercado global debe estar muy atenta a largo plazo.

Es importante notar que los servicios públicos de CCTV y nube de vídeo que exigen protección de datos personales y privacidad son categorizados como un grupo de alto riesgo y pueden estar sujetos a grandes multas en el caso de violación. Por consiguiente, los controladores o procesadores que prestan servicios de videovigilancia a residentes europeos dentro o fuera de Europa deben estar bien preparados.

3.1. Principios relacionados al procesamiento de datos personales, privacidad por diseño y defecto

3.1.1. Limitación del período de almacenamiento y destrucción segura

De acuerdo con el principio de la limitación del período de almacenamiento, las personas en vídeos que hayan superado el período de almacenamiento no deben ser identificadas para evitar la identificación.

Para hacer esto, es aconsejable obligar que el período de almacenamiento de configuración de vídeos sea correspondiente al período de almacenamiento especificado por ley o por el contrato de consentimiento de recogida de datos personales para evitar que los vídeos sean almacenados indefinidamente y suministrar un recurso de exclusión automática para vídeos cuyo período de almacenamiento definido expiró. De la misma forma, registrar y gestionar el período de almacenamiento definido, el nombre del archivo de vídeo excluido, la hora y la fecha de exclusión y el nombre de la persona que definió el período de almacenamiento garantizarán la transparencia en el procesamiento de datos personales.

A fin de garantizar la legalidad y la transparencia del procesamiento de datos personales, la autorización para modificar el período definido o cancelar el período de almacenamiento solo debe ser concedida al administrador. El historial de asuntos relacionados al período de almacenamiento, como el período de almacenamiento recién definido, la fecha y la hora de las modificaciones o la cancelación del período de almacenamiento, y la persona que hizo esas modificaciones, debe ser registrado y administrado.

Los productos Hanwha Techwin suministran recursos relacionados para garantizar que los vídeos no sean recolectados o almacenados más allá del período de almacenamiento especificado por las leyes o directrices relevantes. Por ejemplo, en el caso de dispositivos de almacenamiento de vídeo en red, el período de almacenamiento de datos de vídeo puede ser definido para un número específico de días (1 - 400) desde el día de la grabación, y los datos de vídeo son excluidos de modo automático y secuencial a medida que el período de almacenamiento definido expira.

3.1.2. Restricción de grabación de audio

En conformidad con el principio de la minimización del procesamiento de datos personales, la grabación de audio con uso de sistemas de vigilancia por vídeo es restringida. La grabación de conversaciones entre individuos representa un alto riesgo de invasión de privacidad, por tanto, su grabación de audio no está permitida. Sin embargo, sistemas de vigilancia por vídeo en los cuales la grabación de datos de audio está permitida por razones de seguridad pública exigen grabación de vídeo y audio.

Por tanto, es aconsejable que el recurso de grabación de audio sea desactivado por defecto, pero debe ser controlable separadamente de la grabación de audio. Si la grabación de audio es necesaria, el permiso para habilitar este recurso solo deberá ser concedido a un administrador certificado.

La modificación de las definiciones solo debe ser permitida cuando la grabación sea justificable. Avisos sobre el recurso de audio deben ser exhibidos, y el historial de modificaciones de configuración, hora y fecha de las modificaciones y la persona que hizo modificaciones deben ser registrados y administrados.

De acuerdo con el principio de privacidad por defecto, el recurso de grabación de audio está desactivado en los productos Hanwha Techwin por defecto. Sin embargo, como los datos de audio son una fuente importante que puede suministrar informaciones útiles para los usuarios del sistema de CCTV, los recursos de Detección de Audio, Clasificación de Sonido, Cancelación de Eco de Audio y Reducción de Ruido de Audio son suministrados por defecto.

Los recursos de Detección de Audio y Clasificación de Sonido son procesados en la propia cámara sin realmente grabar el audio, y Hanwha Techwin planifica desarrollar tecnologías inteligentes de análisis de audio, como el Rastreo de Localización de Sonido, usando micrófonos multicanal para tratar con las varias demandas del cliente. Naturalmente, la restricción de audio para otros fines que no sea el análisis de audio será restringida, y el principio de la minimización del procesamiento de datos personales será mantenido.

3.1.3. Restricción de la grabación con PTZ además del alcance de la finalidad

De acuerdo con el principio de la minimización del procesamiento de datos personales, la grabación y la recogida de vídeos en aplicaciones de vigilancia por vídeo CCTV deben ser restringidas a situaciones relevantes que cumplan la finalidad de la vigilancia por vídeo CCTV.

Al contrario de las cámaras fijas, las cámaras PTZ son capaces de cambiar de dirección e incluso ampliación, lo que puede representar un riesgo de violaciones de privacidad. Por tanto, es necesario suministrar un recurso que restrinja el alcance de movimiento panorámico (rotación horizontal) e inclinación (rotación vertical) de acuerdo con la finalidad pretendida para evitar violaciones de privacidad.

Para garantizar la transparencia y la legalidad de la recogida y del almacenamiento de vídeos usando cámaras PTZ, se recomienda que el alcance de movimiento panorámico e inclinación permitido sea definido por un administrador certificado en el momento de la instalación. Además de esto, es aconsejable que el permiso para modificar o retirar las configuraciones del intervalo de movimiento panorámico e inclinación sea dada solamente a un administrador certificado. El historial de definición/cancelación, la fecha y la hora de definición/cancelación y la persona que modificó las configuraciones

también deben ser registrados y administrados. Además de esto, la configuración de las cámaras para interrumpir la grabación o enmascarar vídeos cuando el intervalo de movimiento panorámico e inclinación exceda el intervalo definido por el administrador certificado también debe ser considerada.

Así como todos nuestros productos, las cámaras PTZ de Hanwha Techwin ofrecen un desempeño líder mundial, cumpliendo el principio de minimización del procesamiento de datos personales. Al soportar hasta 24 máscaras de privacidad, las cámaras PTZ de Hanwha Techwin mantienen alta precisión con máscaras de privacidad sincronizadas con la operación de visión panorámica, inclinación y zoom, impidiendo la recogida de vídeos que no cumplen el propósito de la vigilancia por vídeo. Además de esto, el recurso PT Limit, que permite que la cámara solamente haga panorámica e inclinación dentro del alcance definido por el usuario, es suministrado por defecto, impidiendo la grabación de vídeos fuera del alcance permitido.

3.1.4. Desidentificación

La necesidad de desidentificación (enmascaramiento, empañamiento, mosaico, etc.) de objetos (personas o matrículas de vehículos) dentro de vídeos de CCTV varía de acuerdo con la finalidad de la recogida de vídeo y del ambiente de procesamiento.

El RGPD define que, si es posible, se cumpla el objetivo procesando datos desidentificados, como el almacenamiento de datos de vídeo para fines de interés público, investigación científica, histórica o estadística, así como al usar los datos de vídeo sin el consentimiento del titular de los datos para fines diferentes del propósito original de recogida.

Por otro lado, si el pedido de acceso es legítimo (p. ej., en el caso de emergencia o con autorización de órganos de aplicación de la ley/judiciario, etc.), pero es considerado que el suministro del vídeo como esté presenta riesgos de infringir la privacidad de terceros incluidos en el vídeo, puede ser necesaria la desidentificación de terceros en el vídeo.

Para minimizar el procesamiento de datos personales y maximizar la protección de la privacidad, también deben ser considerados modos de suministrar vídeos no identificados al monitorear en tiempo real o reproducir vídeos grabados, dependiendo de los permisos de acceso, como permitir vídeo como esté para administradores (cuenta de administrador) y mostrar solamente vídeos no identificados para el personal de monitoreo de CCTV (cuenta de invitado / usuario). Las ventajas de tales medidas proporcionan varios beneficios, incluyendo la exención del principio de procesamiento de datos personales del RGPD, la reducción de los riesgos de ejecución de los derechos del titular de los datos y mayor facilidad para conformidad y demostración del cumplimiento de las responsabilidades de protección de datos, desidentificando el vídeo lo más rápido posible.

El RGPD exige la implementación de medidas técnicas y organizativas apropiadas, como seudonimización o desidentificación desde la etapa de diseño para cumplir el principio de privacidad por diseño y por defecto. Y también requiere medidas técnicas y organizativas para garantizar la seguridad adecuada en el procesamiento de datos personales. Sin embargo, el controlador deberá aplicar medidas técnicas y organizativas adecuadas, teniendo en cuenta la tecnología más reciente, el costo de implementación, la naturaleza y el alcance del procesamiento de datos personales, las circunstancias, la finalidad, el impacto potencial, la gravedad y los riesgos del procesamiento de datos personales sobre los derechos y la libertad del titular de los datos.

Para aplicaciones de vigilancia por vídeo CCTV, reconocer y desidentificar individuos en cada cuadro del vídeo representa desafíos técnicos, de desempeño y de costo significativos. Por tanto, es necesario determinar si la desidentificación es o no obligatoria para alcanzar la finalidad del sistema de CCTV. Si no es obligatorio, las ventajas y los costos de la desidentificación deben ser ponderados para determinar la necesidad de desidentificación.

Para proteger la privacidad de los titulares de los datos y alcanzar el equilibrio ideal de seguridad y protección en vídeos de CCTV, Hanwha Techwin colaborará con colaboradores para suministrar un producto que transmita vídeos enmascarados en tiempo real al monitorear y productos capaces de enmascarar personas o zonas específicas al suministrar copias de backup para cumplir los derechos de acceso.

3.2. Protección de los derechos de los titulares de los datos

3.2.1. Derecho de acceso

Un cliente que se sintió incómodo con las cámaras de CCTV instaladas en una tienda de departamentos consulta el sitio web de la tienda para confirmar si los vídeos de CCTV son procesados legítimamente y verificar si él / ella fue grabado. En respuesta, a menos que el pedido del titular de los datos carezca de motivos claros o sea excesivo, el controlador debe poder suministrar las informaciones necesarias para verificar el procesamiento adecuado de los datos personales, así como los vídeos grabados del titular de los datos en formato electrónico en el plazo de un mes.

Para ello, el controlador puede solicitar al solicitante las informaciones necesarias para verificar si él/ella es titular de datos con derecho a tal pedido e informaciones detalladas para localizar el vídeo en cuestión, como fecha, hora y lugar.

A fin de garantizar fácilmente el derecho de acceso, el usuario del dispositivo de almacenamiento (NVR / DVR o VMS) debe acceder al vídeo almacenado después de autenticar los permisos, usar interfaz y recurso de investigación inteligente

para localizar el vídeo correspondiente con precisión y rapidez, y verificar el vídeo exhibido en la pantalla y determinar si él debe ser suministrado como está o si terceros, excluyendo el titular de los datos solicitados, deben ser desidentificados (enmascaramiento, empañamiento, mosaico, etc.).

Si el vídeo correspondiente contiene solamente al titular de los datos solicitado, el vídeo podrá ser suministrado como está. Si existen terceros en el vídeo, se debe determinar si hay un riesgo de violación de privacidad para los terceros en el caso que el vídeo sea suministrado. Como resultado de esta evaluación, la desidentificación debe ser implementada si es considerada necesaria.

Además de esto, las informaciones necesarias para verificar el procesamiento legítimo de datos personales incluyen el destinatario de los datos personales (vídeo grabado) y el período de almacenamiento. Para tratar con estas solicitudes fácilmente, es aconsejable que el dispositivo de almacenamiento cree y almacene una lista de todos los usuarios con acceso al vídeo, historial de procesamiento de cada vídeo (como una copia del registro de grabación, backup de vídeos, usuarios que realizaron estas acciones, hora y fecha de las acciones, el período de almacenamiento del vídeo, etc.) y debe ser utilizada una interfaz de usuario que les permita a los usuarios autorizados realizar fácilmente búsquedas y generar archivos electrónicos.

Si demora un período significativo para suministrar los datos de vídeo después del recibimiento de la solicitud, es aconsejable tomar las medidas necesarias para evitar la exclusión automática cuando el período de almacenamiento de los datos de vídeo en cuestión expire.

3.2.2. Derecho al olvido (derecho a la eliminación)

En los pedidos de videovigilancia por CCTV, a pesar de que el derecho a la eliminación sea semejante al derecho de acceso por el cual los vídeos del individuo deben ser buscados, la diferencia es que el cumplimiento del derecho de acceso involucra la retención de la copia original del vídeo de CCTV, al paso que el derecho a la eliminación exige que la copia original del vídeo de CCTV sea destruida. Otra diferencia es que la solicitud por el derecho a la eliminación probablemente será hecha después que una violación de privacidad ya haya ocurrido, por la divulgación externa de un vídeo de CCTV, como en Internet, por alguien.

Un ejemplo de una solicitud basada en el derecho al olvido es el siguiente. Vamos a suponer que la Celebridad A, que vive en una villa de lujo, haya sido grabada entrando en casa con otra Celebridad B por las cámaras de CCTV en el estacionamiento, y el vídeo se filtró. En este caso, A puede solicitar, al administrador del CCTV, la eliminación de vídeos en los cuales aparece con base en la violación de privacidad. El administrador de CCTV debe responder a la solicitud de A, a menos que ella se encuadre en cinco casos* en los cuales se puede negar la solicitud de remoción.

Cinco circunstancias en las cuales el pedido de eliminación puede ser negado

- para el ejercicio de los derechos a la libertad de expresión y de información
- para la ejecución de deberes de interés público o ejecución de obligaciones legales para el ejercicio de deberes
- para intereses públicos relacionados a la salud
- para archivar una finalidad de interés público, investigación científica o histórica o para fines estadísticos
- para el ejercicio o defensa de acciones judiciales

Sin embargo, si una imagen de CCTV es recolectada de acuerdo con una finalidad legítima (por ejemplo, prevención e investigación de crímenes) y es procesada de acuerdo con procedimientos legítimos, el vídeo debe ser almacenado por un período de tiempo definido para alcanzar este objetivo. Por tanto, si un pedido de eliminación es hecho sin que el vídeo de CCTV sea filtrado primero, la respuesta puede ser diferente si los intereses, derechos y libertades del titular de los datos tuvieren precedencia sobre el motivo legítimo para almacenar el vídeo.

Si la solicitud basada en el derecho a la eliminación también es considerada legítima y necesaria, es aconsejable que el usuario del dispositivo de almacenamiento (NVR o VMS) pueda acceder al vídeo almacenado después de la autenticación de los permisos y que el dispositivo de almacenamiento ofrezca una interfaz de usuario y recursos de investigación inteligente para encontrar el vídeo correspondiente de forma rápida y precisa. El usuario debe verificar el vídeo exhibido en la pantalla y determinar si debe borrarlo o solamente enmascarar al titular de los datos solicitado. Si el vídeo contiene solamente al titular de los datos solicitado, el vídeo podrá ser excluido. Sin embargo, si terceros fueren incluidos y el vídeo tiene que ser preservado para alcanzar los objetivos de recogida y almacenamiento, puede ser necesario enmascarar solamente al titular de los datos solicitado.

Por otro lado, si una copia del vídeo ya se ha filtrado en Internet, el titular de los datos podrá solicitar que cualesquiera copias del vídeo sean borradas. En este caso, el controlador debe notificar al administrador del sitio web y garantizar la exclusión de la copia.

Para tratar con estas solicitudes fácilmente, es aconsejable que el dispositivo de almacenamiento cree y almacene el historial de procesamiento de cada vídeo (como una copia del registro de grabación, backup y exclusión de vídeos, usuarios que realizaron estas acciones y hora y fecha de las acciones) y una interfaz de usuario debe ser suministrada para permitir que usuarios autorizados realicen búsquedas fácilmente. Usando estos sistemas, el usuario podrá rastrear cuándo, por quién y por cuál ruta el vídeo se filtró, haciendo posible cumplir las responsabilidades de notificación fácilmente.

3.2.3. Solución de análisis de vídeo Hanwha Techwin

Hanwha Techwin ofrece un conjunto de herramientas que garantizan fácil búsqueda, identificación y recogida de datos grabados individualmente por medio de productos estándar o colaboradores de tecnología.

Usando los recursos de Reconocimiento Facial, Detección de Rostro, Detección de Movimiento, Resumen de Vídeo y Búsqueda Inteligente suministrados por Hanwha Techwin, el controlador puede tratar con solicitudes de un titular de datos individual basadas en el derecho de acceso o en el derecho a la eliminación, cifrar los resultados buscados y enviarlos al solicitante. El conjunto de chips de procesamiento de imagen de última generación que está siendo desarrollado por Hanwha Techwin contará con tecnología de análisis de vídeo basada en aprendizaje profundo para identificar una variedad más amplia de objetos, como personas, vehículos y animales, posibilitando tratar con las necesidades de controladores y procesadores más rápidamente.

3.3. Gestión de problemas de seguridad cibernética

3.3.1. Gestión de permisos de acceso

Usar solamente una cuenta de administrador con los permisos más altos en el sistema puede debilitar la seguridad de todo el sistema si la cuenta es comprometida, llevando al procesamiento no autorizado, procesamiento ilegal, pérdida accidental, destrucción o daños de informaciones personales. Para evitar esto, es esencial un recurso para adicionar cuentas de usuario y restringir los permisos de cada cuenta.

Además de esto, si un intruso intenta o logra infiltrarse en el dispositivo de red, podrán ocurrir incidentes de seguridad, como hacer login con permisos de administrador, crear cuentas de usuario no autorizadas o conceder permisos excesivos.

Para evitar esto, Hanwha Techwin ofrece recursos para crear usuarios o grupos de usuarios con varios niveles y permisos para acceder a la cámara, al dispositivo de grabación o al VMS. Utilizando este recurso, el administrador puede suministrar solamente las funciones mínimas exigidas por el usuario, garantizando una seguridad adecuada que evite el abuso de permisos excesivos y el uso indebido de datos personales.

Hanwha Techwin también ofrece una variedad de recursos de almacenamiento y verificación de registros, incluyendo registros sobre concesiones de permiso, modificaciones y exclusiones, para que controladores y procesadores puedan analizar el camino de intrusión usando registros de dispositivos o determinar cómo ocurrieron incidentes de seguridad, proporcionando, así, un nivel adecuado de seguridad para minimizar los riesgos de violación de datos personales.

3.3.2. Control de acceso

Varios equipos son necesarios para impedir el acceso a dispositivos por intrusos. Estos equipos deben incluir contramedidas contra ataques de fuerza bruta. Si el usuario compra y usar un dispositivo protegido por contraseña sin modificar la contraseña estándar, la contraseña podrá ser fácilmente adquirida online a partir de manuales del usuario. Los usuarios deben tener esto en mente para evitar violaciones críticas de seguridad.

Si el equipo de vigilancia por vídeo está conectado a una red pública, el recurso de encaminamiento automático, que permite búsquedas fáciles en productos, puede ser usado como una ruta para secuestrar datos personales. Si un intruso intencionalmente modificar las configuraciones de fábrica del dispositivo para excluir registros, puede ser difícil analizar o rastrear la ruta de intrusión en el futuro. Por tanto, los recursos para almacenar los registros de acceso son uno de los recursos esenciales en el control de acceso.

Además de esto, el firmware suministrado para el equipo de videovigilancia contiene informaciones esenciales del equipo y, por tanto, no debe ser posible analizar a partir del exterior, debiendo ser incluido un dispositivo para verificar la integridad del firmware distribuido por el fabricante.

Política de contraseñas

Para evitar el uso de contraseñas fácilmente previsibles, Hanwha Techwin impone un nivel mínimo de complejidad de combinación de letras, números y caracteres especiales; repeticiones (p.ej., 1111, aaaa, etc.) y secuencias (p.ej., 1234, abcd, etc.) no están permitidas. Al imponer esta regla de contraseña, Hanwha Techwin impide el acceso de intrusos por medio de adivinación o ataques de fuerza bruta.

Restricción de acceso no autorizado

A fin de impedir el acceso no autorizado al equipo, Hanwha Techwin soporta filtrado de IP, que define el rango de IP de red permitido o prohibido para acceder cámaras o dispositivos de grabación de Hanwha Techwin.

La entrada de contraseña es temporalmente restringida después de 5 intentos de login fallidos para impedir el acceso por medio de ataques de fuerza bruta. El sistema tampoco permite redefiniciones remotas de contraseña sin autenticación de derechos de administrador (solamente acceso local), impidiendo así el acceso no autorizado al equipo.

Conexión segura a la red pública

La política de Hanwha Techwin no permite puertos de servicio remoto arbitrarios que pueden ser usados para acceso al shell, como Telnet, SSH y servidor FTP en cámaras, dispositivos de grabación o VMS. Hanwha Techwin utiliza codificación segura

sin back-doors en los códigos de software y realiza pruebas y monitoreo continuos. El recurso de encaminamiento automático de puertos (NAT Traversal) del UPNP Discovery, que facilita la búsqueda de productos en una red pública, también puede ser una ruta para el secuestro de datos personales, por eso también está prohibido. Se debe notar que el recurso de encaminamiento automático de puertos es permitido en cámaras domésticas conectadas a la nube para suministrar servicios, no obstante, él usa puertos de streaming de vídeo aleatorios para aumentar la seguridad.

Almacenamiento y verificación de registros de conexión

Los productos Hanwha Techwin registran cualesquiera modificaciones en las configuraciones del dispositivo, incluyendo cámaras, dispositivos de grabación y VMS, haciendo posible descubrir cuáles modificaciones fueron hechas y por quién, simplemente verificando el registro. La mayoría de las entradas de registro incluye las configuraciones anteriores y las nuevas configuraciones para facilitar la reversión.

En el caso de cámaras y dispositivos de grabación, los registros son preservados incluso después de una redefinición de fábrica. El recurso que no permite la redefinición de registros impide que intrusos escondan sus rastros redefiniendo el dispositivo y puede ser útil al analizar y rastrear rutas de infiltración.

Prevención de malware

El firmware usado en las cámaras Hanwha Techwin y en los dispositivos de grabación es cifrado, de modo que las informaciones críticas incluidas en el firmware no pueden ser arbitrariamente analizadas, forjadas o adulteradas. El VMS y las aplicaciones móviles (iOS) son firmados con la clave privada de Hanwha Techwin, emitida por una institución de CA confiable. Esto garantiza que la aplicación en cuestión sea distribuida por Hanwha Techwin y esté libre de falsificación o adulteración por malware. Además de esto, el firmware de las cámaras domésticas Hanwha Techwin es actualizado automáticamente para la versión más reciente usando un servidor dedicado, facilitando la mejoría de la seguridad y estabilidad.

3.3.3. Transmisión segura

Para proteger los datos personales (informaciones de autenticación del usuario, flujos de vídeo) compartidos dentro del sistema de CCTV (cámaras de vigilancia, dispositivos de almacenamiento y software de monitoreo), debe ser implementada una protección para las informaciones transmitidas por la red.

Hanwha Techwin usa la autenticación HTTP Digest durante las transmisiones HTTP de cámaras, dispositivos de grabación y VMS para el servidor y el cliente para proteger la contraseña del usuario. El uso de HTTPS protege la contraseña del usuario y los flujos de vídeo transmitidos vía RTSP. Sin embargo, como el modo HTTPS protege solamente los datos enviados en el protocolo HTTP, como informaciones de autenticación del usuario, la configuración adicional de encapsulado RTSP para

HTTPS es necesaria en el extremo del cliente para proteger los flujos de vídeo transmitidos por el protocolo RTSP. Las cámaras domésticas conectadas a la nube usan el SRTP, un protocolo de comunicación de multimedia seguro basado en RTP, para proteger los flujos de vídeo.

3.3.4. Almacenamiento seguro

Informaciones importantes del sistema (incluyendo informaciones de autenticación del usuario) almacenadas en las cámaras de vigilancia, dispositivos de almacenamiento y software de monitoreo deben ser protegidas contra posibles vulnerabilidades de seguridad o falta de seguridad física para evitar el uso no autorizado. Hanwha Techwin usa criptografía unidireccional por hash de informaciones de autenticación del usuario (contraseña) de cámaras, dispositivos de almacenamiento y VMS, y las almacena con seguridad usando criptografía bidireccional, si es necesario.

3.3.5. Versión segura (Backup)

Los datos personales (archivos de vídeo) almacenados en sistemas de CCTV (cámaras de vigilancia, dispositivos de almacenamiento y software de monitoreo) deben ser protegidos para que no puedan ser reproducidos o abusados arbitrariamente por usuarios no autorizados, aunque sean liberados (copiados) del sistema.

Hanwha Techwin aplica protección por contraseña al hacer backup de archivos para la formación de archivos SEC, que es un formato de backup propio, a partir de los dispositivos de almacenamiento y VMS, y también encripta los archivos de vídeo. Una vez que el archivo es cifrado, él no puede ser reproducido por usuarios no autorizados, protegiendo con seguridad los datos personales, aunque el archivo de vídeo sea filtrado. Además de esto, el player (Backup Viewer) necesario para reproducir el archivo es automáticamente incluido en el archivo SEC, lo que significa que los usuarios pueden reproducir el archivo solamente haciendo clic dos veces en el archivo SEC sin la necesidad de instalar players adicionales.

3.3.6. Prevención de falsificación y adulteración

Los datos personales (archivos de vídeo) almacenados en sistemas de CCTV (cámaras de vigilancia, dispositivos de almacenamiento y software de monitoreo) deben ser protegidos para que no puedan ser arbitrariamente falsificados o adulterados por usuarios no autorizados, aunque sean liberados (copiados) del sistema.

Cuando los archivos son copiados de los dispositivos de almacenamiento de Hanwha Techwin o VMS en el formato de archivo SEC, él no puede ser abierto con software de edición normal, evitando falsificación y adulteración de los archivos. Aunque el archivo sea forjado o adulterado, las informaciones de hash del vídeo son marcadas con marca de agua en cada cuadro, lo que posibilita la identificación de

cuadros específicos que fueron adulterados. Y al extraer el vídeo como un archivo SEC del SSM, que es el VMS de Hanwha Techwin, el recurso de firma electrónica es soportado. Él verifica si el vídeo del asunto es extraído del Hanwha Techwin SSM y puede ser usado como prueba de que el vídeo está libre de falsificación o adulteración. La marca de agua y la firma electrónica pueden ser verificadas usando el Visualizador de Backup incluido en el archivo SEC.

4. Conclusión

Debido a su aplicabilidad extraterritorial, alcance expandido de datos personales, estándares de procesamiento legal reforzados, derechos expandidos de los titulares de datos, obligaciones de notificación de violación de datos personales, requisitos de designación de DPD, mayor responsabilidad de las corporaciones, gobernanza reforzada y enormes multas para prepararse para las demandas de los tiempos, promoviendo la economía digital, incluyendo big data, se espera que el impacto del RGPD sea significativo.

Como las aplicaciones de vigilancia por vídeo de CCTV son categorizadas con procesamiento de datos personales de alto riesgo que monitorea sistemáticamente grandes volúmenes de datos personales de vídeo capturados en espacios públicos, las Evaluaciones de Impacto sobre la Protección de Datos (AIPD) deben ser realizadas y un Director de protección de datos (DPD) debe ser designado. Para usuarios de CCTV o proveedores de servicios de vigilancia por vídeo de CCTV, que operan y gestionan aplicaciones de vigilancia por vídeo de CCTV para cumplir el RGPD, medidas deben ser establecidas para probar su conformidad con el principio de la responsabilidad, lo que significa conformidad con los seis principios de procesamiento de datos personales con base en una consciencia correcta del RGPD.

Se debe notar que, cuando el controlador y el procesador de datos personales son obligados a probar la conformidad con el principio de la responsabilidad, no se está exigiendo que el controlador o procesador ofrezca garantías contra violaciones de datos personales, solamente implementando las medidas técnicas y organizativas necesarias. En otras palabras, mientras los controladores o procesadores asumen la responsabilidad inicial por violaciones de datos personales, si ellos prueban el cumplimiento de su responsabilidad y están sujetos a sanciones, como una multa por violaciones de datos personales, la responsabilidad puede ser transferida para el proveedor del sistema de vigilancia por vídeo de CCTV. Este sería particularmente el caso si el proveedor hubiese garantizado la seguridad de los sistemas o de la tecnología, pero la alegación fuese considerada falsa.

Como usted puede ver, desde el punto de vista de la aplicación de vigilancia por vídeo de CCTV, la conformidad con el RGPD no es un problema que afecta solamente a los usuarios finales. Para prepararse de modo eficaz para violaciones de datos personales o fugas causadas por problemas de seguridad cibernética, los usuarios finales, integradores de sistemas y fabricantes de CCTV deben trabajar en estrecha colaboración.

En Hanwha Techwin, continuaremos nuestros esfuerzos incesantes para ofrecer productos que respetan la privacidad, que procesan informaciones relacionadas al usuario y al sistema y datos críticos de vídeo grabados de manera segura, con base en una comprensión correcta y en conformidad con el RGPD (Reglamento General de Protección de Datos).

Hanwha Vision

13488 Centro de I+D Hanwha VIsion
6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL (82) 70.7147.8771-8
FAX (82) 31.8018.3715
http://hanwhavisionamerica.com/

Hanwha Vision