1. Resumen

El grupo Securitas tiene valores sólidos y compartimos un gran sentido de responsabilidad hacia nuestros clientes, empleados y las comunidades en las que operamos: AYUDAMOS A HACER DE SU MUNDO UN LUGAR MÁS SEGURO.

El Consejo de Administración de Securitas AB ("Securitas") ha adoptado esta Política de Privacidad del Grupo y Responsabilidades en Inteligencia Artificial ("Política de privacidad e IA") como parte de la estrategia y el compromiso de **privacidad**, protección de datos y uso responsable de la IA. A su vez la División SSIA ha adoptado la 17. Instrucción de Privacidad e IA responsable.

El director general del Grupo y los presidentes de los países (cuando puedan), emitirán directivas o instrucciones sobre el procesamiento de datos personales y el uso responsable de la IA, cuando proceda. Los documentos directivos emitidos a continuación de esta Política de privacidad e IA no limitan los requisitos de esta Política, sino que proporcionan más detalles en relación con la puesta en práctica de los requisitos.

Esta Política de privacidad se aplica a todas las entidades de Securitas, independientemente de su país de establecimiento. Además de esta política, todas las entidades de Securitas deberán cumplir con todas las leyes y regulaciones locales con respecto a la protección y el procesamiento de datos personales Privacy y las regulaciones y estándares aplicables con respecto al uso responsable de la IA En la medida en que esta Política de privacidad e IA entre en conflicto con cualquier ley o regulación local, prevalecerá la ley o regulación local.

El programa de privacidad de Securitas Group se basa en el principio marco; SU INTEGRIDAD ES NUESTRA PRIORIDAD, así es como ayudamos a hacer de su mundo un lugar más seguro.

Cada entidad de Securitas aplicará su programa de privacidad basado en el principio y cubrirá al menos los componentes básicos descritos en esta Instrucción y en la Política de Privacidad e IA responsable del Grupo.

El marco de IA responsable del Grupo Securitas se basa en principios que se describirán con más detalle en las instrucciones o directivas que se encuentran debajo de esta Instrucción y Política de Grupo. Cada entidad de Securitas aplicará los principios cuando se seleccionen, desarrollen y utilicen los sistemas de IA.

Resumen de los principales cambios desde la última revisión:

- Incorporación de la 17. Instrucción de Privacidad e IA responsable

2.Principios del programa de privacidad

2.1 Procesamiento transparente

La transparencia significa que cada entidad de Securitas sabrá qué y dónde procesa los datos personales y tendrá funciones y responsabilidades claras para su gobierno durante el ciclo de vida del procesamiento. Cada entidad de Securitas informará a las personas sobre el procesamiento de sus datos personales en la forma y con el nivel de detalle requerido por las leyes aplicables y las políticas internas y podrá ejecutar los derechos legales de las personas de manera oportuna.

Legalidad, equidad y transparencia: todos los datos personales deben procesarse de manera legal, justa y transparente en relación con las personas. El principio de procesamiento justo y transparente requiere que las personas estén informadas de la existencia de la operación de procesamiento, sus propósitos y posibles consecuencias. La información a las personas debe incluir al menos lo que se requiere en cada país o jurisdicción local y, por ejemplo, puede proporcionarse a través de un aviso de privacidad o una política de privacidad.

Minimización de datos: los datos personales que se recopilan y procesan de otro modo deben ser adecuados, relevantes y limitados a lo necesario en relación con los fines para los que se procesan. En la medida de lo posible, se utilizarán datos agregados y anonimizados. El Grupo Securitas no utilizará los datos personales o los datos de los clientes de una manera que pueda considerarse como una comercialización de relaciones comerciales específicas.

Derechos de los interesados o de las personas: se tomarán todas las medidas razonables (por ejemplo, estableciendo e implementando procedimientos y políticas internas) para permitir el ejercicio de los derechos legales aplicables a las personas de manera oportuna.

2.2 La integridad guía nuestras decisiones

Principios éticos sobre el tratamiento de datos personales - El marco de privacidad y protección de datos del Grupo Securitas incluirá principios éticos comunes para el tratamiento de datos personales. Los principios éticos se aplicarán al desarrollo de servicios y productos a través del análisis de datos, así como a los servicios y productos que, cuando se aplican a individuos, podría decirse que tienen implicaciones éticas, de privacidad o de integridad. Se realizarán evaluaciones específicas y documentadas de **los riesgos de privacidad** al menos cuando así lo exijan las leyes aplicables o las instrucciones o directivas internas.

Limitación de la finalidad: la finalidad del tratamiento de los datos personales deberá especificarse, ser explícita y legítima antes de iniciar el tratamiento. El tratamiento posterior no será incompatible con la(s) finalidad(es) original(es).

Responsabilidad: cada entidad de Securitas será responsable y deberá poder demostrar el cumplimiento de los principios de esta Política de privacidad e IA.

Las medidas de rendición de cuentas deben incluir documentación escrita y la ejecución de controles que permitan a la entidad demostrar que los procesos son efectivos. Se proporciona una plataforma obligatoria en todo el Grupo para mantener un registro de las actividades de procesamiento, así como otros procesos de gobierno de privacidad. La plataforma común también se utilizará, en la medida de lo posible, para evaluar la madurez con las leyes de protección de datos aplicables en cada división. Cada entidad de Securitas será responsable de seguir los procesos obligatorios en la plataforma como parte de la ambición del Grupo Securitas de gestionar los riesgos de cumplimiento de la privacidad de los datos.

Es obligatorio que los países de SSIA utilicen OneTrust para todas las actividades del programa de privacidad y para el cumplimiento de las leyes de protección de datos.

2.3 Mantener sus datos seguros

Cada entidad de Securitas protegerá los datos personales de acuerdo con las leyes y regulaciones aplicables, las políticas internas y los acuerdos contractuales con los clientes. Al proteger los datos, se tendrá especialmente en cuenta la sensibilidad y la cantidad de datos personales procesados.

Los acuerdos contractuales necesarios deben estar vigentes dentro del Grupo Securitas, así como con clientes y proveedores para mantener seguros los datos personales. Los acuerdos considerarán los requisitos legales e internos para los Acuerdos de procesamiento de datos y los requisitos relacionados con la transferencia de datos personales fuera de un país o región.

Cada entidad de Securitas tendrá la capacidad de descubrir y gestionar un incidente de seguridad que incluya datos personales (**violación de datos personales**) e informarlo internamente y, cuando lo exija la ley o las políticas internas, externamente. Antes de realizar cualquier informe externo, se consultará la parte apropiada de las Comunicaciones del Grupo.

Cada país de SSIA se asegurará de que exista un procedimiento de escalamiento en caso de violación de datos, con roles relevantes definidos, y que cada empleado esté familiarizado con el proceso.

Exactitud: los datos personales serán exactos y, cuando sea necesario, se mantendrán actualizados.

Limitación de almacenamiento: los datos personales no deben conservarse durante un período superior al necesario para lograr los fines del procesamiento, incluidos los requisitos legales de retención de registros. Una vez que se han logrado los propósitos, se recomienda borrar o anonimizar los datos personales.

Integridad y confidencialidad: los datos personales siempre deben procesarse de manera que se garantice la integridad y confidencialidad de los datos personales. Se deben establecer medidas suficientes para proteger los datos contra pérdida, destrucción o alteración no autorizada o accidental, así como para proteger los datos contra el uso o divulgación no autorizados o accidentales. El acceso a los datos personales siempre estará limitado teniendo en cuenta la necesidad de conocer la base y la sensibilidad de los datos.

2.4 Principios globales de privacidad

Todas las personas dentro del Grupo Securitas que manejan datos personales en su trabajo deben estar familiarizadas y cumplir con las leyes de protección de datos y las políticas internas pertinentes.

"Su integridad es nuestra prioridad" será el principio marco, junto con esta Política de privacidad e IA, para Securitas también en jurisdicciones donde no existen leyes más estrictas de privacidad o protección de datos.

Las entidades de Securitas deberán tener una estructura de gobierno de datos sólida y compatible. La estructura de gobierno de datos incluirá, como mínimo, las siguientes funciones: Oficial de Protección de Datos (DPO) / Oficial de Cumplimiento de Datos (DCO), Propietario de la Negocio (Proceso), Propietario del Contrato o Proveedor, Propietario del Activo o Servicio de Información y Propietario de los Datos. El alcance y la definición de estas funciones se definirán en los documentos directivos pertinentes y, en la medida de lo posible, se alinearán entre áreas y funciones, es decir, no serán específicas para el área de privacidad de datos cuando no sea necesario. Se nombrará un DPO/DCO para cada división. Si se considera que un país es una Entidad Cubierta, tal como se define en la Instrucción a la Política de Privacidad Interna del Grupo, también se debe designar a una persona para ese país.

3. Principios de IA

Privacidad y transparencia. La confianza, la transparencia y la integridad son fundamentales para Securitas también en relación con la utilización de la IA. Se proporcionará información clara y precisa sobre el funcionamiento de nuestras soluciones de IA y se respetará la privacidad.

Igualdad y justicia. Antes de poner en uso una solución de IA en Securitas, se deben tener en cuenta los efectos sobre la inclusión y la diversidad. También se evaluará el impacto sobre la sociedad y el medio ambiente.

Calidad de los datos y riesgos de sesgo. La vigilancia es uno de los valores fundamentales de Securitas y, por lo tanto, cada entidad de Securitas debe tomar medidas para mitigar el sesgo o el daño. Esto incluirá la adopción de medidas para garantizar activamente que los datos utilizados en los procesos clave sean de buena calidad.

Seguridad y protección. Los sistemas deben ser robustos y seguros para garantizar prácticas de IA responsables para nuestros clientes, empleados y socios. El uso de soluciones de IA debe tener como objetivo mejorar o hacer que nuestros procesos internos sean mejores o más seguros, o hacer lo mismo para nuestros clientes, empleados y socios.

Innovación y valor de negocio. Securitas debe centrarse en combinar la inteligencia humana y la informática para lograr la eficiencia y la mejora de las ofertas de productos y servicios nuevos y mejorados con la utilización de la capacidad de la IA. Securitas aprovechará responsablemente el poder de la IA para innovar y aportar valor en las oportunidades comerciales tangibles.

La complejidad y la naturaleza multicompetencia de la IA requerirán una colaboración interfuncional. Por lo tanto, se detallarán estos principios de IA, incluido el desarrollo de estructuras de mejor intercambio de prácticas, orientación y gobernanza en instrucciones o directivas adicionales de esta u otras políticas relevantes.

4. Aplicabilidad

Esta Política de privacidad e IA se aplica a todas las empresas, empleados y miembros de la Junta Directiva de empresas del Grupo Securitas, es decir, empresas en las que Securitas AB (publ.) posee directa o indirectamente una participación mayoritaria. Esta Política de privacidad e IA se comunicará e implementará, en la mayor medida posible,

en todas las asociaciones comerciales (incluidos los socios de empresas conjuntas) y las relaciones contractuales de consultoría.

5. Implementación y responsabilidad

5.1 Privacidad de datos

Es responsabilidad de la función de Cumplimiento de Ética Empresarial proporcionar un marco que las Divisiones, deben seguir para garantizar que gestionan adecuadamente los riesgos de privacidad en su negocio. unidades de negocio y los Países deben seguir para garantizar que gestionen adecuadamente los riesgos de privacidad en sus negocios. Es responsabilidad de los presidentes de División y de las unidades de negocio con sus Asesores Generales de División y, a través de ellos, cada presidente de País con los DPO, garantizar que los Política de Privacidad (así como los requisitos de las leyes locales) se implementen completamente en sus áreas o países de responsabilidad. Esto implica la responsabilidad de:

- Implementar los requisitos de privacidad de datos en los procesos (política y procedimientos), incluida la garantía de que se actualicen según sea necesario para reflejar cualquier cambio en las leyes, así como los cambios en esta Política de privacidad e IA. Cualquier desviación en una política de privacidad local de esta política de Grupo debe ser reportada al Oficial de Privacidad del Grupo. El DPO / DCO implementará un programa o política de privacidad local sobre el procesamiento de datos personales para garantizar que los documentos directivos de todo el Grupo estén operativos y que el presidente del País lo apruebe,
- Asignar los recursos que se consideren necesarios para garantizar que los requisitos de esta Política de privacidad e IA se coordinen e implementen a través de programas y / o políticas de privacidad locales. Esto incluirá la implementación de los procesos funcionales necesarios para, por ejemplo, recursos humanos, comunicaciones, legal, TI, ventas, tecnología y propietarios de funciones de compra para garantizar que los proveedores y subcontratistas cumplan con nuestras políticas.
- Asegúrese de que todas las personas relevantes estén capacitadas sobre los requisitos de esta Política de privacidad e IA y las leyes aplicables con respecto al procesamiento de datos personales, que deben revisarse periódicamente.
- Facilitar consejos de privacidad de datos para los empleados.

Es responsabilidad de todos los empleados del Grupo Securitas conocer y cumplir con esta Política de privacidad e IA, las instrucciones y directivas de apoyo, así como la política de privacidad local.

5.2 IA Responsable

Los principios de IA son obligatorios para todas las entidades de Securitas y cada entidad que desarrolle o adquiera el derecho a utilizar soluciones de IA deberá, como mínimo, demostrar que cumple con los principios o, si procede, con los requisitos legales, los compromisos de los clientes o los estándares de la industria. Sin embargo, se anima a todas las entidades de Securitas a esforzarse por alcanzar los más altos estándares de uso ético y responsable de la IA. Los principios reflejan nuestros valores fundamentales de integridad, vigilancia y servicio, así como nuestro compromiso de respetar los derechos humanos y proteger los datos personales.

Es responsabilidad de la función de Cumplimiento y Ética Empresarial desarrollar un marco basado en los principios que todas las funciones globales comunes, las Divisiones, las Unidades de Negocio y los Países deben seguir para garantizar que gestionan adecuadamente los riesgos éticos de la IA en sus negocios.

Es responsabilidad de los presidentes de país y de los directores jurídicos garantizar que la entidad local de Securitas cumpla con los requisitos locales adicionales en virtud de las leyes locales.

6. Seguimiento

El cumplimiento de esta Política por parte de todas las Compañías y Empleados de Securitas será monitoreado como parte del programa de cumplimiento de Ética Empresarial, así como por auditorías internas y externas y seguimiento rutinario de todos los asuntos reportados que requieren resolución.

7. Formación

7.1 Capacitación en privacidad de datos

Es responsabilidad de cada entidad de Securitas garantizar que se brinde la capacitación adecuada periódicamente a todos los empleados que traten datos personales. La función de ética empresarial del Grupo y el DPO/DCO local deben contribuir al desarrollo y, cuando corresponda, a la implementación de dicha capacitación.

7.2 Formación responsable de la IA

Es responsabilidad de cada entidad de Securitas garantizar que se proporcione periódicamente la formación adecuada a los empleados pertinentes que desarrollen, utilicen o sean internamente responsables de una solución de IA. La función de Ética Empresarial del Grupo y el HUB de Impacto de la IA deben contribuir al desarrollo y, en su caso, a la aplicación de dicha formación.

8. Presentación de informes

Todas las entidades y empleados de Securitas están obligados a informar cualquier sospecha de comportamiento indebido contrario a esta Política a sus gerentes inmediatos o, cuando esto no sea posible, a un gerente más senior, Gerente de Riesgo País, Defensor del Pueblo Local o Asesor Legal o representante de Ética Empresarial, según corresponda en cada jurisdicción. Ningún empleado sufrirá consecuencias negativas por cumplir con esta Política, incluso si dicho cumplimiento resulta en la pérdida de negocios, o por informar el incumplimiento.

Todos los eventos o sospechas reportados serán investigados apropiadamente de forma independiente y seguidos.

Si un denunciante no desea, o no puede, informar una sospecha a su gerente inmediato u otro funcionario de su organización, todos estos problemas deben informarse a través de la Línea de Integridad de Securitas en https://securitas.integrityline.com/, por correo

electrónico a integrity@securitas.com o al Director de Cumplimiento de Ética Empresarial de Securitas. La información de contacto actualizada se puede encontrar en el sitio web de Securitas, www.securitas.com.

Cualquier violación de esta Política o de las leyes locales aplicables dará lugar a medidas disciplinarias, hasta e incluyendo la terminación del empleo.

9. Referencia a documentos directivos y plantillas adicionales

El CEO ha publicado las siguientes directrices y plantillas relacionadas con la protección de datos y el cumplimiento de GDPR y el tratamiento ético de datos:

17.1 Instrucciones a la Política de Privacidad e IA Interna del Grupo
17.2 Directiva de Grupo sobre Inteligencia Artificial (IA) Responsable
17.3 Instrucciones de retención de grupo

17.1 Instrucciones sobre la Política de privacidad e IA del Grupo

RESUMEN

- Esta Instrucción a la Política de Privacidad e IA ("Instrucción") debe utilizarse para apoyar la puesta en práctica de la Política.
- La adhesión de todas las Entidades Cubiertas es obligatoria.
- Las entidades de Securitas que no son Entidades Cubiertas deberán cumplir con todas las partes de esta Instrucción, excepto las secciones que se aplican específicamente solo para las Entidades Cubiertas, así como con las leyes, regulaciones y mejores prácticas aplicables en relación con el procesamiento de Datos personales,
- Todas las entidades de Securitas deberán cumplir con los documentos directivos internos aplicables, incluida la gobernanza de datos, las evaluaciones de riesgos de privacidad y los principios éticos para el procesamiento de datos.

Resumen de los principales cambios desde la última revisión:

Los cambios tienen como objetivo principal aclarar los requisitos existentes. Además de algunos cambios de redacción y lenguaje.

Antecedentes y propósito

La Política de privacidad del Grupo y de IA describe los principios de alto nivel para el programa de privacidad de Securitas (el POR QUÉ). Esta Instrucción tiene como objetivo dar más contexto a los principios y constituye el QUÉ. La función de Legal, Riesgo y Ética Empresarial del Grupo emitirá pautas apropiadas para profundizar en el CÓMO. Además, cada entidad de Securitas adoptará los documentos directivos locales apropiados. Los documentos de dirección locales deberán, como mínimo, tener en cuenta las leyes aplicables y los requisitos locales y describir cómo se implementa y supervisa el programa de privacidad en la organización / país local.

Los Principios de privacidad de datos y las funciones y responsabilidades de esta Instrucción se aplican a todas las entidades de Securitas. Además de eso, se aplican requisitos más específicos para las Entidades Cubiertas. Esta Instrucción se emite bajo la Política de privacidad e IA y es adoptada por el CEO del Grupo.

En caso de cualquier inconsistencia entre las Directrices que se emiten de vez en cuando y esta Instrucción, prevalecerá la Instrucción. Lo mismo ocurre con los documentos de dirección local en comparación con los documentos emitidos por la división o el Grupo de Ética Legal, de Riesgo y Empresarial, donde prevalecen los documentos divisionales y globales. Los documentos de dirección locales solo prevalecen en la medida en que las desviaciones se deban a los requisitos legales locales y siempre que la desviación haya sido notificada a la función de Ética Empresarial del Grupo.

Definiciones clave

Controlador	Se entenderá la persona (física o) jurídica que, sola o juntamente con otros, determina los fines y medios del procesamiento de Datos Personales. En otras palabras, el Controlador es quien decide por qué se utilizan los datos, para qué fines y cómo se procesan los datos. Por ejemplo, Securitas es el Controlador cuando Securitas recopila información sobre sus clientes (nombres y dirección de correo electrónico) para enviar correos electrónicos informativos de vez en cuando a tiempo, o cuando Securitas procesa Datos Personales de sus empleados para pagar el salario.
Entidades cubiertas	Entidades de Securitas que están cubiertas por el Reglamento General de Protección de Datos (GDPR) o una legislación local que contenga requisitos similares o igualmente restrictivos.
Titular de los datos	Un sujeto de datos es una persona con la que se relacionan los datos personales (como un empleado, una persona de contacto en un cliente comercial o un cliente privado). El término Sujeto de datos e Individuo se utilizan con el mismo significado en este contexto.
Leyes de protección de datos	El Reglamento General de Protección de Datos (RGPD) (UE) 2016/679 u otras leyes y reglamentos de privacidad/protección de datos que se aplican cuando opera una entidad de Securitas.
Mapeo de Datos	Este es el proceso de identificar, comprender y catalogar todos los datos que procesa una organización (ver también "procesamiento"). Implica mapear dónde se almacenan los datos personales, cómo fluyen a través de la organización y cómo se procesan. En términos de cumplimiento de la privacidad de datos, el mapeo de datos es crucial porque ayuda a las organizaciones a comprender el alcance y la escala de sus actividades de procesamiento de datos, que es el primer paso para garantizar el cumplimiento de las leyes de protección de datos como el GDPR o la CCPA. Permite a las organizaciones identificar todos los casos de procesamiento de datos personales y garantiza que cada uno se realice de conformidad con las leyes pertinentes.
OneTrust	Significará el software de gestión de privacidad utilizado por Securitas Group para gobernar su programa de privacidad. Para la gestión del programa de privacidad, ciertas actividades de cumplimiento o gobernanza, así como el cumplimiento de los requisitos reglamentarios, el uso de OneTrust es obligatorio. La función de ética empresarial del Grupo o la función de gestión de riesgos del grupo emitirán más orientación y detalles.

Datos personales Se refiere a cualquier información relacionada con una persona identificada o identificable (es decir, un sujeto de datos). Esto podría ser información como nombre, dirección de correo electrónico, número de identificación personal, dirección IP, imágenes de fotos / videos, datos bancarios, pero también información relacionada con la identidad física, genética / biométrica, mental, económica, cultural o social del Sujeto de datos, o cualquier otra información protegida por las Leyes de Protección de Datos aplicables.

Elementos de datos personales
Se entenderá por los elementos reales de los Datos Personales tratados. Algunos ejemplos son; nombre, dirección, número de teléfono, datos de la cuenta bancaria y similares.

Privacidad por diseño

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas que plantea el tratamiento, el responsable del tratamiento, tanto en el momento de la determinación de los medios para el tratamiento como en el momento del tratamiento propiamente dicho: implementar medidas técnicas y organizativas apropiadas, como la seudonimización, que están diseñadas para implementar los principios de protección de datos, como la minimización de datos, de manera efectiva e integrar las salvaguardas necesarias en el procesamiento para cumplir con los requisitos de las Leyes de Protección de Datos y proteger los derechos legales de los Interesados.

Tratamiento

Se entenderá cualquier actividad, operación o conjunto de operaciones que se realice sobre Datos Personales o sobre conjuntos de Datos Personales, ya sea por medios automatizados o no. Esto incluye la recopilación, registro, organización, estructuración, almacenamiento, modificación, uso, divulgación, transferencia, anonimización o eliminación de Datos personales.

Procesador

significará la persona física o jurídica que procesa datos personales en nombre de, y bajo las instrucciones de, el Controlador. Si una empresa es un Controlador, los empleados de esa empresa no se consideran procesadores; El procesador es alguien fuera de la organización del controlador. Por ejemplo, si Securitas está utilizando un proveedor de servicios en la nube para almacenar sus registros de empleados, Securitas es el Controlador y el proveedor de servicios en la nube.

Subprocesador:

Un subprocesador es una entidad de terceros contratada por el procesador para ayudar a cumplir con las obligaciones del procesador con respecto al procesamiento de datos personales. Los subprocesadores se utilizan normalmente cuando el procesador principal necesita externalizar algunas de sus actividades de procesamiento de datos a otro proveedor. De acuerdo con el RGPD, los procesadores deben obtener el consentimiento previo por escrito

del controlador antes de contratar a un subprocesador. Además, el procesador debe celebrar un contrato con el subprocesador que imponga al subprocesador las mismas obligaciones de protección de datos que se imponen al procesador mediante el contrato entre el controlador y el procesador.

1. Gobierno y propiedad de los datos

Las entidades de Securitas deberán tener una estructura sólida de gobierno de datos, incluida la puesta en marcha del programa de privacidad global. Dicha estructura de gobierno de datos incluirá, como mínimo, las siguientes funciones: propietario del proceso de negocio/propietario de los datos, gestor de activos o servicios de información, propietario del contrato o del proveedor y responsable de protección de datos o responsable de cumplimiento de datos. Además, se considerará la mejor práctica en las Entidades Cubiertas designar administradores de datos / guardianes de privacidad para cumplir con las tareas obligatorias en, por ejemplo, OneTrust. La descripción de las responsabilidades y la responsabilidad dentro del área de cumplimiento de privacidad para cada rol se detallará en una guía.

Al menos las autoevaluaciones anuales u otras medidas de control serán obligatorias para ser completadas por cada país de Securitas dentro del área de privacidad. En las Entidades Cubiertas, el DPO/DCO ayudará a la empresa a responder a la evaluación/controles. Cada división impulsará la madurez continua y la mejora del cumplimiento de la privacidad con el apoyo de los expertos en privacidad de datos de la división y, cuando corresponda, la función legal, de riesgo y ética empresarial del grupo. Los controles de privacidad de datos / protección de datos serán una parte integral del marco de cumplimiento de ética empresarial y OneTrust se utilizará para completar el flujo de trabajo de controles.

1.1 Marco de privacidad local

La administración local es responsable del establecimiento y las operaciones continuas de los procedimientos y controles que garantizan la implementación del programa de privacidad global en el programa de privacidad de la entidad local. Esto incluye el cumplimiento y el seguimiento del marco relacionado con la privacidad de datos proporcionados por la función de cumplimiento de ética empresarial del grupo y cualquier control adicional incluido para satisfacer los requisitos regulatorios o de supervisión locales.

Los atributos del programa de privacidad global, la documentación de apoyo y los flujos de trabajo se pueden encontrar en: https://securitasgroup.sharepoint.com/sites/OneTrust

1.1.1 Entidades cubiertas

Es obligatorio que las Entidades Cubiertas utilicen OneTrust para todas las actividades del programa de privacidad y para el cumplimiento de las Leyes de Protección de Datos.

1.2 Documentación local

La documentación local complementará la Política de privacidad del grupo e IA, esta Instrucción y cualquier guía adicional para poner en práctica los requisitos dados a las prácticas y requisitos locales. La documentación, la implementación de los informes de controles y y las pruebas se realizarán en OneTrust.

Para las Entidades Cubiertas, esta documentación y controles deben incluir, como mínimo:

- Mapeo de datos que incluye una descripción general de los datos personales recopilados, los sistemas/activos/terceros (procesadores y subprocesadores) involucrados en el

procesamiento, incluida la identificación del propietario del activo de información y el propietario del proceso comercial para cada actividad de procesamiento,

- Mesas locales de toma de decisiones en relación con los riesgos para la privacidad de los datos identificados durante o como resultado de una evaluación de la privacidad de los datos,
- Proceso local de toma de decisiones en relación con la evaluación y, cuando sea necesario, la notificación de una violación de datos personales (en todos los países o regiones donde las violaciones de datos personales se informarán interna o externamente)

2. Procesamiento transparente

2.1 Legalidad y equidad

Una entidad de Securitas tendrá una base legal y un interés comercial legítimo, tal como se define en la ley aplicable, para procesar Datos personales. Cada función que procese Datos personales designará a un Propietario del proceso comercial para evaluar la base legal para el procesamiento y garantizar que la actividad de procesamiento esté documentada en Onetrust. Cuando la base legal se basa en el consentimiento, documente también la parte del atributo de consentimiento del registro de la actividad de procesamiento.

2.1.1 Entidades cubiertas

Cada función en una entidad cubierta documentará la base legal y el propósito (s) para procesar Datos personales en el Registro de actividades de procesamiento[1]. Cualquier procesamiento nuevo o modificado será evaluado y se debe identificar una base legal para que el procesamiento se inicie o continúe.

2.2 Registros de actividades de procesamiento

Cada entidad de Securitas mantendrá un Registro de Actividades de Procesamiento ("ROPA") o una descripción similar de su procesamiento de Datos Personales (ambos denominados ROPA en esta Instrucción). Una Plataforma Global de Privacidad de Datos, OneTrust, por ejemplo, para mantener un registro de procesamiento o ROPA es proporcionada por la función de Ética Empresarial del Grupo y cada entidad de Securitas la utilizará para cumplir con las Leyes de Protección de Datos[2] y del marco relacionado con la privacidad de datos proporcionado por la función de Cumplimiento de Ética Empresarial. El propósito de un ROPA es garantizar que las entidades de Securitas tengan una visión general de las actividades de procesamiento que se llevan a cabo y demostrar responsabilidad con los requisitos internos y externos. Cada entidad de Securitas debe poner su ROPA a disposición durante las revisiones / auditorías internas, así como para una autoridad supervisora previa solicitud.

Más detalles relacionados con el nivel de detalle requerido, así como las funciones y responsabilidades para mantener el ROPA actualizado, se describirán en las Directrices internas del Grupo emitidas por la función de ética empresarial del Grupo y se detallarán a nivel de división cuando corresponda. La responsabilidad incluye el procesamiento de datos personales, pero también a través de qué activos, proveedores, entidades legales, para qué fines y durante cuánto tiempo se procesan los datos.

Véase también la sección 2.2.

OneTrust se utilizará para cumplir con todos los requisitos de la Ley de Protección de Datos que se pueden cubrir en los módulos de la plataforma de vez en cuando.

2.3 Transparencia

Securitas proporcionará información transparente a los Interesados sobre los fines y la base legal para el procesamiento de Datos personales (aviso de privacidad o política de privacidad) en el punto de recopilación y con intervalos apropiados durante el ciclo de procesamiento. El aviso de privacidad incluirá al menos lo requerido por la ley aplicable.

2.3.1 Transparencia en las entidades cubiertas

En las Entidades Cubiertas, el propietario del proceso comercial (o propietario de los datos) será responsable de:

- Saber qué Elementos de Datos Personales se procesan dentro de un proceso o servicio bajo su responsabilidad,
- Verifique si el procesamiento de Datos personales está cubierto por un aviso de privacidad existente y, si no se puede verificar, redacte un aviso de privacidad que incluya toda la información requerida. La información se proporcionará en un lenguaje claro y fácil de entender y, en la medida de lo posible, se basará en la plantilla de aviso de privacidad.[1][2]
- Evaluar el canal apropiado para distribuir el aviso de privacidad para asegurarse de que los Sujetos de datos puedan acceder fácilmente a él,
- Definir el intervalo y las medidas para recordar a los interesados el propósito y la base legal para el procesamiento durante el ciclo de vida del procesamiento.
- El Apéndice 1 incluye más detalles en relación con los requisitos mínimos para los avisos de privacidad en las Entidades Cubiertas y se utilizará como mejor práctica para todas las entidades de Securitas.

2.4 Minimización de datos

Los Propietarios de Procesos Comerciales y los Propietarios de Datos minimizarán el procesamiento de Datos Personales asegurándose de que sea adecuado, relevante y limitado a lo que sea necesario en relación con los fines para los que se procesan, incluidos los requisitos legales de retención de registros.

Se debe considerar si menos datos personales son suficientes para cumplir con el propósito del procesamiento y si los datos seudonimizados o anónimos pueden usarse total o parcialmente.

Securitas Group no utilizará los Datos personales o los datos de los clientes de una manera que pueda percibirse como poco ética o verse como una comercialización de relaciones comerciales específicas de una manera que contradiga los compromisos contractuales.

El principio de minimización de datos se aplica desde el punto de recopilación, incluido cualquier intercambio, y durante todo el ciclo de vida de los datos. Esto significa que, si algunos datos personales en un conjunto de datos ya no son necesarios, esos datos personales se anonimizarán o eliminarán en la medida de lo posible, incluso si el resto de los datos personales aún son necesarios.

2.5 Derechos de los interesados

[1] Véase el apéndice 1.

[2] Comuníquese con DPO / DCO local o legal para obtener asesoramiento y / o apoyo.

Dependiendo de la regulación en el país o jurisdicción local donde se establezca la entidad Securitas, los Sujetos de Datos (Individuos) tendrán diferentes derechos en relación con sus Datos Personales. Sin embargo, todas las entidades de Securitas tendrán en cuenta los derechos de las personas y las expectativas razonables al tomar decisiones comerciales o administrativas. Las expectativas de los Sujetos de Datos pueden limitar el derecho de la entidad a procesar legalmente Datos Personales o requerir acciones específicas antes de que el Procesamiento sea legal.

Cada entidad de Securitas debe tomar todas las medidas razonables (por ejemplo, estableciendo e implementando procedimientos y políticas internas) para permitir el ejercicio de los derechos aplicables por parte de los Interesados de manera oportuna. Securitas informará a las personas en un lenguaje claro y sencillo de sus derechos con respecto a los Datos personales y tendrá procesos establecidos para cumplir con estos derechos. El Proceso de Negocio o el Propietario de los Datos deberá tener el conocimiento necesario de los datos Procesados para poder cumplir con las solicitudes del Interesado.

2.5.1 Entidades cubiertas

Además de lo anterior, cada entidad cubierta que procesa datos personales también podrá responder a las solicitudes del interesado. El proceso debe registrarse a través de OneTrust, pero también las solicitudes que gestionen de otras maneras deben garantizar que los interesados de datos reciban un tratamiento conforme de la solicitud que cumpla con la ley.

3. La integridad guía nuestras decisiones

3.1 Evaluaciones de riesgos de privacidad

Antes de un procesamiento nuevo o modificado de datos personales, se evaluará la privacidad de los datos, así como los riesgos éticos relacionados con dicho procesamiento. Como mínimo, el procesamiento debe cumplir con la Directiva interna del Grupo 17.2 sobre procesamiento ético de datos y la documentación debe realizarse utilizando el cuestionario modelo proporcionado por el Grupo Legal, Risk & Business Ethics. . Cuando se apliquen requisitos adicionales en virtud de la legislación local, dichos requisitos también se cumplirán.

3.1.1 Entidades cubiertas

La evaluación de los riesgos de privacidad para las Entidades Cubiertas se realizará en los siguientes pasos, además del cumplimiento de la Directiva Interna del Grupo sobre el procesamiento ético de datos como se menciona en la sección 3.1;

- La preselección de riesgos de privacidad se realizará respondiendo a una serie de preguntas iniciales para ayudar a indicar si es probable que el procesamiento resulte en un alto riesgo para los Interesados. La función de Ética Empresarial del Grupo en OneTrust proporcionará una plantilla. El DPO/DCO en cada entidad de Securitas realizará los cambios necesarios o la localización en función de las preguntas de la plantilla para ajustarse a los requisitos locales. Si la preselección indica un riesgo bajo, la evaluación inicial se documentará y archivará. Si la preselección indica un riesgo medio, la persona responsable dentro de la función o para el servicio/producto consultará con el DPO/DCO para decidir cómo proceder y, si el resultado indica un riesgo alto, se activará el siguiente paso;

- Se realizará una evaluación de impacto completa de la protección de datos ("DPIA") cuando sea probable que la actividad de procesamiento resulte en un alto riesgo para los

derechos y libertades de las personas. La evaluación del impacto ético, así como los pasos de preselección, forman parte de la EIPD y el proceso se realiza actualmente a través de OneTrust. El Propietario del Proceso de Negocio o la persona responsable del servicio/producto deberá rellenar la plantilla que luego será revisada por el DPO/DCO local. La EIPD completa se documentará como parte de la actividad de tratamiento en cuestión. Es obligatorio nombrar al menos un propietario de riesgo y un aprobador de riesgos, y acordar un plan de tiempo para la mitigación al nivel de riesgo apropiado.

Una DPIA está diseñada para identificar y documentar los riesgos con el procesamiento de datos personales. La DPIA ayudará a evaluar la necesidad y la proporcionalidad y es una forma estructurada de gestionar los riesgos de procesamiento en línea con el apetito de riesgo de Securitas.

El DPO / DCO local puede emitir más orientación.

3.2 Limitación de la finalidad

Los datos personales solo se recopilarán y procesarán para fines específicos y explícitos de acuerdo con la ley aplicable. En las jurisdicciones donde, por ejemplo, los propósitos y los elementos de datos procesados se detallarán en un aviso de privacidad para la actividad de procesamiento, proporcionado en el punto de recopilación, los Datos personales no se procesarán de una manera que sea incompatible con lo que se dijo en el aviso de privacidad (o estipulado de otra manera). Documentar los pasos de limitaciones de propósito tomados como parte de los registros aplicables de las actividades de procesamiento en OneTrust.

3.2.1 Entidades cubiertas

Si una función desea procesar datos personales para un propósito que no se incluyó en el aviso de privacidad, se realizará una evaluación entre los fines comunicados y el nuevo propósito. La evaluación debe evaluar si el nuevo propósito es compatible con el propósito (s) comunicado (s). Si el nuevo propósito no es compatible con ninguno de los fines para los que se recopilaron los Datos personales, la función responsable o el Propietario del proceso comercial deben asegurarse de que todos los Sujetos de datos relevantes den su consentimiento antes del nuevo Procesamiento, en la medida requerida por las Leyes de protección de datos aplicables.

En el apéndice 2 se incluyen los factores que deben tenerse en cuenta.

3.3 Responsabilidad

Cada entidad de Securitas será responsable y deberá poder demostrar el cumplimiento de los principios de la Política de privacidad e IA, esta Instrucción y el marco de ética empresarial para los datos personales en Securitas. Las medidas de rendición de cuentas definidas en el marco de Ética Empresarial incluyen documentación escrita y ejecución de controles que permiten a la entidad evidenciar que los procesos son efectivos.

OneTrust que incluye un proceso para, por ejemplo, mantener un ROPA será puesto a disposición por el Grupo.
Función de Ética Empresarial. Todas las entidades de Securitas deberán utilizar varios módulos de OneTrust para cumplir con los requisitos reglamentarios, los requisitos internos y garantizar la responsabilidad del Grupo Securitas.

4. Mantener sus datos seguros

4.1 Arreglos contractuales necesarios

Cuando una entidad de Securitas instruya a otra entidad interna o externa para que procese Datos personales en su nombre, el acuerdo se regulará mediante un contrato, un Acuerdo de procesamiento de datos ("DPA"). Un DPA cubrirá típicamente una serie de áreas o temas. El contenido requerido dependerá de las Leyes de Protección de Datos aplicables, pero la función Legal, Riesgo y Ética Empresarial del Grupo proporcionará una plantilla que incluya el mínimo que se incluirá para las Entidades Cubiertas. La plantilla DPA emitida por la función Legal, Risk & Business Ethics del Grupo debe utilizarse como mejor práctica para todos los Securitas, a menos que se apliquen requisitos más estrictos a nivel local.

4.1.1 Entidades cubiertas

Las Entidades Cubiertas celebrarán un DPA tanto cuando la entidad de Securitas actúe como Controlador de Datos ("Controlador") como cuando actúe como Procesador de Datos ("Procesador"). Hay ciertos requisitos obligatorios con respecto a lo que debe incluir un DPA. La función Legal, Risk & Business Ethics del Grupo ha adoptado dos plantillas diferentes para este propósito, dependiendo de si la entidad relevante de Securitas actúa como Controlador o como Procesador. Solicite a su Legal local o DPO/DCO que obtenga la versión actual de las plantillas.

Tenga en cuenta que es responsabilidad de la entidad Securitas correspondiente;

- *Evaluar* si actúa como controlador o procesador al procesar datos personales,
- Cuando actúe como Controlador, asegúrese de que sus Procesadores proporcionen *suficientes medidas técnicas y organizativas* para proteger los Datos personales.
- *Documentar los riesgos de residencia de datos en los casos en que el contrato entre Securitas y un proveedor a) está firmado por una entidad de Securitas en la UE /* EEE y dará lugar al procesamiento de datos personales sobre sujetos de datos en la UE / EEE y b) la entidad contratante del proveedor es una entidad en un llamado tercer país, por ejemplo, un país que no se considera que tiene suficiente protección de datos personales. Los riesgos deben documentarse en OneTrust completando una Evaluación de impacto de transferencia.
- *Supervisar, auditar o garantizar de otro modo* que las medidas técnicas y organizativas acordadas estén efectivamente en vigor (rendición de cuentas).
- *Clasificar la criticidad* del proveedor/Procesador, en relación con el Procesamiento de Datos Personales, de acuerdo con una matriz de riesgo definida / esquema de clasificación y utilizar la clasificación como base para la frecuencia y el alcance de los esfuerzos de auditoría / monitoreo,
- *Mantenga lo anterior actualizado y documentado en OneTrust* para garantizar la responsabilidad tanto en relación con las leyes de protección de datos como con los requisitos internos.

4.1.2 Servicios basados en la nube

Al externalizar servicios a terceros, como proveedores de servicios de TI, deben tenerse en cuenta las consideraciones de protección de datos y Securitas acordará y garantizará contractualmente los requisitos de seguridad de la información de acuerdo con las políticas internas y las mejores prácticas. La ubicación donde se alojarán los Datos personales o desde donde se puede acceder a ellos también tendrá en cuenta las Leyes de Protección de Datos y la ubicación se documentará en OneTrust.

4.2 Violación de datos personales

Las entidades de Securitas deberán contar con procesos para poder identificar y reportar incidentes de seguridad que involucren Datos Personales dentro de los plazos definidos en las Leyes de Protección de Datos o documentos directivos internos. Cada entidad de Securitas que identifique un incidente de seguridad que involucre Datos personales deberá informar ese incidente y administrar el proceso en OneTrust. Los incidentes de seguridad pueden derivarse localmente y de ServiceNow con un etiquetado o escalamiento a legal local / DPO / DCO o Oficial de privacidad divisional, dependiendo del alcance del incidente, para documentación interna y seguimiento. Un incidente que probablemente tenga impacto en más de un país deberá al menos ser notificado a la Función de Ética Empresarial del Grupo / Oficial de Privacidad del Grupo. .

4.2.1 Entidades cubiertas

Los incidentes que, de acuerdo con al menos la Ley de Protección de Datos en la UE / EEE, se informarán son *violaciones de seguridad que llevaron a la destrucción accidental o ilegal, pérdida, alteración, divulgación no autorizada o acceso a Datos personales transmitidos, almacenados o procesados de otra manera*. Esto incluirá, por ejemplo; transmisión accidental o ilegal a internos y terceros, acceso accidental o ilegal por parte de internos o terceros, pérdida de datos independientemente de si es dentro de entornos internos o externos o debido a la pérdida de hardware donde se almacenaron o se puede acceder a los Datos personales.

Si la presunta violación de datos personales incluye entidades cubiertas en más de un país, se consultará a la función de ética empresarial del grupo / Oficial de privacidad del grupo para decidir si se debe informar a la autoridad supervisora principal en Suecia o si se deben enviar varios informes para cada país, pero con contenido alineado en la medida de lo posible.

4.3 Precisión

Los datos personales se mantendrán precisos y actualizados y se garantizará que existan procesos para poder hacerlo. La frecuencia de las actualizaciones debe evaluarse en función de la naturaleza de una actividad de procesamiento y de acuerdo con las leyes de protección de datos aplicables. Los Interesados tendrán como mínimo derecho a solicitar que se corrijan los Datos personales incorrectos sin demora indebida. Se deben tomar todas las medidas razonables para garantizar que los Datos personales que sean inexactos se rectifiquen o eliminen.

4.4 Limitación de almacenamiento

Los datos personales no deben almacenarse ni procesarse durante más tiempo del necesario, teniendo en cuenta los fines para los que se procesan los datos personales, incluidos los requisitos legales de retención de registros. Los datos pueden almacenarse durante períodos más largos si son anónimos (es decir, ya no son datos personales) o, dependiendo de la naturaleza y el alcance del procesamiento, están seudonimizados de una manera que elimine o reduzca adecuadamente el impacto en la privacidad de los interesados.

Cada entidad de Securitas debe poder demostrar que los tiempos de retención están definidos y que se ejecutan en los datos relevantes.

4.4.1 Entidades cubiertas

Cada Propietario de Procesos de Negocio/Datos es responsable de garantizar que haya programas de retención para todos los Datos Personales procesados. Los programas de retención se implementarán técnicamente junto con rutinas que garanticen la eliminación oportuna de los Datos personales. Si no se puede implementar la eliminación automática o la anonimización, se debe realizar una revisión periódica para borrar los Datos personales una vez que haya cesado el propósito del procesamiento.

Los períodos de almacenamiento se definen por una combinación de requisitos legales y necesidades comerciales y se incluirán al menos en un alto nivel en un aviso de privacidad para cada actividad de procesamiento. Las Entidades Cubiertas documentarán los tiempos de retención de datos definidos en ROPA en OneTrust.

4.5 Integridad y confidencialidad

Todas las entidades de Securitas implementarán medidas técnicas y organizativas para garantizar un nivel de protección y seguridad adecuado a los riesgos relacionados con el procesamiento de datos personales. Dependiendo de la naturaleza del Procesamiento, las medidas pueden incluir:

- Anonimización o seudonimización y cifrado de Datos personales;
- Controles para garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de procesamiento;
- La capacidad de mantener y restaurar la disponibilidad y el acceso a los datos que incluyen Datos personales; iv) Un proceso para probar, evaluar y evaluar regularmente la efectividad de las medidas técnicas y organizativas.
- Consulte la Política de seguridad digital del grupo para obtener más orientación sobre las medidas de seguridad para proteger los datos y los datos personales.

5. Principios de privacidad global

5.1 Programa de privacidad

La función de Ética Empresarial del Grupo es responsable de desarrollar y monitorear un programa de privacidad que incluya la dirección estratégica del Grupo Securitas. La función de ética empresarial del Grupo también emitirá flujos de trabajo y plantillas que se utilizarán. Las plantillas y los flujos de trabajo, a menos que se indique lo contrario, serán obligatorios para las Entidades Cubiertas y las mejores prácticas para el resto del Grupo Securitas. Cada entidad de Securitas ejecutará y supervisará su cumplimiento del programa de privacidad de acuerdo con la Política de privacidad e IA, esta Instrucción y cualquier Directriz relacionada. La responsabilidad de las diferentes partes del programa de privacidad, por ejemplo, necesidades de capacitación, gestión de riesgos de terceros y similares, se documentará en cada país.

5.1.1 Delegación

La función de Ética Empresarial del Grupo tiene el mandato de emitir más directrices, evaluaciones obligatorias y flujos de trabajo según se considere apropiado para que el programa de privacidad global madure al mismo tiempo que se asegura de que la privacidad y la protección de datos sean un facilitador comercial y una ventaja competitiva.

Sin embargo, cada país informará a la función de ética empresarial del Grupo y a la persona relevante dentro de la división aplicable en caso de que sean necesarias desviaciones de los

documentos directivos emitidos debido, por ejemplo, a las leyes locales de protección de datos.

5.2 Formación

Es responsabilidad de cada Entidad Securitas garantizar que todos los empleados que tratan con Datos Personales proporcionen y completen la capacitación adecuada. El DPO/DCO debe contribuir al desarrollo y, cuando proceda, a la ejecución de dicha formación.

La capacitación básica en privacidad y protección de datos a todos los empleados de la oficina / personal indirecto será proporcionada por la Función de Ética Empresarial del Grupo. Se debe proporcionar capacitación más especializada, al menos en inglés, a grupos clave adicionales de empleados que manejan Datos personales.

El programa de capacitación específico del país, incluida una descripción general de los empleados que deben pasar por qué capacitaciones y evidencia de que se completa la capacitación, será proporcionado al menos una vez al año por el DPO / DCO o Recursos Humanos (dependiendo de quién sea responsable localmente de esta tarea) y previa solicitud al equipo de Ética Empresarial del Grupo.

5.2.1 Entidades cubiertas

Cada DPO / DCO de país es responsable de, con el aporte de las funciones relevantes, identificar los grupos de empleados que deben pasar por capacitación adicional relacionada con la privacidad y la protección de datos, incluida la frecuencia necesaria. La necesidad de traducciones se evaluará y tramitará en cada país.

Apéndice 1

Requisito de transparencia

La obligación de proporcionar información transparente a los Interesados sobre el Tratamiento de Datos Personales se detalla para las Entidades Cubiertas en esta sección y debe utilizarse como mejor práctica o para todas las demás entidades de Securitas en la medida en que sea coherente con las Leyes de Protección de Datos locales aplicables.

1. Información que debe proporcionarse cuando se recopilan datos personales del interesado

Cuando los Datos Personales sean recabados directamente del Titular se deberá proporcionar la siguiente información en el aviso de privacidad, en el momento en que se obtengan los Datos Personales:

- La identidad y los datos de contacto de la entidad Securitas, siendo el responsable del tratamiento de la actividad de tratamiento,
- Los datos de contacto del DPO o dónde se pueden realizar consultas sobre la política de privacidad de datos de la entidad Securitas,
- Los fines del procesamiento para el que se destinan los Datos personales, así como la base legal para el procesamiento,
- Cuando el procesamiento se base en un interés legítimo, información sobre dicho interés legítimo,
- Los destinatarios o categorías de destinatarios de los Datos personales, como terceros, incluidos los procesadores, si los hubiera;
- Cuando corresponda, el hecho de que Securitas tiene la intención de transferir los Datos personales a un tercer país. Las garantías utilizadas para la transferencia también se comunicarán y se pondrán a disposición de los Datos.
- Sujeto a petición,
- El período durante el cual se conservarán los Datos personales o, si eso no es posible, los criterios utilizados para determinar dicho tiempo,
- La existencia de los derechos del interesado (si los hubiera), enumerados en la sección 2.5, y la posibilidad de retirar el consentimiento cuando corresponda,
- El derecho a presentar una queja ante la autoridad supervisora;
- Si los Datos personales se procesan para la toma de decisiones automatizada, incluida la elaboración de perfiles, información significativa sobre la lógica involucrada, así como la importancia y las consecuencias esperadas de dicho procesamiento, cuando proporcionar dicha información no revele los secretos comerciales y conocimientos de Securitas o de un tercero,
- Si es una obligación legal o contractual proporcionar los Datos Personales en cuestión o si es necesario para celebrar un contrato con o para que el Interesado pueda obtener servicios de Securitas, información de que se requiere proporcionar ciertos Datos Personales y las consecuencias de no proporcionar dichos datos,
- En caso de que una función tenga la intención de procesar los Datos personales para un propósito distinto de aquel para el que se recopilaron los Datos personales, cuando lo exijan las Leyes de protección de datos aplicables, la función será responsable de garantizar que los Sujetos de datos estén informados de dicho procesamiento adicional antes de ese procesamiento adicional,
- La información se puede proporcionar verbal, física o electrónicamente, por ejemplo, a través de la llamada política de privacidad o aviso de privacidad. Securitas deberá poder demostrar que se ha facilitado dicha información,

- La función que recopila Datos personales es responsable de garantizar que existan procesos para identificar cuándo se recopilan los Datos personales y que c)-g) y j) para las actividades de procesamiento realizadas por la función se incluyan en la Política / aviso de privacidad o se proporcionen de otras maneras apropiadas al Interesado, en el momento adecuado.

2. Información que debe proporcionarse cuando los datos personales no se hayan recopilado del interesado

Cuando los Datos Personales no se recopilen directamente del Interesado, Securitas proporcionará la información enumerada en los puntos a) k) de la sección 1 de este apéndice. Además, se facilitará información sobre:

- la fuente de los Datos personales y si la fuente es de acceso público y,
- las categorías de Datos personales en cuestión.

La información se facilitará en un plazo razonable, pero a más tardar en el plazo de un mes a partir de su obtención. La función que recopila Datos personales es responsable de garantizar que existan procesos para identificar cuándo se recopilan Datos personales de otras fuentes distintas del Sujeto de datos, que dichas fuentes se incluyen en la Política / aviso de privacidad o se proporcionan de otras maneras apropiadas junto con el resto de la información requerida anteriormente para el Sujeto de datos, en el momento adecuado.

Si los Datos Personales se van a utilizar para la comunicación con el Interesado, la última hora para informar de acuerdo con lo anterior es en el momento de la primera comunicación con el Interesado. Si los Datos personales se divulgan a otro destinatario, el último momento para informar es cuando se divulgan los Datos personales por primera vez.

La información enumerada en los puntos a)-k) de este apéndice, sección 1 y a)-b) de esta sección, así como la información sobre cualquier tratamiento posterior, no es necesaria si:

- El individuo ya tiene la información;
- Proporcionar esa información sería imposible o implicaría un esfuerzo desproporcionado;
- La obtención o divulgación de los Datos personales está expresamente establecida por la legislación de la UE / EEE a la que Securitas está sujeta;
- Los Datos personales deben permanecer confidenciales sujetos a una obligación de confidencialidad u otra obligación legal de secreto; o
- Revelar al Interesado el hecho de que los Datos Personales se han obtenido a través de otra fuente interferiría o comprometería una investigación interna de la Compañía o procedimientos legales anticipados o en curso.

Apéndice 2

Procesamiento posterior y limitación de propósito

La evaluación de la compatibilidad entre la finalidad comunicada y una nueva finalidad tendrá en cuenta lo siguiente:

- Cualquier vínculo entre los propósitos originales y los nuevos propuestos;
- El contexto en el que se han recopilado los datos, incluida la relación entre el interesado y Securitas (es decir, empleado, cliente, solicitante rechazado);
- La naturaleza o categorías de Datos personales (en particular categorías especiales de datos personales o datos personales que, por su naturaleza, son más intrusivos, como fraude, datos financieros sobre calificación crediticia, grabaciones de CCTV);
- Las posibles consecuencias del procesamiento propuesto (si la nueva actividad y propósito del procesamiento tendrá efectos legales para el Sujeto de datos o requeriría una EIPD);
- La existencia de salvaguardas (incluido el cifrado o la seudonimización, que reduce los riesgos de privacidad para los interesados).

- Además de lo anterior, se evaluará cualquier limitación o desviación establecida en otras leyes de vez en cuando.

Apéndice 3

El proceso local de toma de decisiones en relación con la evaluación y, cuando sea necesario, la notificación de una violación de datos personales se realizará de conformidad con el Procedimiento LINEA DE ATENCIÓN TU AMIGO
SECURITAS -CANAL DE DENUNCIA LOCAL - CÓDIGO: RH-PR05

17.2 Directiva de Grupo sobre Inteligencia Artificial (IA) Responsable

1. Resumen

Esta Directiva sobre Inteligencia Artificial (IA) se aplica cuando Securitas combina, recopila, analiza o procesa datos, incluidos, entre otros, datos.

El Grupo Securitas tiene valores sólidos y compartimos un gran sentido de responsabilidad hacia nuestros clientes, empleados y las comunidades en las que operamos: AYUDAMOS A HACER DE SU MUNDO UN LUGAR MÁS SEGURO. Esta Directiva del Grupo sobre Inteligencia Artificial (IA) ("Directiva de IA") forma parte de la estrategia de IA de Securitas y describe nuestro compromiso con el uso responsable de la IA.

Los principios de IA del Grupo Securitas se basan en cinco principios, que se describen con más detalle en esta Directiva. Cada entidad de Securitas aplicará los principios cuando se seleccionen, desarrollen y utilicen los sistemas de IA.

2. Antecedentes y propósito

Securitas es una organización impulsada por el valor con una visión clara para utilizar nuestro conocimiento acumulado sobre las necesidades de los clientes, consumidores y empleados para ofrecer productos y servicios que son excelentes tanto hoy como mañana. Para poder transformar los datos en información, la información en conocimiento, la visión y el conocimiento en ventaja competitiva, al tiempo que se garantiza que los clientes y las personas confíen en nuestras actividades de procesamiento de datos, se requiere una clara responsabilidad y rendición de cuentas, así como un gobierno de datos maduro.

Una cultura de privacidad y uso ético de los datos proporciona una comprensión compartida de cómo los datos pueden y deben usarse para apoyar objetivos estratégicos más amplios.

3. Principios de IA Responsable

3.1 La confianza, la transparencia y la integridad son principios importantes para Securitas. Cada entidad de Securitas respetará la privacidad de los clientes, empleados y el público, y solo recopilará, utilizará y compartirá datos que sean relevantes, necesarios y legales para nuestros fines o los de nuestros clientes. Securitas será transparente sobre nuestros métodos, procesos y resultados de IA, y proporcionará información clara y precisa a nuestros grupos de interés y reguladores. Se exigirá la misma transparencia, integridad y responsabilidad a nuestros proveedores y socios.

Este compromiso se extiende a las soluciones de IA, y el desarrollo responsable y el uso ético van de la mano. Cada entidad de Securitas dará prioridad a proporcionar información clara y precisa sobre cómo funcionan estas soluciones, garantizando que la privacidad de los datos esté siempre en primer plano.

La integridad está estrechamente integrada en el proceso de desarrollo de la IA. Se debe garantizar la exactitud y la seguridad de los datos utilizados, así como mantener los más altos estándares éticos. Esto se extenderá a la identificación y mitigación de

posibles riesgos para la privacidad para ayudar a mantenerse a la vanguardia de los desafíos en el panorama de la IA.

3.2 Igualdad y Justicia

Securitas promueve la igualdad y la justicia en todas las soluciones de IA utilizadas, lo que significa que se deben tomar medidas para mitigar el sesgo, la discriminación o el daño que pueda afectar a los clientes, empleados o al público. Cada entidad de Securitas se asegurará de que nuestras soluciones de IA sean inclusivas, accesibles y respetuosas con la diversidad y la dignidad humana, y estén diseñadas para ayudar a todos los segmentos de la sociedad de manera efectiva. Al desarrollar o seleccionar una solución de IA, cada entidad tendrá en cuenta el impacto en las personas y el medio ambiente.

- Desarrollo inclusivo: reclutar y crear activamente equipos de desarrollo diversos, garantizando una variedad de perspectivas en la creación de IA.

- Evaluación de impacto: evalúe el posible impacto social y medioambiental de las soluciones de IA a lo largo de su ciclo de vida. Esto incluye evaluar los posibles sesgos, las consecuencias no deseadas y garantizar la utilización responsable de los recursos.

- Diversidad de datos: reconozca la importancia de utilizar conjuntos de datos diversos y representativos en el entrenamiento de nuestros modelos de IA. Esto ayuda a prevenir resultados discriminatorios y garantiza que los modelos sean eficaces para una gama más amplia de poblaciones.

- Implementación responsable: tenga en cuenta el contexto en el que se implementan las soluciones de IA. Asegúrese de que se utilicen de manera ética y responsable. Esto incluye evitar aplicaciones que puedan conducir a la discriminación.

3.3 Calidad de los datos

Uno de los valores fundamentales de Securitas es estar atento, lo que en el contexto de las soluciones de IA significará que tomemos medidas para mitigar el sesgo o el daño. Trabaje activamente para garantizar que los datos utilizados en los procesos clave sean de buena calidad. Esté atento a la supervisión, evaluación y mejora de la calidad y la equidad de los datos en las aplicaciones de IA, mediante la creación de una gobernanza y una propiedad de datos adecuadas.

- Gobernanza de datos: contar con marcos de gobernanza de datos sólidos que garanticen que los datos utilizados en nuestras soluciones de IA sean precisos, completos y relevantes. Esto incluye la implementación de controles de calidad de datos y procedimientos de limpieza.

- Detección de sesgos: buscamos identificar y mitigar posibles sesgos en nuestros modelos de datos e IA. Perfeccione continuamente los modelos de IA para minimizar el sesgo y garantizar resultados justos para todos los usuarios.

- Abastecimiento responsable de datos: comprométase a obtener datos de manera responsable y ética. Esto significa obtener datos con el debido consentimiento y respetando la privacidad del usuario. Priorizar la asociación con proveedores de datos de buena reputación que compartan nuestro compromiso con las prácticas éticas de datos.

• Aprendizaje y mejora: reconocer que la calidad de los datos y la mitigación de sesgos son procesos continuos. Debemos aprender y mejorar continuamente nuestras prácticas de datos y modelos de IA para garantizar que sigan siendo justos, imparciales y eficaces.

3.4 Seguridad y Protección

Cada entidad de Securitas se asegurará de que:

• Las soluciones de IA son robustas, resistentes y pueden funcionar de forma fiable y coherente.

• Garantizar la rendición de cuentas interna y externa de las soluciones de IA utilizadas.

• Exigir que las soluciones de IA cuenten con mecanismos adecuados de supervisión, control y retroalimentación.

• Implementar medidas de seguridad para proteger nuestros sistemas de IA contra el acceso no autorizado, la manipulación o el uso indebido.

A través de esto, Securitas tiene como objetivo ayudar a garantizar que la sociedad sea más segura para nuestras partes de interés.

Las consideraciones de privacidad se incorporarán en todas las etapas del proceso de desarrollo de la IA. Esto incluye anonimizar los datos siempre que sea posible, minimizar la recopilación de datos e implementar prácticas sólidas de gobernanza de datos para proteger la privacidad del usuario.

Securitas considerará cuidadosamente los riesgos potenciales y el impacto de nuestras soluciones de IA antes de implementarlas. Esto incluye llevar a cabo una evaluación de riesgos adecuada y contar con procesos claros para mitigar los daños potenciales.

Más allá de proteger nuestros propios sistemas y datos y los de nuestros clientes, Securitas cree que la IA puede ser poderosa para hacer que nuestra sociedad sea más segura. Las soluciones de IA se desarrollarán con el objetivo de ayudar en áreas como la respuesta a emergencias y la detección de fraudes, al tiempo que se mantienen prácticas éticas y responsables.

3.5 Innovación y valor de negocio

La combinación de soluciones impulsadas por IA con visión de futuro con profesionales altamente calificados continuará convirtiendo a Securitas en un líder de la industria. Securitas se esfuerza por garantizar que nuestras soluciones de IA sean tanto locales como escalables y, por lo tanto, tan adaptables como sea necesario para satisfacer las necesidades y expectativas cambiantes de los clientes, nuestra gente y el mercado. Securitas aprovechará el poder de la IA para desbloquear la innovación y el valor empresarial tangible. Securitas desarrollará capacidades de IA para abordar los riesgos potenciales de manera proactiva y ayudar a los clientes a navegar por sus necesidades de seguridad de manera efectiva.

• IA responsable: una IA fiable y responsable es esencial para crear un valor empresarial sostenible y medible.

• Inteligencia colaborativa: una cultura de colaboración entre los humanos y la IA conducirá a un fuerte valor empresarial. Esto implica capacitar a los empleados para que aprovechen las herramientas de IA de manera efectiva y asociarse con expertos en

diversos campos para garantizar que las soluciones de IA sean relevantes e impactantes.

- Creación de valor tangible: Securitas se centrará en el desarrollo de soluciones de IA que aporten un valor empresarial medible. Esto incluye una mayor eficiencia, una mejor mitigación de riesgos, mejores experiencias para los clientes y nuevas oportunidades de servicio. Evalúe el impacto de nuestras soluciones de IA en función de los datos y los comentarios.

- Al combinar la inteligencia humana y la inteligencia artificial de manera responsable, Securitas quiere desbloquear el verdadero potencial de la IA responsable para impulsar la innovación impactante y crear valor comercial tangible.

4. Aplicabilidad

La presente Directiva de IA se aplica a todas las empresas y empleados del grupo Securitas, es decir, empresas en las que Securitas AB (publ.) posee, directa o indirectamente, una participación mayoritaria. La presente Directiva se cumplirá y aplicará, en la mayor medida posible, en todas las asociaciones comerciales y relaciones con proveedores.

5. Implementación y Responsabilidad

Los principios de IA son obligatorios para todas las entidades de Securitas y cada entidad que desarrolle o adquiera el derecho a utilizar soluciones de IA deberá, como mínimo, demostrar que cumple con los principios o, si procede, con los requisitos legales, los compromisos de los clientes o los estándares de la industria. Sin embargo, se anima a todas las entidades de Securitas a esforzarse por alcanzar los más altos estándares de uso ético y responsable de la IA. Los principios reflejan nuestros valores fundamentales de integridad, vigilancia y servicio, así como nuestro compromiso de respetar los derechos humanos y proteger los datos personales.

Es responsabilidad de la función de Cumplimiento de la Ética Empresarial desarrollar un marco basado en los principios que todas las funciones globales comunes, las Divisiones, las Unidades de Negocio y los Países deben seguir para garantizar que gestionan adecuadamente los riesgos éticos de la IA en sus negocios.

Es responsabilidad de los presidentes de país y de los Directivos Jurídicos garantizar que la entidad local de Securitas cumpla con los requisitos locales adicionales en virtud de las leyes locales.

6. Formación responsable de IA

Es responsabilidad de cada entidad de Securitas garantizar que se proporcione periódicamente la formación adecuada a los empleados pertinentes que desarrollen, utilicen o sean internamente responsables de una solución de IA.

La Ética Empresarial del Grupo y el HUB IA deben contribuir al desarrollo y, cuando proceda, a la ejecución de dicha formación.

17.3 Instrucción de retención de grupo

1. Antecedentes y propósito

Esta directriz sobre la retención de Datos Personales es un complemento de la Política de Privacidad e IA. La Instrucción establece principios generales en relación con los períodos de retención, como los períodos máximos y mínimos, etc. El alcance de la aplicabilidad es el mismo que se establece en la sección 4.4 de la Instrucción a la Política de Privacidad e IA.

Es responsabilidad de cada entidad de Securitas cumplir con los principios sobre períodos de retención establecidos en esta Instrucción. Las normas sobre los períodos de retención de datos personales pueden variar de un país a otro debido a los diferentes requisitos legales. Por lo tanto, la responsabilidad de cumplimiento incluye la responsabilidad de establecer e implementar períodos de retención nacionales para cumplir con la ley aplicable y otros requisitos.

2. Principios

El procesamiento de datos personales se basa en diferentes principios establecidos en las Leyes de Protección de Datos aplicables. Securitas siempre debe tener en cuenta estos principios al procesar Datos personales.

El principio de limitación del almacenamiento implica que los Datos personales no deben conservarse durante más tiempo del necesario, teniendo en cuenta los fines para los que se procesan los Datos personales. Una vez que se han logrado los propósitos, se recomienda borrar los datos o anonimizar estos datos. Esto significa que cada controlador de datos debe establecer períodos de retención y revisar periódicamente la ejecución y el cumplimiento de dichos procesos.

Qué período de tiempo debe considerarse necesario, por lo tanto, el período de retención máximo y mínimo, difieren entre las jurisdicciones legales y la categoría de Datos personales.

3. Períodos de retención

La siguiente tabla es una referencia general a los períodos de retención máximos y mínimos según la legislación sueca y otras categorías de datos que podrían estar sujetos a períodos de retención. Por lo tanto, la siguiente tabla solo debe usarse como una guía o herramienta de inspiración para demostrar qué categorías de información podría tener que evaluar y establecer períodos de retención para cumplir con los requisitos aplicables de la ley local, etc. de vez en cuando.

Como regla general, los Datos personales deben eliminarse o anonimizarse rutinariamente al final de cada período de retención. Tenga en cuenta que esta regla podría estar sujeta a excepciones debido a la existencia de un interés legítimo u obligación legal de procesar o retener Datos personales.

Esta instrucción se aplica tanto a los archivos electrónicos como a los registros en papel.

Para cualquier pregunta sobre períodos de retención, eliminación de datos, etc., consulte con su DPO / DCO local o legal.

En general, hay dos enfoques principales al documentar los tiempos de retención de Datos personales en Securitas e independientemente de cuál de esas dos opciones se seleccione, debe complementarse con tiempos de retención en OneTrust conectados a cada actividad de procesamiento y servicio interno según lo requerido por las pautas de Group Legal, Risk & Business Ethics.

Los tiempos de retención podrían:

a) definirse por sistema/activo identificando los principales fundamentos legales y propósitos comerciales para cada categoría de datos y, en función de eso, los tiempos de retención deben establecerse en una política de retención local, matriz/tabla.

b) Los tiempos de retención podrían definirse en función de los fines del procesamiento de los datos personales, independientemente del sistema / activo donde se procesen los datos. Esta opción es más granular y requiere más tiempo, pero si se ejecuta correctamente también es la más compatible.

La siguiente tabla debería servir de inspiración para decidir sobre una matriz de retención específica de un país o entidad jurídica. Los tiempos de retención definidos son referencias a la ley sueca y serán diferentes en cada país. Como parte de un proyecto o la introducción de un nuevo sistema/aplicación/activo de información, será necesario decidir e implementar una matriz de retención aún más granular.

Categoría de datos	**Período de retención e inicio del período de retención**	**Disposición legal pertinente u otra base legal**
[Contabilidad]		
Obligación general de retención de cuentas, libros de cuentas y registros de la empresa	Mínimo 10 años A partir de la fecha del último asiento, documento o comprobante, pudiendo utilizar para el efecto, a elección del comerciante, su conservación en papel o en cualquier medio técnico, magnético o electrónico que garantice su reproducción exacta.	Código de Comercio art. 28
Facturas	Mínimo/máximo: 5 años contados a partir del 1o. de enero del año siguiente al de	Estatuto Tributario art. 632

	su elaboración, expedición o recibo, los siguientes documentos, informaciones y pruebas, que deberán ponerse a disposición de la Administración de Impuestos, cuando ésta así lo requiera	
Informes de gastos de empleados	himo/máximo: 5 años contados a partir del 1o. de enero del año siguiente al de su elaboración, expedición o recibo, los siguientes documentos, informaciones y pruebas, que deberán ponerse a disposición de la Administración de Impuestos, cuando ésta así lo requiera	Estatuto Tributario art. 632
Recibos de efectivo	himo/máximo: 5 años contados a partir del 1o. de enero del año siguiente al de su elaboración, expedición o recibo, los siguientes documentos, informaciones y pruebas, que deberán ponerse a disposición de la Administración de Impuestos, cuando ésta así lo requiera	Estatuto Tributario art. 632

Registros de gastos empresariales	nimo/máximo: 5 años contados a partir del 1o. de enero del año siguiente al de su elaboración, expedición o recibo, los siguientes documentos, informaciones y pruebas, que deberán ponerse a disposición de la Administración de Impuestos, cuando ésta así lo requiera	Estatuto Tributario art. 632
[Lucha contra el blanqueo de capitales]		
Documentos e información relativos a las medidas adoptadas para llevar a cabo la diligencia debida con respecto al cliente con fines de lucha contra el blanqueo de capitales	Mínimo 5 años. No se establece ningún período máximo El plazo se calcula a partir de la adopción de dichas medidas o, en los casos en que se haya establecido una relación comercial, de la terminación de la relación comercial.	Código general del proceso
Registros de personas físicas o jurídicas para evitar la participación en transacciones que constituyan blanqueo de capitales o financiación del terrorismo	Mínimo: 5 años periodo de prescripción de los acuerdos contractuales	Código general del proceso

Documentación relativa a todas las circunstancias que puedan indicar blanqueo de capitales o financiación del terrorismo y cualquier acción y decisión adoptada en el examen de sospechas de blanqueo de capitales o operaciones de financiación del terrorismo	Mínimo 5 años. Periodo de prescripción de los acuerdos contractuales	Código General del proceso

[Derecho corporativo y registros corporativos]		
Registro de accionistas	Durante toda la vida útil de la empresa y 5 años adicionales después de su disolución. Si el registro de accionistas se mantiene por medios automatizados, los datos eliminados se conservarán para un periodo de 5 años adicionales después de su eliminación	Ley 222 de 1995
Políticas de la Junta, resoluciones, actas de reuniones y actas de reuniones del comité	Durante toda la vida útil de la empresa y 5 años adicionales después de su disolución. Si el registro de accionistas se mantiene por medios automatizados, los datos eliminados se conservarán 5 años adicionales después de su eliminación	Ley 222 de 1995
Contratos	Mínimo/máximo: 5 años	Código General del Proceso

Correos electrónicos (relacionados con el negocio)	Mínimo/máximo: 5 años	Ley 222 de 1995
[RRHH y registros de empleo]		
Contrato de trabajo	Mínimo 3 años El período de retención comienza cuando finaliza el empleo	Código Sustantivo del trabajo
Documentos de RRHH y empleo También es probable que esté sujeto a un período máximo de retención basado en las normas de protección de datos: Datos de solicitantes de empleo rechazados	Máximo: 5 años. Los datos personales de los candidatos rechazados deben eliminarse tan pronto como haya concluido el proceso de contratación. El período de retención comienza cuando se notifica al solicitante	Código Penal Colombiano
(*por ejemplo*, cartas de solicitud, CV, referencias, cartas de reconocimiento, certificados de buena conducta, notas de entrevistas de trabajo, evaluación y resultados de pruebas psicológicas)		

Datos relativos a un trabajador temporal	3 años El período de retención comienza cuando finaliza el empleo	Código Sustantivo del trabajo
Informes sobre reuniones de revisión del desempeño de los empleados y entrevistas de evaluación (base de datos de competencias)	3 años	Código Sustantivo del trabajo

Copia de documentos de identificación	Mínimo 5 años de acuerdo con el periodo de prescripción de acciones contractuales	Código General del Proceso
Registro de períodos de trabajo y descanso (en el formato adecuado)	Mínimo 3 años. No hay un período máximo de retención específico, se aplican reglas generales	Código Sustantivo del trabajo
Uso de Internet y correo electrónico por parte de los empleados	máximo 3 años	Código Sustantivo del trabajo
Hoja de vida de empleados (y otra documentación relacionada con la contratación, promoción, degradación, transferencia, terminación o selección para capacitación)	Mínimo: 5 años	Código Sustantivo del trabajo
Registros relacionados con la verificación de antecedentes de los empleados	Mínimo: 3 años	Código Sustantivo del trabajo
Incidente de lesión y enfermedad Informes y resúmenes anuales relacionados; Registros de lesiones y enfermedades relacionadas con el trabajo	Mínimo: 20 años	Decreto 1143 de 2014
Exámenes médicos requeridos por la ley	Mínimo: 20 años	Decreto 1143 de 2014
Pruebas previas al empleado y resultados de las pruebas	Mínimo: 3 años	Código Sustantivo del trabajo

Informes de tiempo	Mínimo: 3 años	Código Sustantivo del trabajo
[Registros legales y de seguros]		
Contratos	Mínimo: 5 años	Código General del Proceso
Reclamaciones/solicitudes de seguros	Mínimo: 10 años	Código General del Proceso
Contratos y pólizas de seguro (Director y Oficiales, General Responsabilidad, Propiedad, Trabajadores Compensación)	Mínimo: 5 años	Código General del Proceso
Arrendamientos	Mínimo: 5 años	Código General del Proceso
Garantías	Mínimo: 5 años	Código General del Proceso
Solicitud y registro de derechos de propiedad intelectual	Mínimo: 5 años a partir de la caducidad del registro de la marca patente o secreto comercial	Decisión 486 de la Comunidad Andina
Documentación de reclamaciones legales	Mínimo: 10 años	Código General del Proceso
[Registros de nómina y salarios]		

El agente de retención (generalmente el empleador) debe mantener una administración de salarios, incluida la exención de impuestos. Reembolsos. Además, el empleador debe informar anualmente a la Agencia Tributaria sueca y al empleado/beneficiario del importe total de los salarios devengados, incluidos el salario, las prestaciones y la pensión, así como	Mínimo 3 años El período de retención comienza en el año siguiente a la expiración del año natural en el que se cerró el año contable (al que se refiere la información)	Código Sustantivo del Trabajo

Soportes de capacitaciones, cursos mandatorios, entrenamientos y reentrenamientos	Mínimo: 5 años	Código General del Proceso
Una empresa debe incluir información sobre los empleados en su administración, incluido el nombre, la fecha de nacimiento, el número de registro fiscal y la dirección. Además, las solicitudes de los empleados para aplicar un descuento de retención de impuestos salariales deben conservarse en la administración de la empresa.	Mínimo 3 años El período de retención comienza en el año siguiente a la expiración del año natural en el que se cerró el año contable (al que se refiere la información)	Código Sustantivo del Trabajo

Los documentos de nómina, salario y asuntos pensionales también pueden estar sujetos a un período máximo de retención basado en las normas de protección de datos: registros de nómina (salarios, impuestos y seguridad social, nóminas, compensación por horas extraordinarias, bonificaciones, gastos, beneficios en especie), registros de indemnización por despido (por *ejemplo*, notificación a las autoridades competentes sobre despido, decisiones del tribunal sobre despido, correspondencia con las autoridades competentes sobre despido, registros de recolocación, cálculos de pagos por terminación)	Mínimo: 80 años	Código Sustantivo del Trabajo Jurisprudencia CE
[Registros de compras o ventas]		
Una organización está obligada a registrar todas las entregas de bienes o servicios, todas las adquisiciones, todas las importaciones y exportaciones, y toda otra información relevante para fines del IVA.	Mínimo/máximo: 5 años contados a partir del 1o. de enero del año siguiente al de su elaboración, expedición o recibo, los siguientes documentos, informaciones y pruebas, que deberán ponerse a disposición de la Administración de Impuestos, cuando ésta así lo requiera	Estatuto Tributario art. 632

Libro mayor, departamento de cuentas por cobrar, departamento de cuentas por pagar,	Mínimo 10 años A partir de la fecha del último asiento, documento o	Código de Comercio art. 28
administración de adquisiciones y ventas, registros de inventario	comprobante, pudiendo utilizar para el efecto, a elección del comerciante, su conservación en papel o en cualquier medio técnico, magnético o electrónico que garantice su reproducción exacta.	

Registros de Compras	Mínimo/máximo: 5 años contados a partir del 1o. de enero del año siguiente al de su elaboración, expedición o recibo, los siguientes documentos, informaciones y pruebas, que deberán ponerse a disposición de la Administración de Impuestos, cuando ésta así lo requiera	Estatuto Tributario art. 632
Es probable que los registros de deudores y acreedores estén sujetos a un período máximo de retención basado en normas de protección de datos	Mínimo 10 años A partir de la fecha del último asiento, documento o comprobante, pudiendo utilizar para el efecto, a elección del comerciante, su conservación en papel o en cualquier medio técnico, magnético o electrónico que garantice su reproducción exacta.	Código de Comercio art. 28

Es probable que los registros de los clientes estén sujetos a un período máximo de retención basado en las reglas de protección de datos	Mínimo 10 años A partir de la fecha del último asiento, documento o comprobante, pudiendo utilizar para el efecto, a elección del comerciante, su conservación en papel o en cualquier medio técnico, magnético o	Código de Comercio art. 28

	electrónico que garantice su reproducción exacta.	
Informes de crédito	Mínimo 10 años A partir de la fecha del último asiento, documento o comprobante, pudiendo utilizar para el efecto, a elección del comerciante, su conservación en papel o en cualquier medio técnico, magnético o electrónico que garantice su reproducción exacta.	Código de Comercio art. 28
[Vigilancia]		
Datos de inicio y cierre de sesión de los visitantes	Mínimo: 10 años	Código General del proceso

Grabaciones de cámara	Hasta que cese la finalidad para la cual se están haciendo grabaciones y máximo hasta 10 años de acuerdo con el tiempo de prescripción de las acciones extracontractuales	Ley 1582 de 2012 y Código General del Proceso
[Impuestos]		
Obligación general de los contribuyentes de proporcionar (a petición del inspector fiscal) toda	Registros y libros: Mínimo 10 años	Código de Comercio art. 28
la información que pueda ser relevante para su posición fiscal, incluidos todos los libros, registros y otros soportes de datos.	Soportes mínimo 5 años	Estatuto tributario art. 632