PROTECCIÓN DE DATOS

Política corporativa

astara

CONTROL DE CAMBIOS

Edición	**versión 1.0**
Fecha de aprobación	
Cambiar acciones	
Cambiar descripción	
Clasificación	

ÍNDICE

1. OBJETO
2. DEFINICIONES
3. PRINCIPIOS
4. FUNCIONES Y OBLIGACIONES
5. REGISTROS DE LAS ACTIVIDADES DE TRATAMIENTO
6. RECLAMACIÓN Y NOTIFICACIÓN AL COMITÉ DE PRIVACIDAD
7. TRATAMIENTO DE DATOS PERSONALES
8. EJERCICIO DE DERECHOS
9. FORMACIÓN
10. SECRETO DE DATOS
11. AUDITORÍAS
12. INVESTIGACIONES INTERNAS
13. SEGURIDAD DE LOS DATOS
14. GESTIÓN DE DATOS
15. EVALUACIÓN DEL IMPACTO DE LA PROTECCIÓN DE DATOS
16. VIOLACIONES DE LOS DATOS DE PROTECCIÓN
17. DISPOSICIONES FINALES
18. REFERENCIAS

1. OBJETO

Esta Política de Protección de Datos es la base vinculante para la protección legal y sostenible de los datos personales en Astara, en relación con el cumplimiento de la normativa sobre protección de datos personales.

Esta política regula el tratamiento de la información conforme a la protección de datos y las responsabilidades al respecto en Astara. Todos los empleados están obligados a cumplir con la política.

Esta política debe estar disponible para todo el personal de Astara.

Esta política y la versión actual se aplican personalmente a todo el personal de Astara.

Los requisitos y prohibiciones de esta política se aplican a todo el tratamiento de datos personales, independientemente de si se realiza de forma electrónica o en papel. También se aplican a todo tipo de interesados (clientes, empleados, proveedores, etc.).

2. DEFINICIONES

Se aplicarán las siguientes definiciones:

- **Astara, Grupo, o Grupo Astara**: incluye Astara Mobility, S.A., y todas sus filiales y sucursales.

- **Filial**: significa cualquier entidad que directa o indirectamente a través de uno o más intermediarios, controla o está controlada por o está bajo control común con la entidad especificada. A los efectos de esta definición, el control de una entidad significa el poder, directo o indirecto, de dirigir o causar la dirección de la administración y las políticas de dicha entidad, ya sea por contrato o de otra manera, y la propiedad de la mayoría de los derechos de voto de otra entidad creará una presunción refutable de que dicha entidad controla esa otra entidad.

- **Personal de Astara**: significa todos los directores y ejecutivos, empleados, consultores que trabajan dentro de Astara y trabajadores que prestan servicio en cualquier negocio de Astara en cualquier parte del mundo.

- **La información y los datos** deben entenderse de forma exhaustiva. Esto incluye, independientemente del contenido, todo lo que se ha grabado en palabra, escritura, imagen, sonido o en forma electrónica en cualquier soporte de datos (papel, disco duro, memoria USB, CD-ROM, etc.).

- **Los datos protegidos** son toda la información y los datos que se recopilan, procesan y gestionan con fines comerciales.

- **Los datos personales** son cualquier información relativa a una persona física identificada o identificable ('interesado'); una persona física identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de esa persona física.

- **Los datos personales que requieren protección especial** son la información y los datos relativos a:

    - *religiosos* (por ejemplo, confesión, pagos a una comunidad religiosa), *ideológicos, políticos* (por ejemplo, afiliación a un partido) o *opiniones o actividades sindicales (por ejemplo, detalles de la asistencia a un acto sindical)*

    - *Salud* (por ejemplo, expediente médico, receta de medicamentos), *privacidad* (por ejemplo, orientación sexual, información sobre temores y otros sentimientos, sueños, terapias, medicamentos; pero no ingresos y activos) o *raciales (*características físicas como el color) o *étnicas* (por ejemplo, basado en una historia compartida o en un sistema de actitudes y comportamientos);

    - *datos genéticos* (análisis dann);

    - *datos biométricos que* identifican de forma única a una persona física (p. ej., huella dactilar, patrón de iris, imagen facial, pero no el tamaño corporal, color de ojos o cabello);

    - *procedimientos* o sanciones administrativas y penales (por ejemplo, procedimientos disciplinarios, retirada del permiso de conducción, medidas penales),

    - *Medidas de asistencia social (por ejemplo, prestaciones de la seguridad social en relación con enfermedades y accidentes, así como medidas de asistencia y bienestar)*

- **Por tratamiento** se entiende cualquier operación o conjunto de operaciones que se realicen sobre datos personales o sobre conjuntos de datos personales, ya sea por medios automatizados o no, como la recogida, registro, organización, estructuración, almacenamiento, adaptación o

alteración, recuperación, consulta, utilización, divulgación por transmisión, difusión o puesta a disposición, alineación o combinación, restricción, supresión o destrucción.

- **Responsable** del tratamiento: la persona física o jurídica, autoridad pública, organismo u otro organismo que, individual o conjuntamente con otros, determina los fines y medios del tratamiento de datos personales; cuando los fines y medios de dicho tratamiento estén determinados por el Derecho de la Unión o de los Estados miembros, el responsable del tratamiento o los criterios específicos para su designación podrán estar previstos por el Derecho de la Unión o de los Estados miembros;

- **Encargado** significa una persona física o jurídica, autoridad pública, agencia u otro organismo que procesa datos personales en nombre del controlador.

3. PRINCIPLES

Los datos personales serán:

(a) tratamiento legal, justo y transparente en relación con el interesado ('legalidad, equidad y transparencia').

(b) recogidos con fines específicos, explícitos y legítimos y no tratados de forma incompatible con dichos fines; tratamiento posterior con fines de archivo en interés público, no se considerarán incompatibles con los fines iniciales (limitación de la finalidad);

(c) adecuada, pertinente y limitada a lo necesario en relación con los fines para los que se tratan ('minimización de datos').

(d) precisa y, en su caso, actualizada; deberán tomarse todas las medidas razonables para garantizar que los datos personales inexactos, teniendo en cuenta los fines para los que se tratan, se borren o rectifiquen sin demora (exactitud).

(e) conservarse en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que se tratan los datos personales (limitación del almacenamiento).

(f) tratados de manera que se garantice la seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daños accidentales, utilizando medidas técnicas u organizativas adecuadas (integridad y confidencialidad).

En consecuencia, el hardware y el software utilizados para el procesamiento de datos se utilizarán para tareas operativas, es decir, para los fines previstos respectivos, y estarán protegidos contra pérdidas y manipulaciones. El uso para fines privados requiere permiso expreso.

Cada empleado es responsable de la implementación de la política en su área de responsabilidad. El cumplimiento debe ser supervisado regularmente por él o ella.

Las personas responsables del tratamiento de los sistemas utilizados se asegurarán de que sus empleados (usuarios) estén informados sobre esta política; esto también se aplica a los empleados temporales y empleados externos.

4. FUNCIONES Y DEBERES

4.1 Responsable

La responsabilidad general de la protección de datos en la empresa es asumida por la dirección de la empresa.

4.2 Comité de Privacidad Corporativa

Astara ha designado voluntariamente un Comité de Privacidad Corporativa al que puede contactar a través del siguiente correo electrónico privacy.es@astara.com

El Comité de Privacidad Corporativa desempeñará sus funciones sin instrucciones y utilizando su experiencia.

El Comité de Privacidad tiene las siguientes tareas/deberes en particular:

- **Contacto:** El Comité de Privacidad Corporativa es el contacto para los interesados, los empleados, la gestión de la empresa y las autoridades responsables de la protección de datos en astara. No obstante lo anterior, existe un punto de contacto para cuestiones de privacidad por país, (en adelante el **Punto de Contacto de Privacidad) de la siguiente manera: TBC (País/ dirección de correo electrónico).**)

- **Formación**: El Comité de Privacidad Corporativa apoya a la empresa en la formación de empleados en el área de protección de datos.

- **Asesoramiento**: El Comité de Privacidad Corporativa asesora e informa a la dirección de la empresa sobre las obligaciones de protección de datos existentes. El Comité de Privacidad asesora a los empleados y ejecutivos sobre cuestiones relacionadas con la protección de datos.

- **Supervisión**: El Comité de Privacidad Corporativa supervisará el cumplimiento de las Regulaciones de Protección de Datos, incluidos los requisitos de ésta y otras políticas de la Compañía sobre protección de datos.

- **Control**: El Comité de Privacidad Corporativa controla los procesos seleccionados de forma aleatoria, orientada al riesgo y a intervalos adecuados con respecto a su conformidad con la protección de datos.

- **Informes**: El Comité de Privacidad Corporativa informa anualmente en un informe de actividad a la gerencia sobre las auditorías que han tenido lugar, las quejas y cualquier deficiencia organizativa que aún debe remediarse.

La dirección proporcionará al Comité de Privacidad Corporativa los recursos necesarios y se le concederá acceso a toda la información, documentos, listas de actividades de procesamiento y datos personales que el Comité de Privacidad Corporativa requiera para realizar sus funciones.

La empresa o sus empleados deberán involucrar al Comité de Privacidad Corporativa en todas las cuestiones de protección de datos en una etapa temprana y apoyarlo en el desempeño de sus funciones.

5. REGISTROS DE LAS ACTIVIDADES DE TRATAMIENTO

La empresa mantiene un registro de todas las actividades de procesamiento. El Comité de Privacidad Corporativa tiene la responsabilidad de recopilar la información necesaria para este propósito sobre las actividades de procesamiento del departamento respectivo (por ejemplo, people, marketing) y documentarlas de acuerdo con los requisitos legales.

Previa solicitud, la empresa pondrá el directorio a disposición de la autoridad de supervisión. De acuerdo con la dirección de la compañía, el Comité de Privacidad Corporativa será responsable de esto y cooperará con la autoridad supervisora.

6. RECLAMACIÓN Y NOTIFICACIÓN AL COMITÉ DE PRIVACIDAD

Todo interesado tiene derecho a presentar una reclamación ante el Comité de Privacidad Corporativa sobre el procesamiento de sus datos si considera que se han violado sus derechos.

Del mismo modo, los empleados pueden ponerse en contacto directamente con el Comité de Privacidad Corporativa con información, sugerencias o violaciones de esta política, por lo que se mantendrá la confidencialidad absoluta a petición ("denuncia de irregularidades").

7. TRATAMIENTO DE DATOS PERSONALES

7.1 Recopilación y tratamiento de datos personales

La recopilación y el tratamiento de datos personales sólo pueden tener lugar en el ámbito de lo legalmente permitido. En este contexto, los requisitos específicos para la recopilación y el tratamiento de datos personales especialmente sensibles y la elaboración de perfiles de alto riesgo también deben cumplirse de conformidad con los requisitos legales. En principio, sólo podrá tratarse y utilizarse la información necesaria para el cumplimiento operativo de las tareas y directamente relacionada con la finalidad del tratamiento ("limitación de la finalidad").

El interesado debe ser informado adecuadamente sobre la utilización de su/ sus datos personales cuando se recopila su/ sus datos personales ("deber de informar"). La información debe incluir la finalidad, la identidad del responsable del tratamiento, los destinatarios de los datos personales y cualquier otra información de conformidad con las disposiciones de la ley de protección de datos, para que el interesado pueda hacer valer sus derechos y se garantice un tratamiento de los datos transparente.

Si los datos personales no se recogen del interesado, sino que se obtienen de otra empresa, por ejemplo, el interesado debe ser informado posteriormente y de forma exhaustiva sobre el tratamiento de sus datos de conformidad con las disposiciones de la ley de protección de datos. Esto también se aplica a los cambios en la finalidad del procesamiento de datos.

Los datos personales deben ser objetivamente correctos y, si es necesario, actualizados ("exactitud"). El alcance del tratamiento de datos debe ser necesario y pertinente con respecto a la finalidad definida ("exhaustividad"). El departamento respectivo debe asegurar la implementación mediante el establecimiento de procesos apropiados. Del mismo modo, los archivos de datos deben ser revisados regularmente para verificar su exactitud, necesidad y actualidad.

Antes de introducir nuevos tipos de recogid de datos, el responsable del tratamiento debe documentar por escrito la finalidad de los datos que determinan la validez. En principio, sólo se permite un cambio de finalidad si el tratamiento es compatible con los fines para los que se recopilaron originalmente los datos. Los criterios de ponderación utilizados en el contexto del cambio de finalidad deben examinarse individualmente. El exámen deberá documentarse para obtener pruebas adecuadas.

También se permite un cambio de finalidad si se ha informado previamente a los interesados.

7.2 Transferencias Internacionales

La transferencia de datos personales de ciudadanos europeos a terceros fuera de la Unión Europea, el Espacio Económico Europeo o el país aplicable requiere medidas especiales para proteger los derechos e intereses de los interesados. Los datos no deben transferirse si el organismo receptor no dispone de un nivel adecuado de protección de datos o si esto no puede lograrse, por ejemplo, mediante cláusulas contractuales específicas.

7.3 Proveedores de servicios externos (encargados de tratamiento)

Los proveedores de servicios externos con acceso potencial a datos personales deben ser cuidadosamente seleccionados antes de adjudicar el contrato. La selección debe documentarse y, en particular, debe tener en cuenta los siguientes aspectos:

- Idoneidad profesional del proveedor para el tratamiento específico de datos
- Medidas de seguridad técnico-organizativas
- Experiencia del proveedor en el mercado
- Otros aspectos que indican la fiabilidad del proveedor (documentación de protección de datos, disposición a cooperar, tiempos de respuesta, etc.)

Si un proveedor de servicios va a recopilar, procesar o utilizar datos personales en nombre de un cliente, se debe firmar un contrato de encargado de taratmiento. La protección de datos y los aspectos de seguridad informática deben estar regulados en este contrato.

El proveedor de servicios tendrá un seguimiento periódico en relación con las medidas técnicas y organizativas acordadas contractualmente con él. El resultado deberá documentarse.

7.4 Minimización de datos, privacidad por diseño/privacidad por defecto

El tratamiento de los datos personales se orientará al objetivo de recopilar, tratar o utilizar la menor cantidad posible de datos de un interesado ("minimización de datos"). En particular, los datos personales deben ser anonimizados o seudónimos en la medida de lo posible en función de la finalidad de uso. Por ejemplo, en el contexto de una evaluación estadística de los datos, no será necesario conocer y utilizar el nombre completo del interesado. Más bien, esta información puede ser reemplazada por un valor aleatorio, que también puede asegurar que la información subyacente es distinguible.

Lo mismo se aplica a la selección y diseño de sistemas de procesamiento de datos. La protección de datos se integrará desde el principio en las especificaciones y la arquitectura de los sistemas de tratamiento de datos para facilitar el cumplimiento de los principios de privacidad y protección de datos, en particular el principio de minimización de los datos.

8. DERECHOS DEL INTERESADO

El interesado será informado en un plazo de 30 días, a más tardar, de cualquier medida adoptada a petición suya/suya.

Astara como responsable del tratamiento, facilitará el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición de los interesados, estableciendo los procedimientos internos necesarios para cumplir con los requisitos legales aplicables. A este respecto, permitirá presentar las solicitudes de forma sencilla, por medios electrónicos, especialmente cuando el tratamiento se realice por estos medios.

9. FORMACIÓN

Los empleados que tengan acceso permanente o regular a los datos personales, recopilen dichos datos o desarrollen sistemas para el tratamiento de dichos datos deberán recibir formación adecuada sobre los requisitos de la normativa de protección de datos aplicable.

El Comité de Privacidad decidirá sobre la forma y frecuencia de la capacitación pertinente.

10. SECRETO DE DATOS

El personal de Astara tiene prohibido recopilar, procesar o utilizar datos personales sin autorización. Todos los empleados deben observar estrictamente los principios de la legislación de protección de datos, a saber, las directivas y directrices internas sobre la protección de la información y los datos.

11. AUDITORÍAS

Con el fin de garantizar un alto nivel de protección de datos, los procesos pertinentes se revisan mediante auditorías periódicas realizadas por organismos internos o por

auditores externos. En caso de que se detecten posibilidades de mejora, se adoptarán medidas correctivas inmediatas.

Los resultados obtenidos durante la auditoría deberán documentarse. La documentación será entregada al Comité de Privacidad Corporativa, a la dirección de la empresa y a las personas responsables del proceso respectivo.

Una auditoría se realiza con éxito cuando se han aplicado todas las medidas documentadas en el informe. En caso necesario, las auditorías de seguimiento se llevan a cabo examinando la aplicación de las recomendaciones de la auditoría inicial.

12. INVESTIGACIONES INTERNAS

Las medidas destinadas a esclarecer los hechos y a evitar o descubrir infracciones penales o infracciones graves del deber en la relación laboral deben llevarse a cabo respetando estrictamente las disposiciones legales pertinentes en materia de protección de datos. En particular, la recogida y el uso de datos asociados deben ser necesarios para lograr el objetivo de la investigación, adecuados y proporcionados en relación con los intereses del interesado que sean dignos de protección.

Se informará lo antes posible al interesado de las medidas que se le hayan adoptado.

13. SEGURIDAD DE LOS DATOS

Con el fin de salvaguardar la confidencialidad, disponibilidad, integridad y trazabilidad de los datos, se establece un concepto general de seguridad que es vinculante para todos los procedimientos. En particular, se debe tener en cuenta el estado de la técnica, así como los medios y medidas para el cifrado y la protección de datos. El concepto de seguridad debe revisarse, evaluarse y evaluarse periódicamente con respecto a la eficacia de las medidas técnicas y organizativas previstas en él.

14. GESTIÓN DE DATOS

Los datos siempre se almacenan en las unidades de red proporcionadas para este propósito. El almacenamiento en soportes de datos móviles o almacenamiento en la nube requiere la aprobación del departamento de TI y el registro por parte del departamento/usuario que utiliza el operador. En el caso de las redes, el departamento de TI es responsable de realizar copias de seguridad de los datos almacenados en el servidor.

Si se requiere una ubicación de almacenamiento diferente por razones técnicas (por ejemplo, portátil, PC de escritorio), el usuario respectivo es responsable de realizar la

copia de seguridad de datos. Si es posible acceder a la red (p. ej., portátil con WLAN, tableta), los datos actuales deben transferirse a la unidad de red reservada para el usuario al menos una vez por semana.

Deben respetarse los plazos legales de conservación y supresión. Se informará al departamento de TI del cumplimiento de los plazos, especialmente en lo que respecta a la eliminación de datos personales en copias de seguridad.

Cuando se transmiten o devuelven componentes de TI que ya no son necesarios, el usuario está obligado a asegurarse de que todos los datos se han eliminado efectivamente de antemano.

15. EVALUACIÓN DE IMPACTO DE LA PROTECCIÓN DE DATOS

El Punto de Contacto de Privacidad está obligado a llevar a cabo evaluaciones de impacto de protección de datos para los procedimientos que tienen lugar bajo su responsabilidad si una operación de procesamiento puede conllevar un alto riesgo para los derechos personales o los derechos fundamentales del interesado. La evaluación de impacto de la protección de datos contiene todas las descripciones requeridas por la ley.

Se requerirá, en particular, una evaluación del impacto sobre la protección de datos en el caso de:

(a) una evaluación sistemática y exhaustiva de los aspectos personales relativos a las personas físicas basada en un tratamiento automatizado, incluida la elaboración de perfiles, y en qué decisiones se basan para producir efectos jurídicos que afecten a la persona física o que afecten de forma significativa a la persona física;
(b) tratamiento a gran escala de categorías especiales de datos o de datos personales relativos a condenas y delitos penales, o
(c) una vigilancia sistemática a gran escala de una zona de acceso público.

16. VIOLACIONES DE PROTECCIÓN DE DATOS ("DATA BREACH")

Todos los empleados están obligados a informar inmediatamente de los fallos, incidentes de seguridad y emergencias en el área de seguridad de la información e incidentes en el área de protección de datos al Punto de Contacto de Privacidad y al CISO ciso@astara.com

La notificación incluirá toda la información pertinente para aclarar los hechos, en particular el organismo receptor, los interesados y el tipo y alcance de los datos transmitidos.

El cumplimiento de cualquier obligación de informar a la autoridad supervisora será realizado por el Punto de Contacto de Privacidad, previamente aprobado por el Comité de Privacidad Corporativa.

17. DISPOSICIONES FINALES

- **Consecuencias de las infracciones**

Un incumplimiento negligente o incluso intencional de esta política puede resultar en acciones bajo la ley laboral, incluyendo despido con o sin previo aviso. También pueden considerarse sanciones penales y consecuencias civiles, como daños y perjuicios.

- **Rendición de cuentas**

El cumplimiento de los requisitos de esta directriz debe ser verificable en todo momento. En este contexto, debe prestarse especial atención a la trazabilidad y transparencia de las medidas adoptadas, por ejemplo mediante la documentación correspondiente.

- **Actualización de la política; verificabilidad**

En el contexto del ulterior desarrollo de la legislación sobre protección de datos, así como de los cambios tecnológicos u organizativos, esta directriz se revisará periódicamente para determinar si debe adaptarse o completarse.

Las enmiendas a esta política serán efectivas informalmente. Los empleados y funcionarios serán notificados de los requisitos modificados de forma inmediata y adecuada.

18. REFERENCIAS

Esta política forma parte de la normativa sobre protección de datos. Esta política es anulada por las leyes y reglamentos, mientras que varios otros reglamentos internos y documentación siguen e implementan esta política. Por ejemplo:

- Código Etico
- Política de uso de medios tecnológicos
- Código Ético de proveedores

La normativa interna y la documentación complementaria podrán incluir, en particular, la realización de las medidas de protección y seguridad de los datos que deban adoptarse. Estos incluyen, entre otros, el estatuto del personal y la declaración de protección de datos.

En caso de oposición, se aplicará el siguiente orden de precedencia:

- Leyes y reglamentos
- Esta Política de Protección de Datos
- Otros reglamentos internos y documentación subordinado.

En caso necesario, los documentos se adaptarán inmediatamente en el sentido de las disposiciones superordenadas.