CD MARINO

Política y protocolo de confidencialidad y protección de datos para empleados

Mediante la presente comunicación se informa de las normas internas de obligado cumplimiento y, además, se recaba, de forma expresa y por escrito, el compromiso, consentimiento y aceptación del Trabajador/a con las mismas.

De conformidad con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y con la LEY ORGÁNICA 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), CD MARINO, con NIF G38105938 y domicilio Avda. Arquitecto Gomez Cuesta, 17 Arona (38660), Santa Cruz de Tenerife (en adelante, "Responsable del Tratamiento"), informa al trabajador/a de las siguientes normas internas de obligado cumplimiento.

Según la AEPD "todo el personal que acceda a los datos de carácter personal está obligado a conocer y cumplir las medidas, normas, procedimientos, reglas y estándares que se refieran a las funciones que desarrolla".

Sirva la presente comunicación del Responsable del Tratamiento para dar cumplimiento efectivo a su deber de informar al personal laboral correctamente, tratando de evitar así eventuales brechas de seguridad y pérdidas de información de las bases de datos.

NORMAS INTERNAS: CLÁUSULAS, FUNCIONES Y OBLIGACIONES DEL PERSONAL

1.- Designación del DPO o persona responsable de la protección de datos

CD MARINO ha designado un DPO o persona responsable de la protección de datos que está a disposición de todos los trabajadores y que se encargará de coordinar, controlar, desarrollar y verificar el cumplimiento de la normativa.
Nombre del DPO: José Manuel Pinto Segovia
Email del DPO: dpd@tudelegado.com

2.- Conceptos básicos de protección de datos

A fin de conocer mejor las normas de protección de datos, se definen los siguientes conceptos básicos de protección de datos:
Datos personales: toda información relativa a una persona física por la cual pueda determinarse su identidad.
Tratamiento: Cualquier operación o conjunto de operaciones realizada sobre datos personales: obtención, acceso, intervención, transmisión, conservación y supresión.
Interesado: Persona física respecto de la que se tratan datos personales.
Responsable del tratamiento: Organización que determina los fines y los medios del tratamiento.
Personal autorizado: Persona autorizada por el Responsable para realizar un tratamiento de datos mediante un compromiso de confidencialidad.
Encargados del tratamiento: Organización que trata datos personales por cuenta del Responsable.
Destinatarios de datos: Organización distinta del Encargado, que recibe una comunicación de datos personales del Responsable.
Datos de categoría especial o especialmente sensibles: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.
Principios fundamentales del tratamiento de datos:
Principio de licitud: se deben tratar los datos personales solo cuando haya una base de legitimación adecuada para ello. Además, los datos deben ser tratados de forma leal y transparente, informando a los interesados.
Principio de limitación de los fines: los datos no pueden ser tratados para finalidades distintas a las determinadas inicialmente.
Principio de minimización de los datos: se deben tratar únicamente los datos personales que sean adecuados, pertinentes y limitados a lo necesario para la finalidad.
Principio de exactitud: se deben adoptar todas las medidas necesarias para que los datos sean exactos y actualizados.
Principio de limitación del plazo de conservación: se deben mantener los datos únicamente durante el tiempo necesario para su tratamiento.
Principio de integridad y confidencialidad: se debe garantizar la seguridad de los datos personales, evitando las violaciones de seguridad.
Principio de responsabilidad proactiva: se debe cumplir con la normativa y demostrar el cumplimiento.

3.- Medidas de seguridad

CD MARINO ha implementado las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado a los riesgos del tratamiento como consecuencia de la destrucción accidental o ilícita de datos, la pérdida, alteración o comunicación no autorizada y el acceso no autorizado a los datos.

El correo electrónico, las redes sociales y/o aplicaciones móviles de mensajería, tales como WhatsApp, Telegram, Facebook Messenger, Snapchat, Viber, Skype, Kik Messenger, etc., perfiles en navegadores de internet (Google Chrome, Mozilla Firefox, Safari, etc), tanto corporativos como personales, que hayan sido instalados en terminales propiedad de la empresa, están sujetos a medidas de supervisión continua a razón de interés legítimo del empresario y de acuerdo con el artículo 20.3 del Estatuto de los Trabajadores.

4.- Funciones y obligaciones del personal

4.1.- Almacenamiento seguro de datos

Se deben almacenar o conservar los datos en el soporte establecido a tal fin, de manera que se garantice la seguridad de los mismos.
Los datos no deberán conservarse de forma desorganizada o desordenada en el escritorio a fin de evitar que personas no autorizadas tengan acceso a los datos personales. Por ello, se seguirá una política de mesas limpias.

4.2.- Instalación por parte del personal laboral de programas por cuenta propia

Los empleados/as tienen prohibido instalar programas sin autorización y/o conocimiento del empleador. Toda vez que se requiera la instalación de un programa en un dispositivo de la compañía se deberá solicitar una autorización al empleador a fin de verificar la seguridad del equipo y de los datos personales contenidos en el mismo.

4.3.- Actualización de software y hardware

Los empleados/as deben actualizar los software y hardware siempre que hayan actualizaciones disponibles.
Las actualizaciones deben obtenerse de una fuente de confianza, prohibiéndose expresamente descargar programas y/o actualizaciones de sitios web no fiables.
En caso de que un software utilizado sea obsoleto y no se realicen más actualizaciones por parte del proveedor, el software dejará de ser utilizado.

4.4.- Destrucción y reutilización de equipos y soportes

La destrucción de la documentación física o impresa que contiene datos personales debe llevarse a cabo siguiendo un protocolo previo. Los trabajadores/as no pueden tirar los documentos directamente a la basura o romperlos en trozos.
Se han establecido métodos seguros por parte del empleador para destruir documentación con datos personales, como triturar el papel con una destructora de papel y/o subcontratar a una empresa especializada en destrucción de papel.

4.5.- Traslado de soportes

El traslado de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado.
El personal con acceso a los soportes y, autorizados para realizar el traslado de los mismos, deberá cumplimentar un registro con los datos identificativos del dispositivo o soporte, la fecha, el lugar de traslado y con el propio nombre de la persona que realiza el traslado:

Soporte con núm. identificativo:

Fecha de traslado:

Traslado/Ubicación:

Trabajador/a:

4.6.- Copias de seguridad

El/la trabajador/a realizará copias de seguridad de la información de forma periódica para garantizar la disponibilidad y continuidad de los datos personales.
Las copias de seguridad deberán almacenarse en el lugar seguro determinado por el Responsable.

4.7.- Uso adecuado internet y redes WIFI

Los trabajadores/as deben procurar un uso seguro de Internet y las redes WIFI, informando en todo caso al Delegado de Protección de Datos o a la persona responsable de cualquier incidencia que pueda comprometer la seguridad del sistema y de los datos de carácter personal.
Los trabajadores/as tienen prohibido expresamente el acceso a páginas web que puedan suponer una actividad ilegal, o de contenido no relacionado con el trabajo, así como también el acceso a páginas que puedan ser contrarios a la moral.
En caso de que los trabajadores/as utilicen los equipos y dispositivos de la empresa fuera del centro de trabajo tienen prohibido conectarse a redes WIFI públicas o de acceso gratuito.

4.8.- Uso de contraseñas

El personal laboral tiene prohibido expresamente compartir o divulgar las claves de acceso tanto a los equipos informáticos, programas y/o cualquier soporte al que se

acceda con contraseña. Asimismo, queda prohibido escribir la contraseña en un lugar visible en el puesto de trabajo.
Se recuerda que para mantener la efectividad de las contraseñas se recomienda cambiarlas periódicamente.

4.9.- Uso adecuado del correo electrónico

El trabajador/a titular de la cuenta de correo electrónico profesional será responsable del uso de la misma y deberá utilizarla de manera profesional.
Las direcciones de email son consideradas datos personales por lo que, en caso de enviar un correo a más de un destinatario, deberá enviarse con copia oculta (marcando la casilla CCO), en caso de que no sea estrictamente necesario que cada uno de los destinatarios conozca la dirección de email del resto. De no proceder de esta manera se podría entender que se ha producido una divulgación no autorizada de datos personales.
El envío de correos con fines comerciales o publicitarios debe realizarse únicamente en caso de disponer del consentimiento del destinatario o de existir una relación contractual previa y ofrecer servicios y/o productos del mismo tipo que los contratados inicialmente.
En este tipo de correos debe constar la cláusula de protección de datos y la opción de baja en el envío de comunicaciones comerciales de forma totalmente gratuita e inmediata.

4.10.- Ejercicios de derechos

En caso de que el/la empleado/a reciba una solicitud de ejercicio de derecho de acceso, de supresión, de rectificación, de limitación del tratamiento, de portabilidad o de oposición por parte de algún interesado o de su representante legal, éste deberá dar traspaso de esta solicitud a la persona responsable de protección de datos o, en su caso, al Delegado de Protección de Datos en el menor tiempo posible.
El/la trabajador/a debe tener en cuenta que las solicitudes de ejercicio de derechos deben ser atendidas en un plazo máximo de un mes, por lo que es de vital importancia que se de traslado en tiempo y forma a quien corresponde para que cuente con el tiempo suficiente para atender la petición.

4.11.- Gestión de incidentes de seguridad

En caso de producirse una violación de seguridad respecto de datos personales el/la trabajador/a deberá comunicar este hecho de forma inmediata y sin dilación indebida al responsable de protección de datos o al Delegado de Protección de Datos.
Se entiende por violación de seguridad cualquier hecho que suponga una destrucción o pérdida accidental o indebida de los datos personales, así como cualquier alteración, acceso o comunicación no autorizada a los datos.
El/la trabajador/a debe tener en cuenta que las violaciones de seguridad deben comunicarse a la autoridad competente en un plazo máximo de 72 horas desde que

se tuvo conocimiento del incidente. Por tanto, la notificación inmediata a quien corresponde tiene una importancia capital puesto que la falta de notificación a la autoridad competente en plazo puede acarrear consecuencias económicas para la organización. Asimismo, la no comunicación de un incidente puede agravar sus consecuencias, al no tomarse las medidas correctivas necesarias.

4.12.- Confidencialidad

Se recuerda a los trabajadores que, de conformidad con la Ley 1/2019, de 20 de febrero, de Secretos Empresariales (LSE), el/la trabajador/a tiene la obligación de mantener la confidencialidad de la información calificada como secreto empresarial, definiéndose como secreto empresarial toda aquella información que ha sido objeto de medidas razonables por parte de su titular para mantenerla en secreto y que tiene un valor comercial.
La prohibición de revelación de secretos empresariales se extiende incluso una vez finalizada la relación laboral entre el/la TRABAJADOR/A y CD MARINO.

4.13.- Denuncias internas

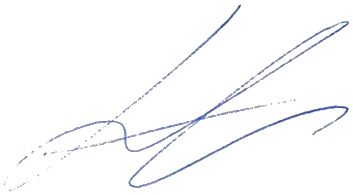
En caso de que el/la empleado/a detecte que se ha cometido un acto contrario a la normativa general o sectorial de protección de datos aplicable podrá realizar una denuncia de forma anónima mediante el canal de denuncias internas.

Declaro haber leído, entendido y comprendido toda la información que contienen las cláusulas informativas que incorpora el presente documento.

En Arona, a 28 de febrero de 2023

Nombre y apellidos del trabajador/a: Juan García Zuleta

DNI del trabajador/a: 49517322R



CD MARINO

Contrato de confidencialidad con trabajadores

En Arona, a 28 de febrero de 2023

REUNIDOS

De una parte, D./Dª Francisco García Santamaría, con NIF 42046198J y domicilio a estos efectos en Avda. Arquitecto Gomez Cuesta, 17 Arona (38660), Santa Cruz de Tenerife.

De otra parte, D./Dª Juan García Zuleta con DNI/NIE núm. 49517322R.

INTERVIENEN

El primero, en nombre y representación de CD MARINO, (en adelante, RESPONSABLE).

El segundo, en nombre y representación propia (en adelante, TRABAJADOR/A).

Y, reconociéndose ambas partes, mutua y recíprocamente con capacidad legal suficiente para el presente acto,

EXPONEN

A.- Que, Juan García Zuleta es trabajador/a de CD MARINO.

B.- Que de conformidad con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y la LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, de Protección de datos y garantía de derechos digitales (LOPDGDD), el/la TRABAJADOR/A, como persona que tiene asignadas tareas o funciones que implican un eventual acceso o tratamiento de los datos personales ha sido informado de las normas y políticas relativas al tratamiento de datos personales, las cuales son de obligado cumplimiento.

En particular, el/la trabajador/a:

Se compromete a ser diligente en el uso de los datos personales a los que tenga acceso por razón de su puesto de trabajo.

Sólo puede utilizar los datos personales objeto de tratamiento para las finalidades que le haya indicado expresamente el Responsable del Tratamiento. En ningún caso podrá utilizar los datos para fines propios.

Siempre deberá tratar los datos personales de acuerdo con sus funciones laborales.

Debe mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del desarrollo de sus funciones o tareas laborales, incluso después de que finalice su relación laboral.

Debe garantizar y respetar la confidencialidad de los datos personales a los que tenga acceso, así como mantener el compromiso de cumplir con las medidas de seguridad correspondientes.

Tiene la obligación de notificar sin demora injustificada cualquier incidencia de la que tenga conocimiento al DPO o persona responsable de la protección de datos para su conocimiento y aplicación de medidas técnicas y organizativas para mitigar los efectos que esta hubiera podido ocasionar. El conocimiento y no notificación de una incidencia por parte del trabajador se considerará sancionable.

C.- Que, de conformidad con la Ley 1/2019, de 20 de febrero, de Secretos Empresariales (LSE), el/la TRABAJADOR/A tiene la obligación de mantener la confidencialidad de la información calificada como secreto empresarial, definiéndose como secreto empresarial toda aquella información que ha sido objeto de medidas razonables por parte de su titular para mantenerla en secreto y que tiene un valor comercial.

La prohibición de revelación de secretos empresariales se extiende incluso una vez finalizada la relación laboral entre el/la TRABAJADOR/A y CD MARINO.

D.- Ley aplicable y foro.

El presente contrato se regirá e interpretará conforme a la legislación española en aquello que no esté expresamente regulado, sometiéndose las partes, para las controversias que pudieran surgir en relación con el mismo, a la competencia de los Juzgados y Tribunales del lugar de prestación de los servicios, del lugar del domicilio social de la empresa o del lugar de residencia habitual del/la TRABAJADOR/A.

Y en prueba de su conformidad, firman las partes el presente contrato en duplicado ejemplar y a un sólo efecto, en lugar y fecha señalados en el encabezamiento.

Francisco García Santamaría (13 mar. 2023 10:31 GMT)

D./Dª. Francisco García Santamaría

Por RESPONSABLE

D./Dª. Juan García Zuleta

TRABAJADOR/A

CD MARINO

Cláusula de cesión de derechos de imagen

El Trabajador/a abajo firmante autoriza a CD MARINO a que incluya en cualquier soporte audiovisual, para efectos de reproducción y comunicación pública, la imagen del trabajador/a en el marco del desempeño de sus actividades laborales, con fines de dar a conocer su producto/servicio en redes sociales, para la realización de acciones comerciales u otras campañas online.

Esta autorización que firma expresamente el trabajador, es una autorización de uso del contenido grabado y de su imagen, y se hace al amparo de lo dispuesto en la Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen. La autorización que aquí se concede tendrá un uso de carácter publicitario, para la realización de acciones comerciales y formará parte de las campañas publicitarias de la empresa en redes sociales y otros medios online.

El consentimiento otorgado por el/la trabajador/a es revocable en cualquier momento.

Autorizo al Responsable del Tratamiento para que incluya en cualquier soporte audiovisual, para efectos de reproducción y comunicación pública, mi imagen, y que la utilice con fines de dar a conocer su producto/servicio en redes sociales, para la realización de acciones comerciales u otras campañas online

En Arona, a 28 de febrero de 2023

Nombre y apellidos trabajador/a: Juan García Zuleta

NIF: 49517322R

CD MARINO

Cláusula de uso de redes sociales como sistema de comunicación de la empresa

Se informa al trabajador/a que CD MARINO ha establecido como sistema de comunicación interno, como método válido para realizar comunicaciones de empresa, el uso de redes sociales y/o aplicaciones móviles de mensajería, tales como WhatsApp, Telegram, Facebook Messenger, Snapchat, Viber, Skype, Kik Messenger, etc.

Los trabajadores/as aceptan y consienten el uso de estas redes sociales o aplicaciones móviles, también en sus propios equipos móviles y dispositivos, es decir, no sólo en los de la empresa, para enviar y facilitar información de la empresa, si bien se comprometen a aplicar en sus equipos móviles las medidas de seguridad equivalentes para evitar hipotéticas brechas y violaciones de seguridad de la información.

Por su parte, CD MARINO ha adoptado una política de desconexión digital que se encuentra a disposición de los trabajadores a fin de garantizar que los trabajadores puedan conciliar su vida laboral con su vida familiar. En virtud de dicha política no existe obligación alguna por parte del trabajador/a de hacer uso de los dispositivos móviles y los sistemas de comunicación de la empresa fuera del horario laboral, no pudiendo ser sancionados por este hecho.

Autorizo el uso de redes sociales y aplicaciones móviles, en los equipos móviles y dispositivos de mi propiedad, como sistema de comunicación interna con los demás trabajadores/as y para recibir/enviar directrices, órdenes e información de la empresa

En Arona, a 28 de febrero de 2023
Nombre y apellidos trabajador/a: Juan García Zuleta
NIF: 49517322R

Cláusulas Protección de Datos Juan García - CD_MARINO

Informe de auditoría final 2023-03-13

Fecha de creación:	2023-02-28
Por:	TuDelegadoCom Protección de Datos (info@tudelegado.com)
Estado:	Firmado
ID de transacción:	CBJCHBCAABAA1Z7FDdIzGDwXmp1szglptBPEpMkS7sIW

Historial de “Cláusulas Protección de Datos Juan García - CD_MARINO”

TuDelegadoCom Protección de Datos (info@tudelegado.com) ha creado el documento.
2023-02-28 - 18:41:02 GMT- Dirección IP: 88.13.108.111.

El documento se ha enviado por correo electrónico a juancdmarino@gmail.com para su firma.
2023-02-28 - 18:42:26 GMT

El documento se ha enviado por correo electrónico a presidentecdmarino@gmail.com para su firma.
2023-02-28 - 18:42:26 GMT

juancdmarino@gmail.com ha visualizado el correo electrónico.
2023-02-28 - 18:52:44 GMT- Dirección IP: 104.28.88.126.

El firmante juancdmarino@gmail.com firmó con el nombre de Juan Camilo GZ
2023-03-01 - 9:32:13 GMT- Dirección IP: 77.211.5.206.

Juan Camilo GZ (juancdmarino@gmail.com) ha firmado electrónicamente el documento.
Fecha de firma: 2023-03-01 - 9:32:15 GMT. Origen de hora: servidor.- Dirección IP: 77.211.5.206.

presidentecdmarino@gmail.com ha visualizado el correo electrónico.
2023-03-13 - 10:28:59 GMT- Dirección IP: 104.28.88.123.

El firmante presidentecdmarino@gmail.com firmó con el nombre de Francisco García Santamaría
2023-03-13 - 10:31:14 GMT- Dirección IP: 176.87.38.14.

Francisco García Santamaría (presidentecdmarino@gmail.com) ha firmado electrónicamente el documento.
Fecha de firma: 2023-03-13 - 10:31:16 GMT. Origen de hora: servidor.- Dirección IP: 176.87.38.14.

Documento completado.
2023-03-13 - 10:31:16 GMT