Adaptación al nuevo Reglamento Europeo de Protección de Datos RGPD

SUSANA PÉREZ REGLERO

Mayo 2018

ÍNDICE

.

ANEXOS:

1.- NUEVO REGLAMENTO

El 25 de mayo de 2018 se cumplen dos años desde la entrada en vigor del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante, RGPD. Desde ese momento, será aplicable el RGPD y será obligatorio el cumplimiento de los requerimientos y obligaciones para el responsable y el encargado de tratamiento que este incluye, entre las que destaca, la necesidad de llevar a cabo un análisis de riesgos con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

Ante la constante evolución tecnológica y los procesos de transformación digital que sufren las actividades de tratamiento de datos personales, la reforma de la regulación de protección de datos supone un cambio del modelo tradicional para afrontar las medidas que garantizan la protección de los datos personales hacia un nuevo modelo más dinámico, enfocado en la gestión continua de los riesgos potenciales asociados al tratamiento desde su diseño.

El diseño adecuado de las actividades de tratamiento es un aspecto clave para poder garantizar los derechos y libertades de los interesados. La fase de diseño de un tratamiento define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo. De igual modo, es el momento idóneo para definir las medidas de control y seguridad para garantizar los derechos y libertades de los interesados con el objetivo de que un tratamiento nazca respetando los requerimientos de privacidad asociados al nivel de riesgo a la que está expuesto.

SUSANA PÉREZ REGLERO ha procedido a la elaboración de la normativa de seguridad de obligado cumplimiento para todo el personal con acceso a los datos de carácter personal. En el presente Documento se recogen las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

2.- NUEVOS PRINCIPIOS

1- **PRINCIPIO DE RESPONSABILIDAD (ACCOUNTABILITY)**. Habrá que implementar mecanismos que permitan acreditar que se han adoptando todas las medidas necesarias para tratar los datos personales como exige la norma. Es una responsabilidad proactiva. Las organizaciones deben ser capaces de demostrar que cumplen dichas exigencias, lo cual obligará a desarrollas políticas, procedimientos, controles, etc.

2- **PRINCIPIOS DE PROTECCIÓN DE DATOS POR DEFECTO Y DESDE EL DISEÑO**. Se deberán adoptar medidas que garanticen el cumplimiento de la norma desde el mismo momento en que se diseñe una empresa, producto, servicio o actividad que implique tratamiento de dato, como regla y desde el origen.

3- **PRINCIPIO DE TRANSPARENCIA**. Los avisos legales y políticas de privacidad deberán ser más simples e inteligibles, facilitando su comprensión, además de más completos. Incluso se prevé que, con el fin de informar sobre el tratamiento de los datos, puedan utilizarse iconos normalizados.

3.- NUEVOS CONCEPTOS E INTERPRETACION

1- **GESTION DE RIESGOS**. Es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como, las medidas para su reducción o mitigación.

   La gestión de riesgos se puede dividir en **tres etapas** diferenciadas: La identificación, la evaluación y el tratamiento de los riesgos.

2- **PROTECCIÓN DE DATOS DESDE EL DISEÑO Y LA GESTION DE RIESGOS.** El responsable del tratamiento que realiza o desea realizar actividades de tratamiento con datos personales, debe establecer procedimientos de control que garanticen cumplir los principios de protección desde el diseño y por defecto.

   Definir y establecer medidas de control y seguridad es una tarea fundamental que se debe realizar de acuerdo a las particularidades de las actividades de tratamiento.

3- **REGISTRO ACTIVIDADES DE TRATAMIENTO**. Cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad". Adicionalmente indica que "cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable".

   En la práctica, puede identificarse un tratamiento como el conjunto de operaciones dirigidas a conseguir una determinada finalidad que se legitiman en una misma base jurídica. Cada tratamiento incluirá una serie de operaciones como, por ejemplo la recogida, registro, organización, estructuración, consulta o utilización de los datos.

4- **MEDIDAS TACNICAS Y ORGANIZATIVAS. E**l Reglamento Europeo de Protección de Datos obliga a las empresas a implementar **medidas técnicas y organizativas apropiadas** a fin de que se puedan acreditar y garantizar su cumplimiento. El reglamento nos avanza medidas pero no nos dice cuáles o cuáles de las existentes las considera óptimas "apropiadas para acreditar y garantizar" la protección.

   A cada riesgo previamente identificado y evaluado debemos establecerle un control que nos lleve a poder medir – y acreditar – que hemos puesto esa medida de control y que funciona.

4.- NUEVAS OBLIGACIONES Y GARANTIAS

1- En ocasiones, será obligatorio designar un Delegado de Protección de Datos (DPO), anteriormente Encargado de Seguridad, interno o externo, que asista a las organizaciones en el proceso de cumplimiento normativo. Esta figura sólo será necesaria en las empresas que hayan trabajadores contratados.

2- En ciertos casos, se deberán realizar **EVALUACIONES DE IMPACTO SOBRE LA PRIVACIDAD**, que determinen los riesgos específicos que supone tratar ciertos datos de carácter personal y prevean medidas para mitigar o eliminar dichos riesgos.

3- Las empresas multinacionales tendrán como interlocutora a una sola autoridad de control nacional: la del establecimiento principal de la entidad. Es lo que se conoce como **VENTANILLA ÚNICA**.

4- Las **BRECHAS DE SEGURIDAD** deberán ser comunicadas a las autoridades de control y, en casos graves, a los afectados, tan pronto sean conocidas, estableciéndose el plazo máximo de 72 horas.

5- **DATOS SENSIBLES:** Se amplían los datos especialmente protegidos, incluyendo ahora los datos genéticos y biométricos. Se incluyen también en esta categoría las infracciones y condenas penales, aunque no las administrativas.

6- **CONSENTIMIENTO EXPRESO:** Ya no sirve el consentimiento tácito que se tenía en cuenta anteriormente.

7- La **SELECCIÓN** de un encargado del tratamiento se endurece, puesto que habrá que elegir uno que aporte suficientes garantías de cumplimiento normativo.

8- **GARANTÍAS ADICIONALES PARA LAS TRANSFERENCIAS INTERNACIONALES DE DATOS:** Establecimiento de garantías más estrictas y mecanismos de seguimiento en relación con las transferencias internacionales de datos fuera de la Unión Europea.

9- **SELLOS Y CERTIFICACIONES:** Se prevé que se creen sellos y certificaciones de cumplimiento que permiten acreditar la Accountability por parte de las organizaciones.

10- **DESAPARECE LA OBLIGACIÓN DE INSCRIBIR LOS FICHEROS**, que se sustituye por un control interno y, en algunos casos, un inventario de las operaciones de tratamiento de datos que se realicen, lo que se denomina Registro de Actividades.

11- **SANCIONES:** Las cuantías de las sanciones por incumplimiento de la norma crecen, pudiendo llegar a los 20 millones de euros o el 4% de la facturación global anual (no se excluye de las multas a las Administraciones Públicas, aunque los Estados Miembros pueden acordarlo así).

5.- NUEVOS DERECHOS

Se informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:

Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.

Para el **derecho de acceso** se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.

Para el **derecho de rectificación** se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.

Para el **derecho de supresión** se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.

Para el **derecho de portabilidad** los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

6.- MEDIDAS DE SEGURIDAD EXIGIDAS

Las medidas que el RGPD exige a los responsables, y en ocasiones a los encargados, aplicar para garantizar que los tratamientos se realizan adecuadamente y puedan demostrarlo son las siguientes:

1. Análisis de riesgo. El nuevo GDPR exige que todas las organizaciones que tratan datos realicen un **análisis de riesgo** de sus tratamientos para poder determinar qué medidas han de aplicar y cómo hacerlo.

El tipo de análisis variará en función de:

- Los tipos de tratamiento
- La naturaleza de los datos
- El número de interesados afectados
- La cantidad y variedad de tratamientos que una misma organización lleve a cabo

2. Registro de actividades de tratamiento. Principio de Transparencia "Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado". (art. 5.1.a GDPR) Su materialización conlleva un importante cambio, ya que desaparece la obligación de notificar y registrar los ficheros que contienen datos personales ante la autoridad de control por un nuevo **"Registro de actividades de tratamiento"**.

Este registro se llevará a cabo de forma interna y contendrá, entre otros, los siguientes datos:

- nombre y datos de contacto del responsable del tratamiento,
- nombre y datos del Delegado de Protección de Datos,
- finalidad del tratamiento,
- descripción de categorías del interesado,
- descripción de categorías de datos tratados,
- las transferencias internacionales de datos.

En España, este nuevo registro puede integrarse de momento en el **Documento de Seguridad**, hasta que la Agencia Española de Protección de Datos facilite Instrucciones concretas acerca de su formato y gestión.

3. Protección de datos desde el diseño y por defecto. Actualmente el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (LOPD) establece en España la obligación de aplicar diferentes medidas en función del nivel de seguridad - básico, medio o alto - de los datos tratados.

El nuevo RGPD no distingue entre los niveles de los ficheros, sino que especifica que se apliquen medidas de seguridad teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas. (**Artículo 25 Protección de datos desde el diseño y por defecto**).

La protección de datos desde el diseño y por defecto es una cuestión de estrategia que, tanto el responsable como el encargado del tratamiento, deben tener en consideración para asegurar el derecho a la protección de datos mediante la adopción de medidas que consideren al titular de los datos personales

El RGPD, bajo el principio de responsabilidad proactiva (Artículo 5.2), exige al responsable del tratamiento que aplique las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. Algunas de estas medidas serían por ejemplo la custodia de soportes, la seguridad en redes de comunicación, las copias de respaldo o el control de acceso a los datos.

El RGPD propone, como mecanismos efectivos de verificación del cumplimiento, la adhesión a **códigos de conducta** o a **mecanismos de certificación** (artículo 42.3 del RGPD).

Por tanto, lo que el RGPD exige es que las empresas tengan una actitud consciente, diligente y proactiva del tratamiento de los datos, pudiendo demostrar, si llegara el caso, las medidas de seguridad aplicadas.

El nuevo Reglamento europeo de protección de datos habla de **"medidas técnicas y organizativas apropiadas"** para garantizar un nivel de seguridad adecuado al riesgo, para el caso de datos de bajo riesgo como son los que se manejan en este caso.

7.- PRINCIPALES OBJETIVOS A SEGUIR

1- **Analizar los tratamientos y preparar el registro de actividades**

2- **Garantizar el principio de Transparencia, Responsabilidad o "Accountability"**

3- **Regularizar y legitimar el consentimiento**

4- **Actualizar los contratos con encargados de tratamientos**

5- **Atender a los nuevos derechos incorporados en el RGPD**

6- **Crear protocolo de notificaciones de violaciones de seguridad**

8.- PROCEDIMIENTOS DE NOTIFICACION RENOVADO

Otra de las novedades más importantes se trata de una nueva obligación que el RGPD impone al responsable del tratamiento: notificar las violaciones de seguridad de los datos.

Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: https://sedeagpd.gob.es

9.- DELEGADO DE PROTECCION DE DATOS

Se introduce la nueva figura del Data Protection Officer o Delegado de Protección de Datos, que asume nuevas y cualificadas competencias en materia de coordinación y control del cumplimiento de la normativa de protección de datos. Sus funciones se centran en:

- Informar y asesorar al responsable del tratamiento de datos de las obligaciones que debe efectuar para cumplir con el Reglamento General. Debe dejar constancia en papel de las comunicaciones con el responsable del tratamiento y sus respuestas.
- Supervisar la aplicación de las normas por el encargado del tratamiento en materia de protección de datos personales. Dentro de este apartado se incluyen: asignación de responsabilidades, formación del personal y auditorías correspondientes.
- Supervisar la documentación, notificación y comunicación de las violaciones de datos personales.
- Supervisar la respuesta a las solicitudes de la autoridad de control y cooperar con ella por solicitud de las mismas o por iniciativa propia.
- Ejercer de punto de contacto con la autoridad de control sobre cuestiones relacionadas con el tratamiento de datos personales.

Dicha figura será obligatoria cuando:

- El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.

- Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de datos a gran escala.

- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas o infracciones penales.

Las empresas que no encajen en esta clasificación pueden valorar contar con esta figura, que tendrá como funciones la gestión y el control de la protección de datos dentro de la empresa, así como actuar como punto de contacto entre esta y la AEPD.

Recomendación: Nombrar a un responsable interno y contratar un servicio externo de resolución de consultas especializadas y para disfrutar de un servicio de seguimiento jurídico.

ANEXO A. DOCUMENTO DE ANALISIS BASICO DE RIESGOS "SUSANA PÉREZ REGLERO"

OPERACIONES DE TRATAMIENTO		
CAPTURA DE DATOS	ALMACENAMIENTO	USO

RIESGOS POR DEFECTO

	TIPO DE RIESGO	RIESGO	MEDIDAS
PROTECCION DE DATOS PERSONALES	- CONFIDENCIALIDAD - INTEGRIDAD - DISPONIBILIDAD	- ACCESO ILEGITIMO - PERDIDA DE DATOS	- ANTIVIRUS - COPIA SEGURIDAD - ENCARGADO TRATAMIENTO
DERECHOS Y LIBERTADES DE LOS INTERESADOS	- TRATAMIENTO ILICITO - AUSENCIA ATENCION DERECHOS	- RECLAMACIONES	- SEGUIMIENTO DATOS

Teniendo en cuenta el análisis básico de riesgos realizado, los siguientes anexos se han confeccionado para tratamientos de datos personales de bajo riesgo de donde se deduce que el mismo no podrá ser utilizado para tratamientos de datos personales que incluyan datos relativos al origen étnico o racial, ideología política religiosa o filosófica, filiación sindical, datos genéticos y biométricos, datos de salud, y datos de orientación sexual de las personas así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas.

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

Según el tipo de tratamiento que se ha puesto de manifiesto en el análisis de riesgo, las medidas mínimas de seguridad adoptadas son las siguientes:

ANEXO B. MEDIDAS DE SEGURIDAD ADOPTADAS POR "SUSANA PÉREZ REGLERO"

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.

- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.

- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.

- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).

- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.

- **ANTIVIRUS**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

- **FIREWALL**: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.

- **CIFRADO DE DATOS**: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.

- **COPIA DE SEGURIDAD**: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica.

MEDIDAS ORGANIZATIVAS

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

DEBER DE CONFIDENCIALIDAD Y SECRETO

- Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.

- Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.

- No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

- No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.

- El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)

- **UBICACIÓN DE LAS CÁMARAS**: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.

- **UBICACIÓN DE MONITORES**: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.

- **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.

- **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo. En la página web de la Agencia disponen de modelos, tanto del pictograma como del texto.

- **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

- **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.

  No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

Para más información puede consultar las guías de videovigilancia de la Agencia Española de Protección de Datos que se encuentran a su disposición en la sección de publicaciones de la web www.agpd.es.

ANEXO C. REGISTRO DE ACTIVIDADES DE TRATAMIENTO (RESPONSABLE DE TRATAMIENTO)

Responsable de tratamiento	SUSANA PÉREZ REGLERO - 13158327G - C/ LUIS CERNUDA, nº 11-4 – 09006 – BURGOS
Delegado de Protección de Datos	NO PROCEDE

Actividad de tratamiento	GESTION DE CLIENTES

Finalidad	PUBLICIDAD Y RESERVA DE VIAJES

Categorías de interesados	CLIENTES

Categorías datos personales	DATOS IDENTIFICATIVOS

Cesión de datos	NO SE CONTEMPLAN

Transferencias internacionales	NO SE CONTEMPLAN

Periodo de conservación	HASTA QUE FINALICE LA RELACION COMERCIAL

Medidas de seguridad	COPIAS SEGURIDAD, CIFRADO DATOS, FIREWALL, ANTIVIRUS Y ACTUALIZACION DE LOS EQUIPOS

ANEXO D. DESCRIPCION DE LAS ACTIVIDADES DE TRATAMIENTO

CICLO DE VIDA DE LOS DATOS EN LAS OPERACIONES DEL TRATAMIENTO DE "SUSANA PÉREZ REGLERO"

CAPTURA DE DATOS	**Actividades del proceso**	Formulario web, teléfono y correo electrónico
	Datos tratados	Nombre y apellidos, NIF, dirección, teléfono y correo electrónico.
	Intervinientes involucrados	Responsable de tratamiento y el propio interesado
	Tecnologías intervinientes	Servidor web y aplicación correo electrónico

ALMACENAMIENTO DE LOS DATOS	**Actividades del proceso**	Se almacenan en el equipo informático y servidor web
	Datos tratados	Nombre y apellidos, NIF, dirección, teléfono y correo electrónico.
	Intervinientes involucrados	Responsable y encargado de tratamiento
	Tecnologías intervinientes	Servidor web y aplicación correo electrónico

USO Y TRATAMIENTO DE LOS DATOS	**Actividades del proceso**	Gestión de la relación con los clientes
	Datos tratados	Nombre y apellidos, NIF, dirección, teléfono y correo electrónico.
	Intervinientes involucrados	Responsable y encargado de tratamiento y personal contratado
	Tecnologías intervinientes	Servidor web y aplicación correo electrónico

TRANSFERENCIAS Y CESIONES PREVISTAS	**Actividades del proceso**	No se contemplan cesiones ni transferencias
	Datos tratados	No se contemplan cesiones ni transferencias
	Intervinientes involucrados	No se contemplan cesiones ni transferencias
	Tecnologías intervinientes	No se contemplan cesiones ni transferencias

DESTRUCCION	**Actividades del proceso**	Eliminación y destrucción
	Datos tratados	Datos facilitados por el interesado
	Intervinientes involucrados	Responsable y encargado de tratamiento
	Tecnologías intervinientes	Eliminación de base de datos y destructora en caso de datos en papel

ANEXO E. REGISTRO DE ACTIVIDADES DE TRATAMIENTO (ENCARGADO DE TRATAMIENTO)

Encargado del tratamiento	FJ CONSULTING TRAVEL SERVICES, S.L. - B98915044 – C/ CREU ROJA, Nº 1 BLOQUE 5, SS 17 – 46014 VALENCIA
Delegado de Protección de Datos	NO PROCEDE

DESCRIPCION DE LOS TRATAMIENTOS DE DATOS

RESPONSABLE DEL TRATAMIENTO

Responsable del tratamiento	SUSANA PÉREZ REGLERO - 13158327G - C/ LUIS CERNUDA, nº 11-4 – 09006 – BURGOS

CATEGORIA DE TRATAMIENTO

Categoría de tratamiento	DATOS IDENTIFICATIVOS

TRANSFERENCIAS DE DATOS PERSONALES

Transferencias y cesiones	NO SE CONTEMPLAN

MEDIDAS DE SEGURIDAD

Medidas de seguridad	COPIAS SEGURIDAD, CIFRADO DATOS, FIREWALL, ANTIVIRUS Y ACTUALIZACION DE LOS EQUIPOS

ANEXO F. DERECHOS DE INFORMACION PARA ENVIAR A CLIENTES

.

TRATAMIENTO DE DATOS DE CLIENTES

Clausula informativa:

Estimado cliente,

En Europa hay una nueva normativa para proteger la privacidad de los clientes y usar correctamente sus datos. Por eso, a partir del 25 de mayo, nuestros términos de protección de datos cambian, y necesitamos tu autorización para poder seguir comunicándonos contigo.

Aquí tienes un resumen de los términos. Léelo y dinos si aceptas.

En cumplimiento de lo establecido en el nuevo Reglamento General de Protección de Datos (RGPD), de 25 de mayo 2016, le informamos que todos sus datos, pasarán a formar parte de un tratamiento cuyo responsable es:

SUSANA PEREZ REGLERO - NIF: 13158327G Dirección postal: C/ LUIS CERNUDA, Nº 11 P - 4
Teléfono: 659754225 Correo electrónico: susana@viajesluengotours.com

En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado y realizar la facturación del mismo. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en SUSANA PEREZ REGLERO estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios a la dirección postal indicada en los datos de la empresa. En caso de no estar satisfecho con nuestros procedimientos de sus derechos puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

Asimismo solicito su autorización para ofrecerle productos y servicios relacionados con los solicitados y fidelizarle como cliente.

SI ☐
NO ☐

Por favor, marca la opción deseada y reenvíanos este correo electrónico para tener constancia de tu decisión.

AVISO: Debe tener en cuenta que si su cliente marca la opción NO, en ningún caso podrá enviarle publicidad

ANEXO G. DERECHOS DE INFORMACION PARA INCLUIR EN LAS FACTURAS

En cumplimiento de lo establecido en el nuevo Reglamento General de Protección de Datos (RGPD), de 25 de mayo 2016, le informamos que todos sus datos, pasarán a formar parte de un tratamiento cuyo responsable es la empresa que figura en el encabezamiento de esta factura, cuya finalidad es la gestión, administración y mantenimiento de los productos y servicios solicitados por sus clientes relacionados con la venta de viajes en general.

En nombre de la empresa tratamos la información que nos facilita con el fin de prestarles el servicio solicitado y realizar la facturación del mismo. Los datos proporcionados se conservarán mientras se mantenga la relación comercial o durante los años necesarios para cumplir con las obligaciones legales. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en SUSANA PEREZ REGLERO estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios.

Con la firma de este documento, nos da su autorización para ofrecerle productos y servicios relacionados con los solicitados y fidelizarle como cliente.

ANEXO H. DERECHOS DE INFORMACION PARA CORREO ELECTRONICO Y MAILING

En cumplimiento de lo establecido en el nuevo Reglamento General de Protección de Datos (RGPD), de 25 de mayo 2016, le informamos que todos sus datos, pasarán a formar parte de un tratamiento cuyo responsable es:

SUSANA PEREZ REGLERO - NIF: 13158327G Dirección postal: C/ LUIS CERNUDA, Nº 11 P - 4
Teléfono: 659754225 Correo electrónico: susana@viajesluengotours.com

En nombre de la empresa tratamos la información que nos facilita con el fin de enviarle publicidad relacionada con nuestros productos y servicios por cualquier medio (postal, email o teléfono) e invitarle a eventos organizados por la empresa. Los datos proporcionados se conservarán mientras no solicite el cese de la actividad. Los datos no se cederán a terceros salvo en los casos en que exista una obligación legal. Usted tiene derecho a obtener confirmación sobre si en SUSANA PEREZ REGLERO estamos tratando sus datos personales por tanto tiene derecho a acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios para los fines que fueron recogidos a la dirección postal indicada en los datos de la empresa. En caso de no estar satisfecho con nuestros procedimientos de sus derechos puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

AVISO: Si compra datos personales a terceros para realizar publicidad de sus productos y servicios, debe tener en cuenta que los mismos proceden de fuentes accesibles al público y que están contrastados con la lista Robinson.

AVISO: Recuerde que debe borrar los datos cuando haya trascurrido un tiempo sin hacer uso de los mismos.

ANEXO I. DERECHOS DE INFORMACION PÁGINA WEB

Para sustituir el párrafo que hace mención a la Protección de datos dentro del aviso legal.

En cumplimiento de lo establecido en el nuevo Reglamento General de Protección de Datos (RGPD), de 25 de mayo 2016, le informamos que todos sus datos, pasarán a formar parte de un tratamiento cuyo responsable es SUSANA PÉREZ REGLERO con domicilio social en C/ Luis Cernuda, nº11-4, en la ciudad de Burgos, código postal 09006 y NIF: 13158327G, cuya finalidad es la gestión, administración y mantenimiento de los productos solicitados por sus clientes relacionados con la venta de viajes y productos turísticos en general.

Sus datos serán cedidos dentro del canal de ventas que colabora con SUSANA PÉREZ REGLERO en la comercialización de sus servicios, así como a aquellas otras personas o entidades cuya intervención sea necesaria para la prestación de los servicios por parte de SUSANA PÉREZ REGLERO al cliente o para responder a las solicitudes de productos o servicios realizadas por el cliente a través de los servicios de Internet prestados por SUSANA PÉREZ REGLERO. Dicha cesión solo podrá tener como finalidad la realización por parte de los cesionarios de labores de información, formación y comercialización en relación con los referidos productos y servicios solicitados por el cliente.

Para garantizar la protección y mantener la seguridad, integridad y disponibilidad de sus datos, utilizamos diversas medidas de seguridad. Aunque en las transmisiones de datos a través de internet o desde una web no es posible garantizar una protección absoluta, tanto nosotros como nuestros proveedores contratados, dedicamos los máximos esfuerzos para mantener las medidas de protección adecuadas para garantizar la protección de sus datos de acuerdo con las exigencias legales aplicables en esta materia. Entre eses medidas se encuentran la instalación de antivirus y firewalls para impedir accesos no autorizados.

Sus datos personales serán conservados durante el tiempo necesario para cumplir con la finalidad para la cual se recogieron. En todo caso, limitamos el acceso a sus datos sólo a aquellas personas que necesiten utilizarlos para el desempeño de sus funciones.

Nuestros plazos de conservación de datos están basados en necesidades de negocio, por tanto, los que ya no sean necesarios quedaran limitados al acceso de los mismos para dar cumplimiento a la normativa actual o se destruirán de forma segura.

Le informamos que puede ejercitar sus derechos de acceder a sus datos personales, rectificar los datos inexactos o solicitar su supresión cuando los datos ya no sean necesarios, dirigiéndose al domicilio social de SUSANA PÉREZ REGLERO. En caso de no estar satisfecho con nuestros procedimientos de sus derechos puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

ANEXO J. CONTRATO EMPRESAS DE SERVICIOS

SE ADJUNTA APARTE