MANUAL DE PROTOCOLOS Y PROCEDIMIENTOS SOBRE LA POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

INTRODUCCIÓN

El objetivo de este documento es la completa adaptación de **MARQUEZ JAIME, RAFAEL** al nuevo marco jurídico en materia de protección de datos, impuesto por el Reglamento (UE) 2016/679, del Parlamento Europeo y el 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 éstos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), plenamente aplicable en España desde el pasado 25 de mayo de 2.018.

MARQUEZ JAIME, RAFAEL incorpora así, a sus protocolos internos, todas las medidas, seguridades, controles y procesos exigidos por la referida normativa.

I. NORMATIVA APLICABLE.

La implementación de ésta Política de Privacidad y Protección de Datos Personales se ha llevado a cabo en virtud del Reglamento (UE) 2016/679, del Parlamento Europeo y el 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 éstos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD) y, a nivel nacional, del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (PLOPD), que reconfiguran todo el régimen jurídico de la protección de datos personales en nuestro país, sin olvidarnos de la Ley 34/2002, de 11 de julio, de Servicio de la Sociedad de la Información y de Comercio Electrónico (LSSI), así como sus normativas de desarrollo.

Este conjunto normativo tiene el objetivo general de proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de datos personales.

Como principal novedad, se introduce el principio de responsabilidad proactiva, que exige del responsable realizar un análisis detallado de los datos personales que se utilizan, de las finalidades y de los tipos de operaciones de tratamiento que se desarrollan en la entidad para aplicar las medidas que garanticen que dichos tratamientos son conformes al RGPD. Sin embargo, no es suficiente cumplir minuciosamente con la precitada normativa, sino que, además, éste principio implica que la entidad ha de estar en condiciones de demostrar el cumplimiento, ante posibles interesados y, en su caso, ante el órgano de control correspondiente.

II. POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES.

1.- Objetivos.

Este Manual de Protocolos y Procedimientos de **MARQUEZ JAIME, RAFAEL** consiste en un programa dirigido a aplicar las medidas técnicas y organizativas oportunas en función de los riesgos para los interesados detectados en cada uno de los tratamientos que realizamos con sus datos personales, a fin de eliminarlos o mitigarlos.

Es su finalidad última garantizar la implantación de la Política de Protección de Datos en la empresa, lo que implica que todo su personal, responsable o dependiente, la asuma como propia y, en consecuencia, actúe conforme a los códigos éticos y de conducta idóneos para que su actividad profesional se ajuste a la legalidad vigente, en una doble vertiente: por un lado, tomando todas las precauciones oportunas para garantizar la licitud del tratamiento y el ejercicio de los derechos por el interesado; y, por otro lado, aplicando las seguridades desde el diseño oportunas a fin de minimizar o eliminar los riesgos para los interesados que se desprendan del tratamiento. Lo que, adicionalmente, redunda también en el correcto funcionamiento y mejora de reputación de la entidad.

2.- Procedimientos de actuación:

La Política de Privacidad y Protección de Datos Personales se encuentra determinada por los siguientes elementos, los cuales, de forma conjunta, sirven a los fines indicados en el apartado anterior:

·**Análisis del riesgo inicial y Evaluación de Impactos de la protección de datos:** se trata de la identificación y valoración continuada de los diferentes riesgos para los derechos y libertades de los interesados que pueden acaecer en función de la actividad y del sector del negocio del responsable. Dentro de la fase de análisis, pueden diferenciarse los siguientes puntos:

-Análisis de los tratamientos realizados por la empresa: consiste en identificar las operaciones de tratamiento que realiza la entidad con los datos personales de sus clientes, empleados, profesionales o personas de contacto de otras empresas. Deberán definirse con claridad los fines del tratamiento, las categorías de interesados y de datos personales afectados, los posibles destinatarios (incluidas transferencias internacionales) y los plazos de supresión de datos previstos.

-Estimación de los riesgos que implica cada tratamiento (muy alto, alto, medio, bajo o muy bajo), que dependerá de la probabilidad de ocurrencia o materialización del riesgo (cierta posibilidad de que ocurra, poco probable que ocurra, no es posible que ocurra o es

sumamente improbable que ocurra) y de la gravedad del impacto para los interesados (máxima, considerable, moderada, insignificante o inexistente), en caso de producirse, que dependerá principalmente de la extensión geográfica del tratamiento, número de interesados, número de datos personales afectados y su periodo de conservación. Esta variable define el riesgo estimado para cada tratamiento.

-Cuando el tratamiento entrañe un alto riesgo, será obligatorio realizar, antes del tratamiento, una evaluación de impacto relativa a la protección de datos, si bien es siempre recomendable realizarla. Dicha evaluación deberá incluir: una descripción de las operaciones de tratamiento, su finalidad y su legitimación; una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; la evaluación de los riesgos para los derechos y libertades de los interesados; las medidas para afrontar los riesgos, incluidas las garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales. Con esta evaluación inicial, el dato que obtendremos será el riesgo máximo admisible de cada tratamiento.

-Consulta previa al organismo de control, en caso de que el riesgo estimado sea superior al riesgo máximo admisible, es decir, en caso de que, con carácter previo al inicio de la actividad de tratamiento, el nivel de seguridad previsto por la empresa en función de las medidas de seguridad de las que dispone sea inferior al nivel de riesgo estimado.

-Implementación de las seguridades oportunas, es decir, de las medidas técnicas y organizativas adecuadas para cada una de las operaciones de tratamiento detalladas según la concreta conducta o modo en que se realiza la operación dentro de la entidad, para lo que se requerirá la colaboración y actitud proactiva de todo el personal implicado.

-Calificación de las medidas: cada una de las medidas tiene asociada una o varias comprobaciones destinadas a supervisar el cumplimiento normativo. Cada responsable de actividad o de departamento (designado por el representante de la empresa) debe calificar dichas comprobaciones en función del grado de eficacia y cumplimiento de todas y cada una de las medidas para cada una de las conductas que se realizan en la empresa en relación con una determinada operación de tratamiento. Se determinan varios niveles de cumplimiento diferenciando los siguientes: muy buena, buena, aceptable, escasa o mínima.

-Periodicidad de las calificaciones: para poder realizar una evaluación global y continuada, se recomienda realizar una primera verificación inicial de cada una de las medidas asociadas a conductas que se desarrollan en el seno de la empresa, a la que seguirán otras verificaciones cuya realización se hará con la periodicidad que el representante de la empresa determine, siendo aconsejable que sea, como mínimo, trimestral.

-Evaluación y supervisión continua. Informe de nivel de seguridad: a consecuencia de tales calificaciones, se generan unos informes periódicos que muestran, en forma de gráfico, el nivel de seguridad de la empresa que, consecuentemente, dependerá del nivel de riesgo, de las medidas aplicadas y de la frecuencia de la supervisión o seguimiento. El nivel de seguridad podrá ser muy bueno, bueno, aceptable, escaso o mínimo.

De este modo, el responsable y, en su caso, el Delegado de Protección de datos, puede valorar, de forma plenamente eficaz, la existencia o no de la necesidad de implantar nuevas medidas de seguridad o preventivas, o bien de perfeccionar las existentes para aumentar su nivel de aceptación y realización por el personal encargado de las conductas a las que hagan referencia. El informe reflejará la mejora o empeoramiento progresivos de los controles de cumplimiento que se lleven a cabo en la empresa.

En caso de que el nivel de seguridad de la empresa en un momento determinado sea inferior al nivel de riesgo, habrá que abrir la correspondiente no conformidad y acción correctiva, a fin de poner solución cuanto antes a la incidencia o vulnerabilidad detectada, según el procedimiento que se detalla en el apartado correspondiente al Comité de quiebras de seguridad.

·**Protocolos de actuación:** consiste en la determinación de la actitud práctica, en la toma de decisiones y demás procedimientos dirigidos, por un lado, a tomar todas las precauciones oportunas para garantizar la licitud del tratamiento y el ejercicio de los derechos por el interesado; y, por otro lado, a la aplicación y cumplimiento efectivos de las seguridades desde el diseño oportunas a fin de minimizar o eliminar los riesgos para los interesados que se desprendan del tratamiento. Dichos protocolos vendrán referidos, principalmente, a las siguientes categorías:

-Precauciones a adoptar en el uso de soportes automatizados: se trata de una serie de cautelas que los empleados deben adoptar al manejar sus equipos informáticos o, en general, cualquier soporte automatizado al que tengan acceso a consecuencia de su actividad diaria.

-Precauciones a adoptar en el uso de soportes manuales: consiste en serie de cautelas que los empleados deben adoptar al manejar cualquier soporte manual al que tengan acceso en el cumplimiento de sus funciones habituales.

-Salidas de datos: llevanza por la persona designada por el responsable de un registro de las salidas de datos fuera de las instalaciones de la entidad, identificando su fecha, qué empleado la realiza, quién las ha autorizado y la fecha en la que regresan los datos a la empresa.

-Destrucción de datos: procedimiento de eliminación total de los soportes manuales o automatizados, una vez haya finalizado su plazo de vigencia y de prescripción, durante el que puedan derivarse responsabilidades para el responsable.

-Ejercicios de derechos por los interesados: implantación de un procedimiento ágil, sencillo y efectivo para que los interesados puedan retirar, en su caso, el consentimiento otorgado, obtener confirmación sobre si se están tratando sus datos o no y ejercer ante el responsable los derechos de acceso, rectificación, supresión, oposición, limitación, portabilidad y oposición a la toma de decisiones automatizadas, bien sea por vía telemática, por correo postal o por entrega física en las dependencias de **MARQUEZ JAIME, RAFAEL**. Dicho procedimiento ha de ser conocido y asumido por todos los empleados. El responsable del tratamiento designará, en cada caso, los responsables de dar respuesta a los distintos

derechos ejercidos, en el plazo de un mes desde la recepción de la solicitud y, extraordinariamente, en los tres meses siguientes, debiendo notificar dicha ampliación del plazo de respuesta en el primer mes desde la recepción de la solicitud.

-Formación de los trabajadores en materia de Protección de Datos: se trata de un curso *on-line*, gratuito, de 70 horas, que se abrirá automáticamente a todo el personal de la entidad, facilitándose usuario y contraseña de acceso al mismo.

-Contratos con encargados del tratamiento. El personal autorizado a firmar contratos de encargo con prestadores de servicios habrá de verificar, con carácter previo a su contratación, que el encargado ofrece las garantías suficientes para aplicar las medidas técnicas y organizativas de conformidad con la presente Política. Adicionalmente, habrá de asegurarse de que suscribe el pertinente contrato de encargado del tratamiento de conformidad con la Política de **MARQUEZ JAIME, RAFAEL** y la normativa aplicable en materia de protección de datos.

-Canal de denuncias internas: mecanismo de comunicación interna que permite el acceso del órgano responsable del cumplimiento de la Política a toda la información relativa a los posibles riesgos e incumplimientos detectados por los programas o el personal de la empresa.

·**Comité de DPD:** En función del sector de actividad, del riesgo del tratamiento o con carácter voluntario, la entidad podrá designar un Delegado de Protección de Datos, bien entre los empleados que reúnan los conocimientos y cualificación necesaria para desempeñar las funciones que le son propias, o bien externo, que, entre otras actividades, deberá atender las solicitudes o reclamaciones que presenten los interesados y actuará como punto de contacto con la autoridad de control. El Delegado rendirá cuentas directamente al más alto nivel jerárquico del responsable y no podrá ser destituido ni sancionado por el ejercicio de sus funciones, debiendo serle facilitados por el responsable y, en su caso, por el encargado, todos los recursos necesarios para el desempeño de sus funciones, contando también con todas las autorizaciones y permisos necesarios para ello.

·**Comité de quiebras de seguridad e investigación de las violaciones de seguridad.** El responsable podrá designar a un grupo de empleados a fin de crear un comité de investigación de quiebras de seguridad, que podrá estar presidido, en su caso, por el Delegado de Protección de Datos. La función de dicho comité será, siempre que se le notifique o sea conocedor de cualquier incidencia, abrir la correspondiente no conformidad, a fin de ponerle solución inmediata y proceder posteriormente a investigar la causa que ha originado dicha no conformidad, con el objetivo de abrir la acción correctiva destinada a solucionar definitivamente el problema, procediéndose a cerrar la acción correctiva, una vez se comprueba que la causa ha desaparecido definitivamente.

·**Auditoría interna o externa. MARQUEZ JAIME, RAFAEL** realizará, al menos, una vez al año, una auditoría, interna o externa, que evalúe el grado de implantación, cumplimiento y efectividad de las medidas adoptadas. Dicha auditoría habrá de realizarse por el Delegado de

Protección de Datos, en su caso, o bien por el personal designado a tal efecto y, en última instancia, por el responsable del tratamiento, o bien por el profesional o entidad designada a tal efecto.

·**Registros e informes de cumplimiento:** en último término, a los efectos de evidenciar el efectivo cumplimiento de la normativa, se mantendrá actualizado el registro de actividades de tratamiento de la entidad y se elaborarán periódicamente informes que acrediten y garanticen el cumplimiento de las obligaciones indicadas.

·**Encuestas a interesados.** A fin de comprobar el grado de satisfacción de los interesados con la Política de Protección de Datos de (LA ENTIDAD) se enviarán, con la periodicidad que estime oportuna el responsable, encuestas a los interesados, que vendrán referidas, entre otras cuestiones, a su experiencia en las comunicaciones con la empresa o el Delegado, al procedimiento de ejercicio de derechos o reclamaciones y a la posibilidad de retirar el consentimiento otorgado, a la forma de utilización de sus datos y a las medidas de seguridad que se aplican para protegerlos.

·**Sistema disciplinario:** determinación de las medidas dirigidas a sancionar el incumplimiento de los controles y procedimientos implantados por la Política para la prevención o reducción del riesgo para los interesados. A estos efectos, el representante de la empresa establecerá un sistema de faltas y sanciones en función de la gravedad del incumplimiento, pudiendo considerarse leve, grave o muy grave, que habrá de ser acorde al Estatuto de los Trabajadores y al Convenio aplicable.

III.-REVISIÓN, MODIFICACIÓN Y ACTUALIZACIÓN DE LA POLÍTICA.

Según se ha indicado, las actividades de la empresa, su estructura y las medidas de seguridad adoptadas se encuentran bajo supervisión constante, a fin de adaptarse adecuadamente a los cambios que se produzcan a causa de infracciones relevantes de la presente Política, por lo que resulta evidente que la misma no puede permanecer inalterada. Por ello, es importante que conozca la siguiente información:

Procedimiento de diseño de la Política: Esta Política se ha confeccionado teniendo en consideración la realidad y situación actual de **MARQUEZ JAIME, RAFAEL**, así como los valores y principios que rigen su actividad y estructura interna, a fin de adaptar por completo sus protocolos al Reglamento (UE) 2016/679, del Parlamento Europeo y el 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 éstos datos y por el que se deroga la Directiva 95/46/CE.

Procedimiento de control: MARQUEZ JAIME, RAFAEL ha verificado el análisis de riesgo oportuno por cada uno de los tratamientos que realiza en el seno de su actividad, tomando en consideración no sólo los propios de su sector, sino también las conductas

concretas que se realizan en el seno de la organización, por lo que se trata de una Política totalmente sectorizada y personalizada según las necesidades concretas de la entidad.

Una vez individualizada la Política, se realiza una labor de revisión periódica de la misma, con la finalidad de adaptarla a los cambios que se van efectuando a consecuencia de la evolución natural de la entidad, bien se trate de cambios estructurales dentro de su organización o de procedimientos de toma de decisiones, o bien de ampliaciones o reducciones de su ámbito negocial. Se trata, en consecuencia, de una Política en constante desarrollo.

La Política requiere, para su efectividad, que exista uno o varios sujetos encargados principalmente de vigilar su funcionamiento y observancia y que tome las medidas concretas necesarias con el fin de asegurar su adecuada actualización y ejecución, así como su patente validez ante terceros.

Dentro del régimen jurídico impuesto por el RGPD, la responsabilidad en materia de protección de datos recae directamente sobre el responsable del tratamiento, si bien podrá o estará obligado, según los casos, a ser asistido por un Delegado de Protección de Datos, que ha de contar con los todos los recursos y medios, humanos, técnicos o de cualquier índole, y autorizaciones o permisos de la alta dirección para llevar a cabo una labor de supervisión, control y ejecución de los diversos aspectos de esta Política. Es por ello que, en caso de estar presente, es a dicho Delegado a quien corresponde la evaluación constante de los diferentes escenarios de riesgo, así como llevar a cabo la oportuna información y comunicación con los sujetos a los que esta Política resulta aplicable.

Procedimiento de mejora continua: La Política es un instrumento dinámico, que se evalúa a través de la supervisión continua de los posibles escenarios de riesgo implicados en los tratamientos realizados por la empresa, permitiendo así la obtención constante de información acerca de su correcto funcionamiento y de la efectividad de los medidas técnicas y organizativas adoptadas.

Esta obtención continuada de información garantiza que la actualización de las medidas adoptadas por la entidad se realice de forma automática, en función de los cambios, tanto de carácter interno como externo, que se produzcan en su ámbito de actuación.

Corresponde al Delegado de Protección de Datos, en su caso, o a los empleados designados a tal efecto por el responsable y, en última instancia, al propio responsable del tratamiento, la implementación de esta Política en la estructura de la entidad, su seguimiento y control efectivos, la proposición de mejoras o modificaciones en caso de detectar nuevos escenarios de riesgo o nuevas operaciones de tratamiento, así como la inclusión de nuevas medidas técnicas u organizativas que se vayan adoptando en función del grado de cumplimiento de la presente Política.

El responsable indicado en el párrafo anterior debe promover la adecuada difusión de la Política en todas las áreas a las que resulte de aplicación, debiendo facilitar la oportuna formación respecto a los códigos éticos y de conducta que marcan el espíritu corporativo de la tolerancia cero contra los incumplimientos normativos.

Procedimiento disciplinario: En caso de vulneración de esta Política y, en consecuencia, de producirse un incumplimiento de la normativa aplicable en materia de protección de datos, es necesaria la correspondiente aplicación de un sistema disciplinario que prevea las sanciones adecuadas, en función de las medidas que se hayan infringido y de la gravedad de las posibles consecuencias que se generen o puedan generarse tanto para los interesados como para **MARQUEZ JAIME, RAFAEL**

El sistema disciplinario aplicable tiene carácter exclusivamente interno, de forma que su aplicación no impide la apertura de acciones penales, civiles o administrativas contra los responsables de las infracciones.

Por todo lo expuesto, **MARQUEZ JAIME, RAFAEL** se reserva el derecho a modificar su Política de Privacidad y Protección de Datos, bien de acuerdo a su propio criterio a la vista de los análisis de riesgos que se vayan realizando, o bien motivado por un cambio legislativo, jurisprudencial o doctrinal de la Agencia Española de Protección de Datos.

Cualquier modificación de la Política de Privacidad les será comunicada al menos ….. días antes de su efectiva aplicación, por la misma vía que la presente.

Sin otro particular, atentamente,

El responsable.