PRAGMA Solucions

Reglamento general de protección de datos (UE 2016/679)

Introducción

El nuevo Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016 y será **aplicable a partir del 25 de mayo de 2018**. En este periodo transitorio debemos ir preparando y adoptando las medidas necesarias para estar en condiciones de cumplir con las previsiones del RGPD en el momento en que sea de aplicación.

Dos elementos de carácter general constituyen la mayor innovación del RGPD y se proyectan sobre todas las obligaciones de las organizaciones:

1. El principio de responsabilidad proactiva; y
2. El enfoque de riesgo

¿Qué es el derecho de protección de datos?

La función del derecho a la protección de datos consiste en «***garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado***» (STC 292/2000 FJ 6).

Ejemplo: Multa de 300.000 € confirmada por el Tribunal Supremo, sentencia de fecha 25 de enero de 2006:

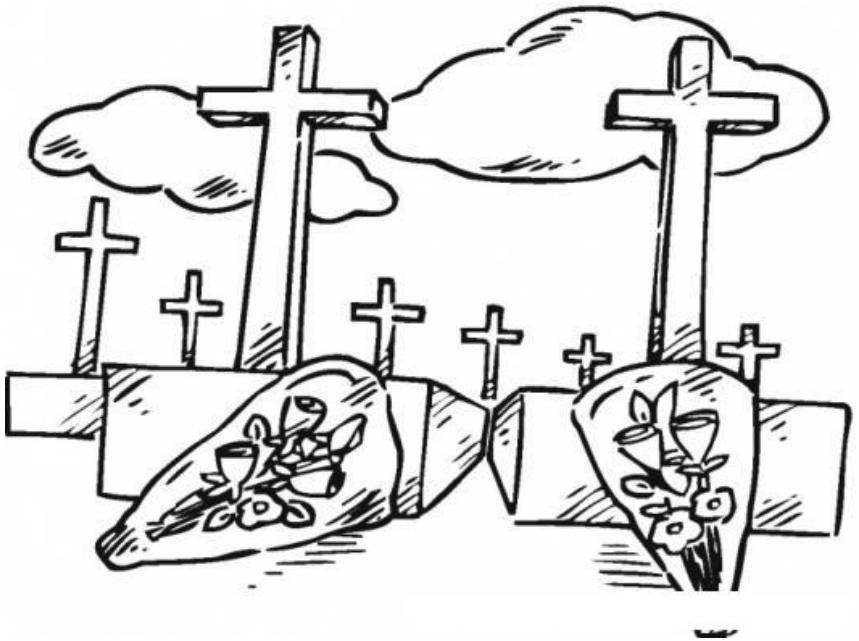
En el mes de marzo de 1999, D. . . . . ., Director del Gabinete del Vice consejero de Seguridad del Gobierno Vasco, recibe en su lugar de trabajo un envío publicitario remitido por el Hotel ….., invitándole a una fiesta. 2.- En el sobre de la invitación aparece el nombre, apellido, dirección profesional y las siglas "PNV". 3.- La entidad recurrente y propietaria del hotel que envió la invitación es la titular del fichero automatizado denominado "Mailing98.MDB" y "Mailing.MDB". 4.- En estos ficheros aparecen registrados los siguientes datos del denunciante ante la Agencia de Protección de Datos, D. . . . . ., nombre, apellidos, cargo, partido, institución y domicilio laboral. 5.- En la guía de comunicación del Gobierno Vasco constan los datos del citado denunciante referentes a su nombre, apellidos, cargo, dirección profesional y de correo electrónico y teléfono. 6.- El nombramiento del denunciante ante la Agencia de Protección de Datos como Director del Gabinete del Vice consejero de Seguridad, se produjo por Decreto 476/1991, de 30 de agosto, publicado en el Boletín Oficial del País Vasco de 6 de septiembre de 1991.

Excepción doméstica (*artículo 2.2.c) RGPD*)

El RGPD no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una **actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial**.

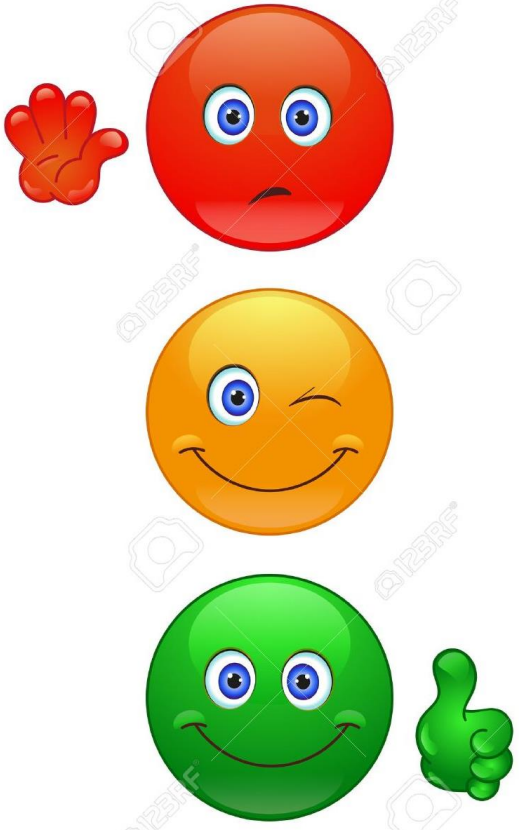
Si un usuario actúa en nombre de una empresa o de una asociación y utiliza una red social como una plataforma **con fines comerciales, políticos o sociales, la exención doméstica no se aplicaría**.

Persona física



El Considerando 27 del RGPD dispone que "*El presente Reglamento* ***no se aplica a*** *la protección de datos personales de* ***personas fallecidas****. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas*".

Persona física: ¿Hasta cuando se considera menor?



Los **menores de 13 años, en cualquier caso**, deberán contar con la **autorización de los padres o tutores legales**.

Entre los **13 y 16 años** dependerá de la legislación interna de cada uno de los Estados Miembros.

El RGPD prevé que el consentimiento será válido **a partir de los 16 años**,

PRAGMA Solucions

Datos personales

El artículo 4.1 del RGPD lo define como "***toda información sobre una persona física identificada o identificable*** *(«el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*;".

PRAGMA Solucions

Tratamiento

El artículo 4.2 del RGPD lo define como "***cualquier operación*** *o conjunto de operaciones* ***realizadas sobre datos personales*** *o conjuntos de datos personales, ya sea por procedimientos* ***automatizados o no****, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción*;".

Tercero

El artículo 4.10 del RGPD lo define como "***persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado***, *del responsable del tratamiento, del encargado del tratamiento* ***y de las personas autorizadas*** *para tratar los datos personales bajo la autoridad directa del responsable o del encargado*;".

PRAGMA Solucions

LOS DERECHOS QUE TIENES PARA PROTEGER TUS DATOS PERSONALES

EL 25 DE MAYO DE 2018 SE APLICA EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ES IMPORTANTE QUE CONOZCAS CUÁLES SON TUS DERECHOS

1 DERECHO A CONOCER

* PARA QUÉ UTILIZAN TUS DATOS
  - Quién los tiene
  - Para qué los tienen
  - A quién los pueden ceder
  - Quiénes son sus destinatarios
* EL PLAZO DE CONSERVACIÓN DE TUS DATOS o Hasta cuándo van a ser utilizados
* QUE PUEDES PRESENTAR UNA RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
* LA EXISTENCIA DE DECISIONES AUTOMATIZADAS, LA ELABORACIÓN DE PERFILES Y SUS CONSECUENCIAS

2 DERECHO A SOLICITAR AL RESPONSABLE

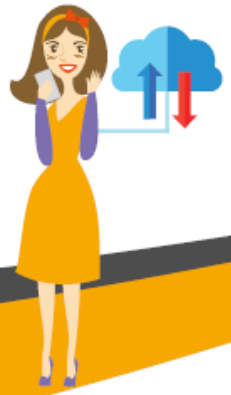
* LA SUSPENSIÓN DEL TRATAMIENTO DE TUS DATOS
  - Si impugnamos la exactitud de los datos, mientras se verifica dicha exactitud por parte del responsable
  - Si hemos ejercitado nuestro derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre tus derechos
* LA CONSERVACIÓN DE TUS DATOS
  - Si el tratamiento es ilícito y nos oponemos a la supresión de los datos solicitando la limitación de su uso
  - Si los datos se necesitan para la formulación, ejercicio o defensa de reclamaciones
* LA PORTABILIDAD DE TUS DATOS A OTROS PROVEEDORES DE SERVICIOS
  - En un formato estructurado, de uso común y lectura mecánica, siempre que sea técnicamente posible para su portabilidad y cuando los hayan utilizado/tratado con tu consentimiento o por existir un contrato

3 DERECHO A RECTIFICAR TUS DATOS

* CUANDO SEAN INEXACTOS
* CUANDO ESTÉN INCOMPLETOS

4 DERECHO A SUPRIMIR TUS DATOS

* POR TRATAMIENTO ILÍCITO DE DATOS
* POR LA DESAPARICIÓN DE LA FINALIDAD QUE MOTIVÓ EL TRATAMIENTO O RECOGIDA
* CUANDO REVOCAS TU CONSENTIMIENTO
* CUANDO TE OPONES A QUE SE TRATEN



5 DERECHO DE OPOSICIÓN AL TRATAMIENTO DE TUS DATOS

* POR MOTIVOS PERSONALES SALVO QUE QUIEN TRATA TUS DATOS ACREDITE UN INTERÉS LEGÍTIMO
* CUANDO EL TRATAMIENTO TENGA POR OBJETO EL MARKETING DIRECTO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es

PRAGMA Solucions

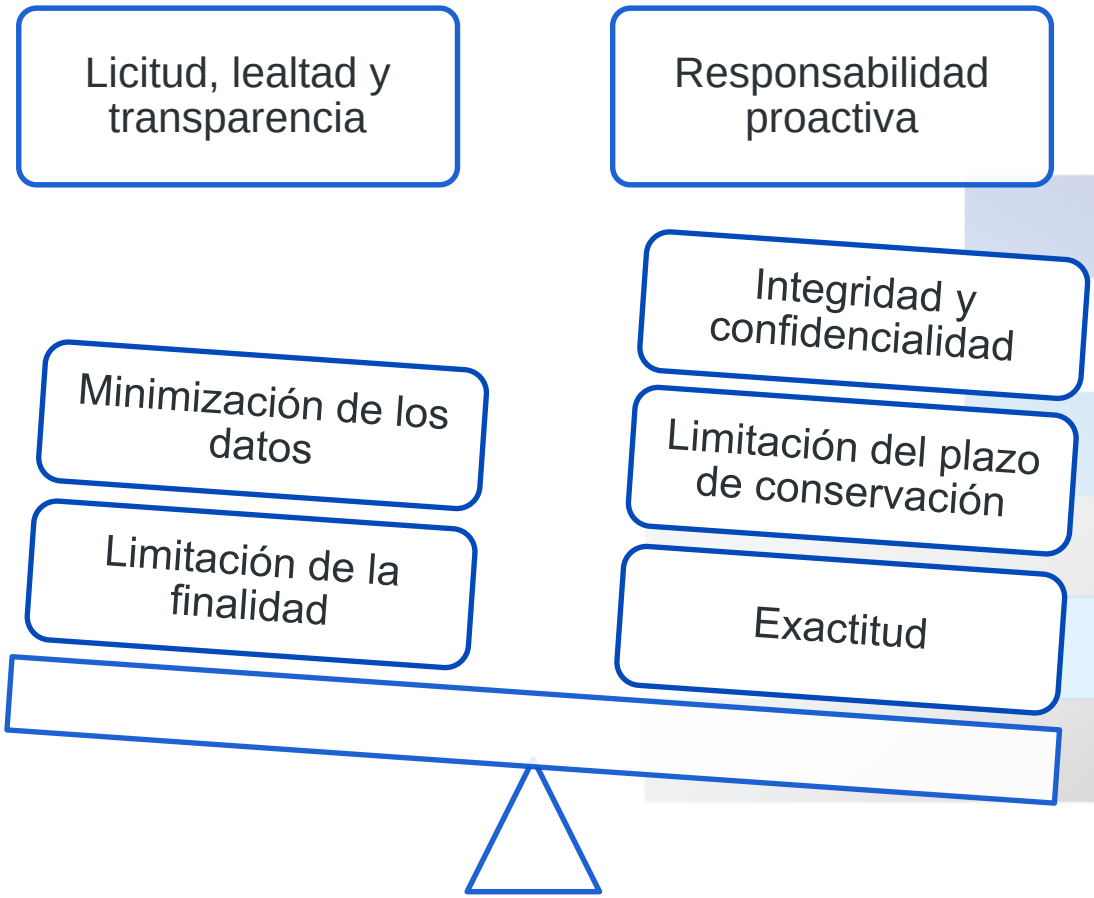
Derechos de las personas

- Procedimiento para el ejercicio
- Derechos tradicionales: ARCO
- Olvido
- Portabilidad
- Limitación tratamiento
- No decisiones automatizadas

PRAGMA Solucions

Objetivos del nuevo Reglamento LOPD de la UE

Principios de la protección de datos



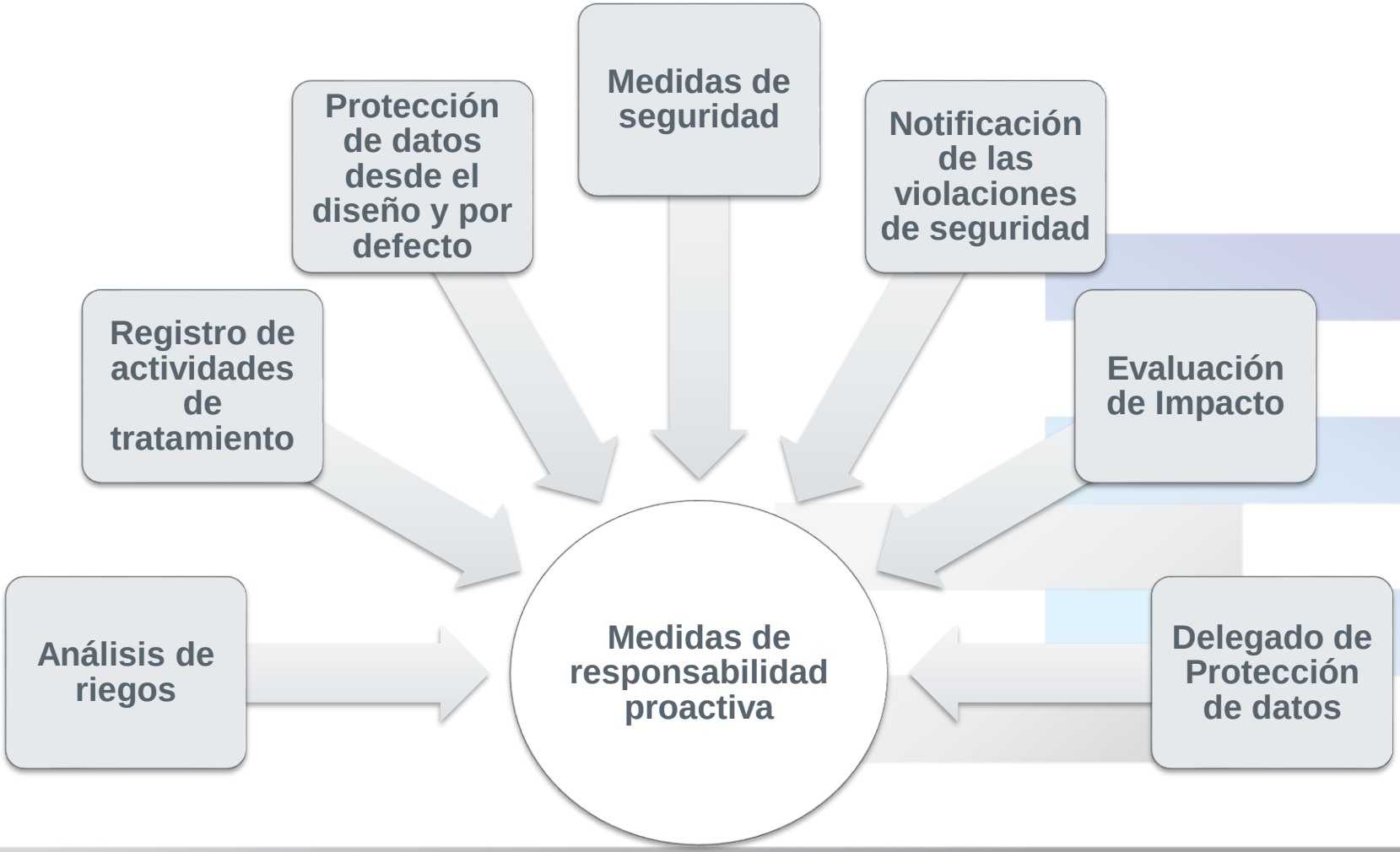
¿Qué implica la responsabilidad proactiva recogida en el RGPD?

Uno de los aspectos esenciales del **RGPD** es la **prevención** en el tratamiento de datos. Es lo que se conoce como responsabilidad activa; ya que **actuar sólo cuando ya se ha producido una infracción es insuficiente** como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

Las empresas **deben adoptar medidas que aseguren razonablemente el cumplimiento de los principios, derechos y garantías que el RGPD establece**.

PRAGMA Solucions

Medidas de responsabilidad proactiva



Violación de la seguridad de los datos personales

El artículo 4.12 del RGPD la define como "*toda violación de la seguridad que ocasione la* ***destrucción, pérdida o alteración accidental o ilícita*** *de datos personales* ***transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados*** *a dichos datos;*".

Disponemos de **72 horas para notificar** la violación de seguridad a la Agencia de Protección de Datos. **Si no lo hacemos** nos enfrentamos a una **multa de hasta 10.000.000 €**.

¿Qué implica el enfoque de riesgo del RGPD?

El RGPD **condiciona la adopción de las medidas de responsabilidad activa al riesgo** que los tratamientos puedan suponer para los derechos y libertades de los interesados.

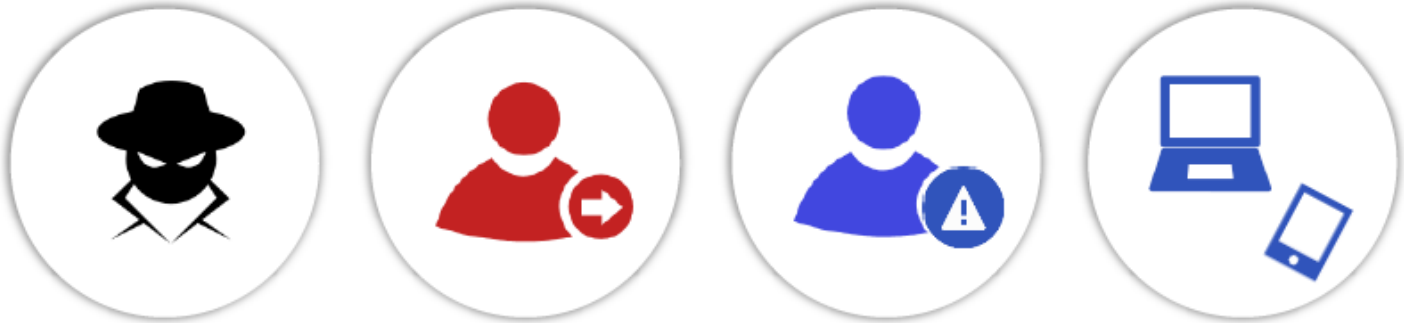
Se maneja el riesgo de dos maneras:

1. En algunos casos, prevé que determinadas medidas solo deberán aplicarse cuando el tratamiento suponga un alto riesgo para los derechos y libertados.
2. En otros casos, las medidas deberán modularse en función del nivel y tipo de riesgo que el tratamiento conlleve.

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo.

PRAGMA Solucions

Riesgos potenciales

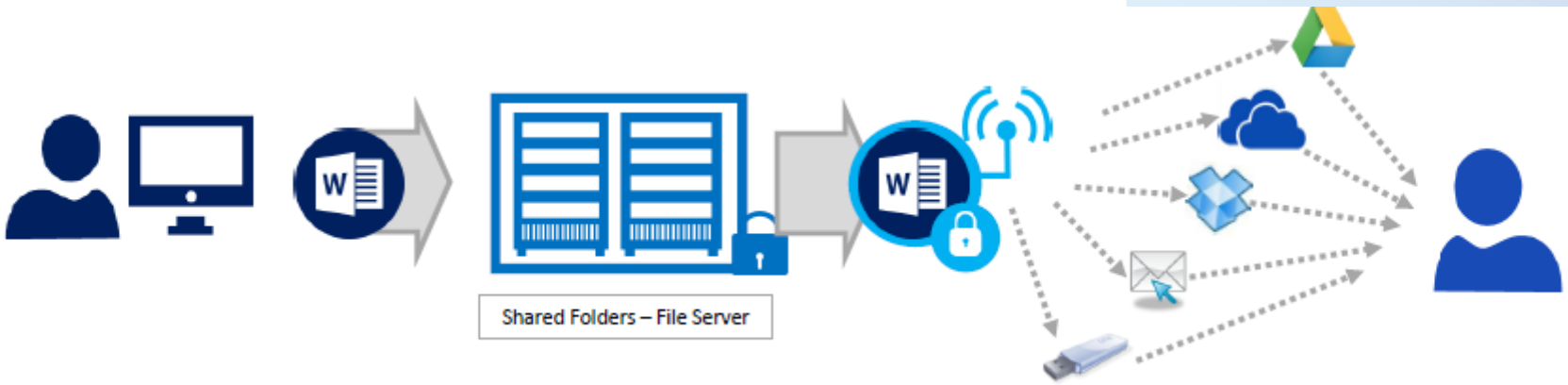


Ataques Malware

Ex-empleados

Negligencias y descuidos

Pérdidas o robos de dispositivos



Medidas de seguridad

La protección de la información se articula se articula en torno del respecte de tres principios básicos:

1. La **confidencialidad** implica que la información sea accesible únicamente por el personal autorizado.
2. La **integridad** de la información implica que la información sea correcta y esté libre de modificaciones y errores. Hay que tener presente que la información puede ser alterada intencionadamente o ser incorrecta, lo que supone un riesgo si basamos nuestras decisiones en ella; y
3. La **disponibilidad** de la información, accesible para las personas o sistemas autorizados cuando sea necesario.

El **esquema de medidas de seguridad previsto en el Reglamento** de Desarrollo de la LOPD **no seguirá siendo válido de forma automática** a partir del 25 de mayo de 2018.

Planteamiento del RGPD sobre confidencialidad

Considerando 39

"*… Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para* ***impedir el acceso o uso no autorizados*** *de dichos datos y del equipo utilizado en el tratamiento*."

Considerando 74

"*Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta... Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el* ***riesgo para los derechos y libertades*** *de las personas físicas*"

Planteamiento del RGPD sobre confidencialidad

Considerando 75

"*Los **riesgos para los derechos y libertades** de las personas físicas, de gravedad y probabilidad variables, **pueden deberse al tratamiento de datos que pudieran provocar** daños y perjuicios físicos, materiales o inmateriales, **en particular en los casos en los que** el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, **pérdida de confidencialidad de datos sujetos al secreto profesional**…*"

Planteamiento del RGPD sobre confidencialidad

Considerando 83

"*A fin de mantener la seguridad y* ***evitar que el tratamiento infrinja*** *lo dispuesto en el presente Reglamento,* ***el responsable o el encargado deben*** *evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben* ***garantizar un nivel de seguridad adecuado, incluida la confidencialidad****, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse….*"

PRAGMA Solucions

Delegado de Protección de Datos

El RGPD establece la figura del Delegado de Protección de Datos (DPD), que será obligatorio en:

- Autoridades y organismos públicos
- Responsables o encargados que tengan entre sus actividades principales las operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
- Responsables o encargados que tengan entre sus actividades principales el tratamiento a gran escala de datos sensibles.

El artículo 35 APLOPD incorpora una lista, no cerrada, de quienes se consideran incluidos en los supuestos anteriores (artículo 37.1 del RGPD).

PRAGMA Solucions

Delegado de Protección de Datos

Los conocimientos jurídicos en la materia son sin duda necesarios, pero también **es necesario contar con conocimientos ajenos a lo estrictamente jurídico**, como por ejemplo en materia de tecnología aplicada al tratamiento de datos o en relación con el ámbito de actividad de la organización en la que el DPD desempeña su tarea.

La designación del DPD y **sus datos de contacto deben hacerse públicos** por los responsables y encargados y deberán ser comunicados a las autoridades de supervisión competentes.

Se permite que el DPD mantenga con responsables o encargados una relación laboral o mediante un contrato de servicios. Es decir, permite que pueda contratarse el servicio de DPD con personas físicas o jurídicas ajenas a la organización.

PRAGMA Solucions

Delegado de Protección de Datos

La posición del DPD en las organizaciones tiene que cumplir los requisitos establecidos, entre los que se encuentran:

- total autonomía en el ejercicio de sus funciones
- necesidad de que se relacione con el nivel superior de la dirección
- obligación de que el responsable o el encargado faciliten al DPD todos los recursos necesarios para desarrollar su actividad

La AEPD ha optado por promover un **sistema de certificación de profesionales** de protección de datos como herramienta útil a la hora de evaluar que los candidatos a ocupar el puesto de DPD reúnen las cualificaciones profesionales y los conocimientos requeridos.

¿Qué debo hacer?

Verificación

- Situación actual frente a las nuevas obligaciones del RGPD

Evaluación riesgo

- Análisis del riesgo existente para los derechos de las personas

Implantación medidas

- Definición, priorización e implantación de medidas preventivas

Mejora continua

- Ir adoptando nuevas medidas, en función de la técnica y su coste, para minimizar el riesgo

PRAGMA Solucions

Hoja de ruta

PRAGMA Solucions

Decálogo de la protección de datos

Decálogo

- Trata los datos de las personas como quisieras que trataran los tuyos
- ¿Estás seguro de que tienes que acceder a esos datos? Piénsalo, sólo debes acceder si es necesario para los fines de tu trabajo
- Tus accesos quedan registrados en el sistema. Se sabe quién y cuando ha accedido, y los accesos se auditan con posterioridad
- Evita informar a terceros sobre los datos de cualquier persona, salvo que tengas una justificación lícita
- Cuando abandones tu puesto de trabajo, asegúrate de cerrar la sesión abierta de tu ordenador. No facilites a nadie tu clave y contraseña

PRAGMA Solucions

Decálogo de la protección de datos

Decálogo

- No tires documentos con datos personales a la papelera; destrúyelos tu mismo
- No envíes información con datos personales por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si fuera imprescindible, no olvides cifrar los datos
- Al finalizar la jornada, cierra con llave los armarios o archivadores que contengan datos personales
- No dejes documentación, con datos personales, a la vista sin supervisión
- No crees por tu propia cuenta ficheros con datos personales: consulta siempre antes

PRAGMA Solucions

"If you think compliance is expensive, try non-compliance"

Paul McNulty, Former US Deputy Attorney General (2009)

Gràcies per la vostra atenció

Avgda. Meridiana nº 350, 4t D
08027 Barcelona
931 128 127
www.pragma-solucions.com
jharo@pragma-solucions.com