AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS 2016/679.

18 de Mayo de 2018

ProtechPlus
seguridad de la información

1

CONTENIDO DE LA JORNADA

1- Nuevo Reglamento Europeo 2016/679. Un nuevo marco legal
2- La protección de datos desde el diseño y por defecto.
3- Registro de actividades de Tratamiento.
4- Bases Jurídicas de Legitimación del Tratamiento.
5 -El deber de Informar
6- Relación Responsable del Tratamiento Encargado del Tratamiento
7- Código de Conducta Certificación
8- Evaluaciones de Impacto en Protección de Datos.
9- Análisis de Riesgos
10 - Auditoría

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

1 – Nuevo Reglamento Europeo de Protección de Datos UE 2016/679

Un Nuevo Marco Legal

El nuevo Reglamento General de Protección de Datos (RGPD) entró en vigor en mayo de 2016 y será aplicable a partir del día 25 de mayo de 2018.

El RGPD es una norma directamente aplicable, que no requiere de normas internas de transposición, por eso lo Responsables deben asumir que la norma de referencia es RGPD, no obstante la Ley que sustituirá a la actual LOPD, que en esto momentos se encuentra en sus fases finales de tramitación, podrá incluir algunas precisiones o desarrollos en las áreas que RGPD lo permite y siempre y cuando no vaya en contra de lo establecido en el mismo.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

3

ProtechPlus
seguridad de la información

2 –La Protección de Datos desde el diseño y por defecto.

El nuevo Reglamento General de Protección de Datos (RGPD) describe este principio como la necesidad de que el Responsable del Tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el Tratamiento es conforme con el Reglamento.

ACTITUD CONSCIENTE DILIGENTE Y PROACTIVA

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

4

ProtechPlus
seguridad de la información

2.1 –La Protección de Datos desde el diseño y por defecto.

En términos prácticos este principio requiere que las organizaciones analicen que datos tratan, con que finalidades lo hacen y que tipo de operaciones de tratamiento llevan acabo.

A partir de este conocimiento deben determinar de forma explicita las forma en que se aplican las medidas que el RGPD prevé, asegurándose que esas medidas son las adecuadas para cumplir con el mismo y que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

ADAPTACIÓN DESDE EL DISEÑO
Responsabilidad Activa

SISTEMA DE GESTIÓN SEGURIDAD INFORMACIÓN

ESPIRAL DE MEJORA

- PLANIFICAR
- HACER
- AUDITAR
- ACTUAR

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

6

ProtechPlus
seguridad de la información


PLANIFICAR
TRIPLE VISIÓN
MEDIDAS TÉCNICAS
ENTORNO JURÍDICO
ORGANIZATIVAS O PROCESOS DE GESTIÓN
AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES
ProtechPlus
seguridad de la información
7

2.3 El Enfoque del Riesgo

El RGPD señala que las medidas dirigidas a garantizar su cumplimiento 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.

De acuerdo con este enfoque, algunas de aquellas medidas que el RGPD establece se aplicarán solo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y del tipo de riesgo que los tratamientos presenten.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

8

2 El Enfoque del Riesgo

La aplicación de las medidas por tanto deberán adaptarse, por tanto, a las características de las organizaciones.

Lo que puede ser adecuado para una organización que maneja datos de millones de interesados, en tratamientos complejos, no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamiento de datos no sensibles.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

3- Registro de Actividades de Tratamiento. Articulo 30

Cada responsable y en su caso su representante llevaran un registro de las actividades de tratamiento efectuadas bajo su responsabilidad.

Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y datos de contacto del responsable y, en su caso del corresponsable del representante del responsable, y del delegado de protección de datos;

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

3- Registro de Actividades de Tratamiento. Articulo 30

b) los fines del tratamiento

c) una descripción de las categorías de los interesados y de las categorías de los datos personales

d) Las categorías de destinatarios a quienes se comunicaran los datos,.

3- Registro de Actividades de Tratamiento. Articulo 30

e) Transferencias de datos internacionales , con las excepciones establecidas en el articulo 49, consentimiento explicito del interesado, ejecución de un contrato entre las partes.

f) Plazos previstos de supresión de las diferentes categorías de datos.

g)Descripción general medidas técnicas y organizativas.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

3- Licitud del Tratamiento.

El Tratamiento solo será licito si cumple, al menos una de las siguientes condiciones.

a) El interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

Este consentimiento debe ser inequívoco

b) El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

BASES JURÍDICAS PARA EL TRATAMIENTO (continuación)

c) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

d) El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
Seguridad de la información

BASES JURÍDICAS PARA EL TRATAMIENTO (continuación)

e) El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea menor

5- El deber de informar

Transparencia e información a los interesados

La información a los interesados , tanto respecto a las actividades de tratamiento que les afecten como a las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso y con un lenguaje claro y sencillo.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

5- El deber de informar

Actualmente la LOPD establece las siguientes obligaciones respecto a la información

- La existencia de fichero o tratamiento, su finalidad y destinatarios.
- El Ejercicio de derechos de acceso, rectificación, cancelación y oposición.
- La identidad y los datos del responsable del Tratamiento.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

5- El deber de informar

El RGPD añade requisitos adicionales:

- Los datos de contacto del Delgado de Protección de datos, en su caso .
- La base jurídica o legitimación para el tratamiento.
- Los plazos de conservación de los datos
- La existencias de decisiones automatizadas
- La elaboración de perfiles.
- La previsión de transferencias a terceros países.
- El derecho a reclamar ante la autoridad de control.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

5- El deber de informar

Ejercicio de derechos
A los ya existentes de

Acceso.
Rectificación .
Cancelación .
Oposición .
Rectificación

Se incorpora el derecho al olvido
Y el derecho a la portabilidad de los datos

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

5- El deber de informar

Información por capas

Información Básica
En el mismo momento o medio en el que se en el que se recojan los datos.

Información adicional
En el segundo nivel donde se presentara de forma detallada el resto de información.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

6 – Relación Responsable – Encargado del Tratamiento

EL RESPONSABLE DEL TRATAMIENTO ACTUARÁ CON DILIGENCIA EN LA ELECCIÓN DEL ENCARGADO DEL TRATAMIENTO.

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado del tratamiento que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados , de manera que el tratamiento se a conforme con los requisitos del RGPD.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
Seguridad de la Información

6 – Relación Responsable – Encargado del Tratamiento

El Encargado del Tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, especifica o general del responsable .

En este ultimo caso el encargado informará al responsable en la incorporación o sustitución de otros encargados (subcontrataciones del servicio)

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

6 – Relación Responsable – Encargado del Tratamiento

El Tratamiento por el encargado se regirá por un contrato u otro acto jurídico

Dicho contrato estipulará que :

1. Tratará los datos siguiendo las instrucciones documentadas del responsable , inclusive con respecto a las transferencias a terceros países .

2. Garantizará que las personas autorizadas para tratar los datos se hayan comprometidos a respetar la confidencialidad .

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

6 – Relación Responsable – Encargado del Tratamiento

3- Tomara las medidas necesarias en el Tratamiento de los datos tal y como establece el articulo 32 de RGPD.

4- A elección del responsable, suprimirá o devolverá todos los datos personales una vez que finalice la prestación del servicio , conservará copia si requiere la conservación en virtud del Derecho de la Unión Europea o de los estados miembros.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

6 – Relación Responsable – Encargado del Tratamiento

Articulo 28

Cuando se vaya a realizar el tratamiento por cuenta de un responsable , este elegirá únicamente a un encargado que ofrezca garantías suficientes para aplicar las medidas de acuerdo al cumplimiento del RGPD.

Licitación de los Encargados del Tratamiento.

Autorización previa y por escrito de las subcontrataciones

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

6 – Relación Responsable – Encargado del Tratamiento

Adhesión del encargado a un código de conducta a tenor del articulo 40 a un mecanismo de certificación a tenor del 42.

6 – Relación Responsable – Encargado del Tratamiento

Código de Conducta :
Los Franquiciadores y otros organismos representativos de categorías de responsables o encargados de tratamiento podrán elaborar códigos de conducta con objeto de especificar la aplicación de RGPD.
Asumiendo compromisos vinculantes e inherentes al código.

Supervisión de códigos de conducta , podrá ser realizado por organismo acreditado para ese fin por la autoridad de control.

.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

7 – El inventario de Tratamiento a Terceros

Cada Encargado y en su caso , el representante del encargado, llevara un registro de todas las categorías de actividades de tratamiento efectuadas por cuentas de un responsable.

Deberá contener:
Nombre y datos del contacto del responsable.
Las categorías del tratamiento efectuadas por el responsable.
Descripción general de medidas técnicas o actividad de tratamiento registrada por le encargado para tal fin.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

8– Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Una PIA o una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) es, en esencia, un ejercicio de análisis de los riesgos que una actividad de Tratamiento determinada, sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

29

8– Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Una PIA o una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) es, en esencia, un ejercicio de análisis de los riesgos que una actividad de Tratamiento determinada, sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados.

8 – Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Que debe incluir:

- Una descripción sistemática de la Actividad de Tratamiento.
- Una Evaluación de la Necesidad y proporcionalidad del tratamiento respecto a la necesidad.
- Una Evaluación de riesgos
- Las medidas Previstas para afrontar los riesgos , técnicas , organizativas y de garantía jurídica.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

8 – Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

La evaluación de impacto se realizara cuando exista un alto riesgo para los derechos y libertades de las personas físicas.

Recabará el asesoramiento de la figura del delegado de protección de datos si ha sido nombrado .
Se requerirá si existe una

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas.
- Sobre cuyas base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecte de significativamente de forma similar

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

8 – Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

- Una Evaluación de la Necesidad y proporcionalidad del tratamiento respecto a la necesidad.

- Legitimación
- Justificación

Unidos a la finalidad ?
Minimizados?
Tecnologías Adecuadas?
Principio de limitación del plazo de conservación.

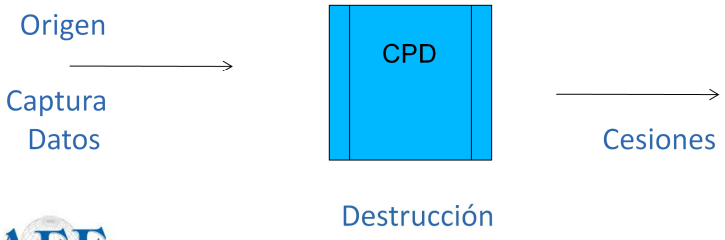
AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

8– Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Contexto .

-Describir el ciclo de vida de los datos.
Descripción detallada del ciclo de vida y del flujo de datos en el tratamiento.



8– Evaluación de Impacto en Protección de Datos DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

RACI

FASE	RESPONSABLE DEL TRATAMIENTO	DELEGADO PROTECCIÓN DATOS	ENCARGADO DEL TRATAMIENTO	PROTECHPLUS ASESORÍA GDPR
Descripción de ciclo de vida del tratamiento de datos.				
Necesidad y Proporcionalidad del tratamiento.				
Identificación de Amenazas				
Evaluación de Riesgos				
Tratamiento de los Riesgos				
Plan de Acción y Conclusiones.				

9 – Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Analisis de Riesgos

- **Identificación - Evaluación – Tratamiento**
- **Análisis Cualitativo y Cuantitativo**

Monitorización Continua → **Identificar los Riesgos**

Tratar los riesgos

AEF ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus seguridad de la información

36

9 – Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Analisis de Riesgos

Amenaza	Riesgo	impacto
Salida no Autorizada de datos	Vulneración de derechos	Daño moral físico material

9 – Evaluación de Impacto en Protección de Datos DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Análisis de Riesgos

Análisis cuantitativo

Maxima 4	**4**	**8**	**12**	**16**
Significativa 3	3	6	9	12
Limitada 2	2	4	6	8
Despreciable 1	1	2	3	4

PROBABILIDAD X IMPACTO

AEF ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus seguridad de la información

9 – Evaluación de Impacto en Protección de Datos
DENOMINADO EIPD Y PIAs (Privacy Impact Assesment)

Análisis de Riesgos

Establecimiento de medidas para la atenuación del nivel de riesgo
Hasta eliminarlo o convertirlo en residual asumible

Puntuando las medidas hasta convertir el riesgo en Despreciable 1

Ver catálogos de amenazas y posibles soluciones

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

El Delegado de Protección de Datos DPD

a)Cuando el tratamiento lo lleva a cabo una autoridad u organismo público.

b) Cuando las actividades principales del responsable o el encargado del tratamiento consisten en operaciones de tratamiento que requieren el seguimiento regular y sistemático de los interesados a gran escala.

c) Cuando las actividades principales del responsable o el encargado del tratamiento consisten en el tratamiento a gran escala de categorías especiales de datos o datos personales relacionados con condenas y delitos penales.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

El Delegado de Protección de Datos DPD

a)Cuando el tratamiento lo lleva a cabo una autoridad u organismo público.

b) Cuando las actividades principales del responsable o el encargado del tratamiento consisten en operaciones de tratamiento que requieren el seguimiento regular y sistemático de los interesados a gran escala.

c) Cuando las actividades principales del responsable o el encargado del tratamiento consisten en el tratamiento a gran escala de categorías especiales de datos o datos personales relacionados con condenas y delitos penales.

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

41

El Delegado en Protección de Datos DPD

Como parte de estas funciones de control del cumplimiento, los DPD pueden, en particular:

- Recabar información para determinar las actividades de tratamiento,
- Analizar y comprobar la conformidad de las actividades de tratamiento,
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.

El control del cumplimiento no significa que el DPD sea responsable personalmente en caso de algún incumplimiento.

AEF ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus seguridad de la información

42

La NGPD declara taxativamente que es el responsable del tratamiento, no el DPD, quien está obligado a «implementar las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento se lleva a cabo con arreglo al presente Reglamento

10 La Auditoría

Auditar las medidas implantadas en las Actividades de Tratamiento

Medidas Adecuadas

Establecimiento de medidas correctoras

Plan de mejora y seguimiento

Certificado de cumplimiento ante terceros

AEF
ASOCIACION ESPAÑOLA DE FRANQUICIADORES

ProtechPlus
seguridad de la información

44

Información y datos de contacto

Shocktech y Protechplus SLU.

Sede Social

C/ Lisboa 3 28008 Madrid

José Caballero Carmona

Director Técnico y CEO

josecaballero@Protechplus.es