

**INFORME DE CUMPLIMIENTO DEL REGLAMENTO (UE) 2016/679 GENERAL DE PROTECCIÓN
DE DATOS POR PARTE DE**

Asociación Española de Movilidad Laboral Internacional



La Asociación Española de Movilidad Laboral Internacional -FEEX- (a la que en adelante en el presente documento nos referiremos como FEEX) se ha sometido durante el mes de octubre del año 2018 a un proceso de adaptación al Reglamento (UE) 2016/679, de 27 de abril General de Protección de Datos (RGPD o GDPR) anterior al 25 de mayo de 2018 a fin de revisar, actualizar e implantar las obligaciones que FEEX debe cumplir en el tratamiento de los datos personales.

I.- ANTECEDENTES

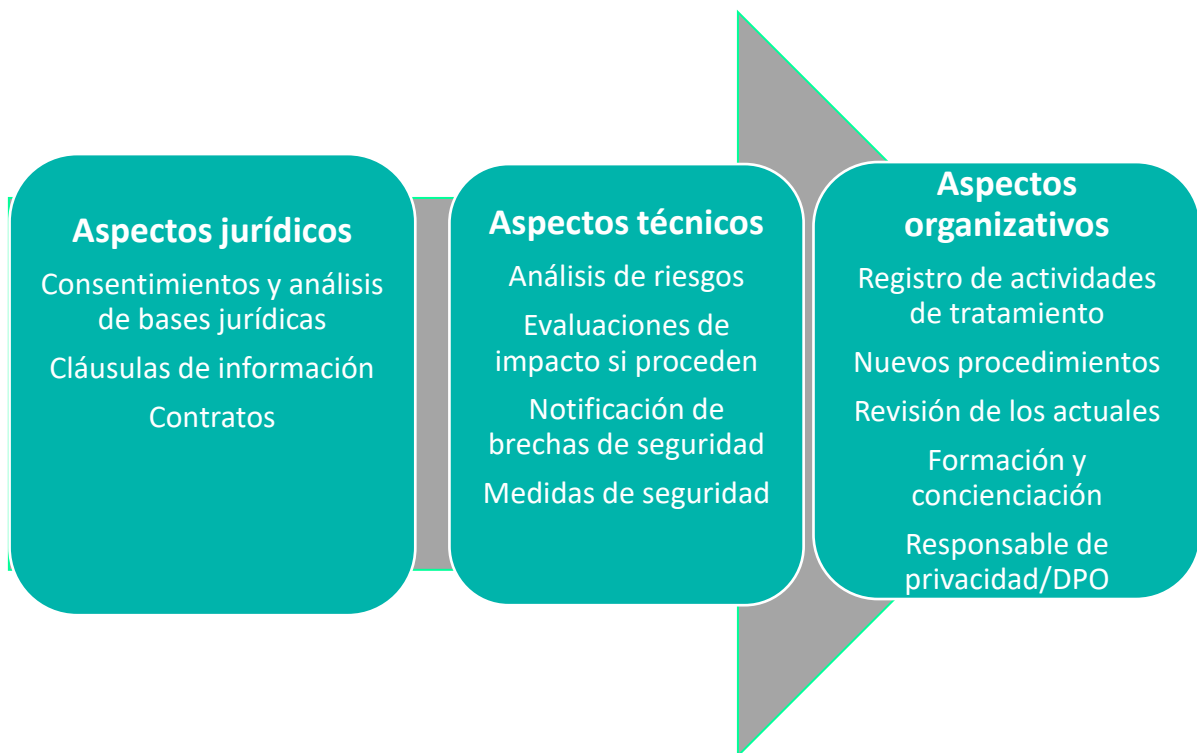
El RGPD recoge obligaciones para los responsables de tratamiento.

La fecha de entrada en vigor del RGPD se ha producido el día 25 de mayo de 2018 y ello implica el cumplimiento obligatorio del mismo en toda su extensión.

Algunos puntos del RGPD se remiten a la adopción de medidas internas por parte de los estados miembros en algunos aspectos (procedimiento sancionador, minoría de edad mínima para tratamiento de datos, etc).

Estos puntos se recogerán en una nueva Ley Orgánica de Protección de Datos que se publicará en un breve plazo.

Dicho lo anterior, reflejamos en el siguiente cuadro el conjunto de aspectos concretos de cumplimiento que todo responsable de tratamiento y por ende FEEX tiene que cumplir realizando a continuación un resumen de lo realizado hasta la fecha y su estado actual.



II.- Resumen ejecutivo de acciones de cumplimiento RGPD

Se ha acometido un plan de acción de que puede resumirse en el cumplimiento de las obligaciones recogidas en el RGPD.

FEEX previamente a la entrada en vigor del RGPD ha venido observando el cumplimiento de la LOPD por lo que el proceso actual ha sido y es de adaptación a la nueva normativa sobre la base previa anterior de cumplimiento.

A continuación se resumen las obligaciones específicas concretas que cualquier responsable de tratamiento y en particular FEEX, en todas sus actividades. Se referencia en cada obligación las acciones concretas que dentro del plan de acción se han realizado:

1.- Revisión y actualización de las cláusulas de información

Se ha realizado una adaptación de todas las cláusulas de información con respecto a todos los tratamientos identificados.

Esta tarea supone:

- Revisión y actualización de la web
- Revisión y actualización de documentos y contratos
- Revisión y actualización de cláusulas de información relacionadas con el tratamiento de los datos personales de los empleados y de la gestión de los Recursos Humanos incluyendo la gestión de la selección de personal y los Currícula vitae.

2.- Identificación de las bases jurídicas de los tratamientos

La determinación de la base jurídica de los tratamientos viene identificada por el propio tratamiento recogiendo estos extremos en el ya confeccionado “registro de actividades de tratamiento” al que nos referimos más adelante.

3.- Actualización de los contratos con terceros que tengan acceso a datos personales

Se han documentado las relaciones con terceros relaciones en cuanto supongan un acceso a los datos de terceros para la prestación de un servicio (gestoría, auditoría, página web, informática...)

No obstante, el recientemente publicado *Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos establece en su Disposición transitoria segunda lo siguiente en cuanto a “Contratos de encargo del tratamiento”:*

Los contratos de encargo del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679.

Lo anterior sólo es aplicable si existía un contrato de encargo de tratamiento anterior. En el caso de FEEX se han confeccionado contratos nuevos para regular todas las relaciones con terceros existentes.

4.- Confección de un registro de actividades de tratamiento

Se ha realizado un registro de actividades de tratamiento atendiendo a la estructura y tratamiento de datos actuales. Dicho registro será completado de forma paulatina teniendo en cuenta que el registro de actividades es un documento vivo que debe reflejar la realidad de la entidad y del tratamiento de sus datos.

5.- Adopción de medidas de seguridad

FEEX adopta unas medidas mínimas de seguridad debido a su sencilla estructura.

Como resumen debe tenerse presente que al menos deben adoptarse medidas de:

- Control de acceso físico y lógico (a ordenadores y sistemas)
- Identificación y autenticación (contraseñas en los ordenadores)
- Copias de seguridad
- Seguridad en las comunicaciones (correo seguro, certificado de seguridad web)
- Gestión de soportes (si se utilizan pen drives o discos duros externos deben cifrarse y custodiarse para evitar accesos indebidos)
- Gestión del papel: acceso restringido, custodia segura y destrucción confidencial.

Como punto de partida dicho cumplimiento y su revisión periódica puede ser suficiente sin perjuicio de los necesarios procedimientos de cifrado y pseudoanonimización siguiendo el texto del propio RGPD.

6.- Creación de procedimiento para la satisfacción de nuevos derechos (limitación y portabilidad) además de revisión de los actuales para comprobar su eficacia en los tiempos legalmente previstos

Puesto que hasta la fecha ya era obligatoria la satisfacción de los llamados derechos ARCO (acceso, rectificación, cancelación y oposición), no sólo se mantienen y se han actualizado dichos procedimientos sino que se han creado los nuevos de portabilidad y de limitación en los plazos exigidos atendiendo a las circunstancias de cada uno.

No se tiene constancia de que se hayan solicitado dichos derechos hasta la fecha.

7.- Creación de un procedimiento para la detección, gestión y notificación de las brechas de seguridad

Se ha confeccionado un procedimiento específico para la notificación de brechas de seguridad ya que el procedimiento de gestión de incidencias obligatorio bajo la anterior normativa seguirá vigente y deberá mantenerse para canalizar también aquellas que puedan ser etiquetadas como “brechas” y por lo tanto notificables ante la Agencia Española de Protección de Datos en el plazo máximo de 72 horas.

8.- Confección de un análisis de riesgos y en el caso de que existan riesgos elevados ex artículo 35 del RGPD realización de una evaluación de impacto.

El enfoque de cumplimiento del RGPD ha de ser, en todo caso, desde el riesgo por lo que se ha realizado un análisis de riesgos que valora las amenazas a las que FEEX está sometida y en su caso, las medidas necesarias para mitigarlas. El riesgo en FEEX es muy bajo en general si atendemos a que el acceso a datos es muy restringido y en principio se cumplen las medidas mínimas y existe conciencia de confidencialidad.

Al no haberse detectado tratamientos de datos de alto riesgo contemplados en el RGPD, no es necesaria la realización de una evaluación de impacto.

9.- Formación del personal en sus obligaciones. Acuerdos de confidencialidad y políticas internas

Se transmitido formación al personal de la entidad sobre competencias en protección de datos y privacidad.

Igualmente se han revisado y/o actualizado los acuerdos de confidencialidad y los documentos y políticas en las que se recojan las obligaciones de secreto y de uso de herramientas informáticas así como protocolos de tratamiento de datos personales.

10.- Designación de un Delegado de Protección de Datos si procede o, en el caso de no ser obligatorio, designación de las personas responsables de privacidad en la organización.

Teniendo en cuenta que la actividad de FEEX se desarrolla básicamente en el entorno empresarial, no es necesaria la designación de un delegado de protección de datos en la entidad al no encajar sus tratamientos, de forma estricta, en los requisitos del artículo 37 del RGPD.

No obstante lo anterior, existe un responsable de seguridad que de momento puede ser suficientes para garantizar un pleno y adecuado cumplimiento. En este sentido deberá realizarse el nombramiento oficial para que así conste internamente.

11.- Revisión de cumplimiento de los principios del RGPD

El RGPD establece nuevos principios: responsabilidad proactiva, privacidad desde el diseño y por defecto, transparencia, minimización.

El cumplimiento de estos principios se constata en tanto que la entidad viene y está realizando un esfuerzo de adaptación y cumplimiento sin perjuicio de una revisión constante y el establecimiento de un plan de auditorías y revisiones para garantizar dicho cumplimiento.

12.- Emailing informativo y revisión de bases legitimadoras de los tratamientos de datos realizados

Al confeccionar el registro de actividades de tratamiento se han analizado las bases que legitiman los citados tratamientos.

Se ha constatado que en la mayoría de los tratamientos la base legitimadora es la ejecución contractual o la obligación legal por lo que no ha sido necesario actualizar los consentimientos sino únicamente informar.

Por ello, se ha enviado una circular informativa a los asociados de la entidad actualizando la política de información.

13.- Documentación de procedimientos

FEEX cuenta con una aplicación de gestión de la privacidad en la que se encuentran recogida la información mínima de cumplimiento del RGPD.

III.- Conclusión

Por lo anteriormente expuesto, estamos en condiciones de afirmar que la entidad **Asociación Española de Movilidad Laboral Internacional (FEEX)**, dentro de su plan de adaptación y cumplimiento del RGPD, se encuentra orientada al mismo y ha adoptado los pasos necesarios para garantizar que dicho cumplimiento sea adecuado.

Es cuanto procede informar con la información y datos disponibles a la fecha de firma del presente informe y salvo criterio mejor fundado.

En Madrid, a 26 de noviembre de 2018.

Paz Martín
Abogado.
CEO
LEGAL THINGS ABOGADOS