Adaptándonos a la era post-RGPD: supervisión del Modelo de Cumplimiento

Breves Regulación Digital

Septiembre 2019

En este número de Breves:

En el presente número de Breves: Recordamos la necesidad de llevar a cabo una revisión continuada del grado de cumplimiento de las obligaciones establecidas en el RGPD, mediante, entre otras acciones, el diseño de un Modelo de Gobierno de la Privacidad, que incorpore un mecanismo para la correcta adopción de medidas y controles, que permitan el adecuado despliegue del cuerpo normativo, el cumplimiento de los principios de transparencia y deber de información y la identificación de las amenazas y los riesgos para los derechos y libertades de los personas físicas. Así analizamos la siguientes medidas Post Adecuación GDPR:

- Modelo de Gobierno y Marco de Control
- Metodología de análisis de cumplimiento
- Gestión eficiente de la privacidad

Introducción

El cumplimiento normativo en materia de protección de datos no finaliza con la conclusión del procedimiento de adaptación de 25 de mayo 2018, sino que debe mantenerse en activo como un proceso estratégico más del negocio.

Las últimas resoluciones dictadas por la AEPD en procedimientos sancionadores han puesto en evidencia que la mayoría de los incumplimientos obedecen a una incorrecta gestión de la protección de datos que podrían haberse evitado con un adecuado Modelo de Gobierno de la Privacidad.

Así por ejemplo, el incumplimiento de los principios de protección de datos previstos en el art. 5 supone el 68% de los procedimientos sancionadores resueltos con apercibimiento o sanción. De este 68%, el 17% de las sanciones lo es por falta de adopción de medidas organizativas.

Medidas Post adecuación RGPD

La fecha de exigencia de adecuación a la normativa europea sirvió como fecha clave para que las compañías identificasen los tratamientos que llevaban a cabo, la legitimización con la que tratan los datos personales, evaluasen el riesgo e impacto en la privacidad que éstos podían comportar, y actualizasen sus políticas de privacidad.

Pero todo ese ejercicio devendrá ineficaz y a la vez quedará desactualizado si no se supervisa y monitoriza de forma continuada, creando un sistema de gestión y gobierno de la privacidad, en el marco del cumplimiento de la “Accountability”.

Podemos afirmar por tanto que no existe una correcta adecuación a la normativa europea si la organización no ha diseñado un Modelo de Gobierno de la Privacidad y un adecuado Marco de Control.

1. Modelo de Gobierno y Marco de Control.

Por Modelo de Gobierno de la Privacidad, entendemos el conjunto de metodologías, políticas y herramientas que permite la gestión de los datos personales y de la información para que la compañía pueda asegurar su calidad, su control y explotación según los objetivos estratégicos definidos dentro de la organización, en el marco del cumplimiento de la normativa aplicable.

El cumplimiento normativo en materia de protección de datos no finaliza con la conclusión del procedimiento de adaptación de 25 de mayo 2018, sino que debe mantenerse en activo como un proceso estratégico más del negocio”

Por Modelo de Gobierno de la Privacidad, entendemos el conjunto de metodologías, políticas y herramientas que permite la gestión de los datos personales y de la información para que la compañía pueda asegurar su calidad, su control y explotación”

Este modelo organizativo y de gestión dependerá obviamente del tamaño, volumen e intensidad en el tratamiento de los datos de cada organización, pero como mínimo debe contemplar los siguientes dominios:

- Identificación de las obligaciones a monitorizar en materia de protección de datos.

- Identificación de riesgos y amenazas: qué circunstancias pueden tener mayor impacto en los derechos y libertades de los ciudadanos.

- **Definición de roles, responsabilidades y metas**: El Gobierno de la Privacidad requiere de una estructura organizativa de roles que den soporte al responsable dentro de la organización (el DPO o el Responsable de Privacidad), de funciones y responsabilidades claramente definidas asignadas a cada rol, así como de las metas, políticas y otros procedimientos asociados al Modelo de Gobierno de la Privacidad.

- **Despliegue del cuerpo normativo interno**. Para poder poner en funcionamiento un modelo de gestión de la privacidad de forma eficaz, es esencial diseñar procesos sencillos para que todos los empleados puedan cumplir con la normativa sin que les suponga una carga.

  Para ello, es necesario contar con políticas y procedimientos que rijan la protección de datos y que deberán ser comunicadas de manera efectiva a los miembros de la organización.

- Con objeto de poder dar cumplimiento al Principio de Responsabilidad Proactiva, y que la compañía sea capaz de acreditar dicho cumplimiento, es necesario contar con **controles efectivos y definir KPI’s de cumplimiento** que garanticen que el Modelo de Gobierno está logrando sus objetivos y se mantiene vigente. Asimismo, para garantizar la efectividad de dichos controles, la organización deberá recabar las correspondientes evidencias, al objeto de acreditar documental o digitalmente el resultado y efectividad del control.

- Una vez diseñado el **Modelo de Gobierno** y establecido el **Marco de Control**, éstos, junto con el resto de obligaciones en materia de protección de datos, **deben ser objeto de verificación al menos una vez al año.**

2. Metodología de Análisis de cumplimiento.

El análisis de cumplimiento comporta un ejercicio de revisión del Modelo diseñado, incluyendo las medidas adoptadas y los Controles definidos para comprobar su efectiva implantación, el nivel de despliegue en la organización y la suficiencia éstos, de acuerdo con la siguiente metodología:

- **Revisión de la documentación existente:** idoneidad de la documentación generada que responda a las actividades de tratamiento que lleva a cabo la organización. La documentación objeto de revisión incluye tanto el Registro de actividades de tratamiento, análisis de las bases que legitiman el tratamiento, la metodología de análisis de riesgo empleada y resultado de las evaluaciones de impacto efectuadas, como los modelos de cláusulas y textos informativos, modelos contractuales, políticas de privacidad adaptadas a los distintos tratamientos identificados, criterios de conservación y almacenamiento de datos.

- En estas se incluyen las políticas y procedimientos de bloqueo, de gestión y notificación de incidentes de seguridad, identificación de tratamientos transfronterizos, entre otras.

- Del mismo modo, deberá revisarse la ponderación efectuada para determinar la necesidad de contar con Delegado de Protección de Datos, así como la Matriz de Riesgos y Controles desarrollada por la entidad, evaluando la adecuación de los Responsables, periodicidad, evidencias, soporte definidos e indicadores de cumplimiento definidos.

- **Análisis de cumplimiento**: Revisión de dicha documentación y los criterios aplicados en su elaboración para evaluar si cumple con los Principios de: responsabilidad proactiva; minimización, calidad y limitación del tratamiento; transparencia (deber de información a los interesados); privacidad desde el diseño y por defecto y licitud del tratamiento.

- **Revisión del Marco de control**: Respecto al Marco de Control, el objetivo es evaluar el catálogo de medidas identificado, el grado de implantación de las medidas que la organización ha puesto en marcha, su conocimiento por parte de la organización y la idoneidad del diseño de las actividades de control.
  Para ello será necesario llevar a cabo, entre otras, las siguientes acciones: identificación del catálogo de medidas; evaluación de su idoneidad, evidencia y actividad de control asociada; determinación de si existe periodicidad asignada a la actividad de control; ejecución de una prueba de testing por control para comprobar el nivel de implantación y grado de efectividad; identificación de las actividades de control a monitorizar de manera periódica; identificación del área responsable de la actividad de control y documentación de la evidencia.

- **Resultados**: Los resultados obtenidos se plasmarán en un cuadro de mando en el que se visualizarán y/o monitorizarán de forma continuada los siguientes aspectos: el mapa de calor con los riesgos de la entidad; organigrama de los encargados de dar soporte al responsable de la privacidad o al DPO; tareas y funciones asignadas a los intervinientes en el Gobierno de la Privacidad; prioridad y estado de las tareas y controles definidos; monitorización de los KPI's de cumplimiento para determinar la eficacia de las medidas y controles adoptados; recomendaciones y/o áreas de mejora que mitiguen los gaps de cumplimiento o que mejoren la eficacia del modelo de gobierno y gráficas que muestren de forma continua el grado de cumplimiento de la normativa.

3. Gestión eficiente de la privacidad.
Las nuevas exigencias y deber de responsabilidad proactiva o accountability han supuesto un notable aumento de tareas de compliance. Esto se ha traducido en una mayor carga de las organizaciones que, además de centrarse en el desarrollo y gestión del negocio, deben dotarse de mecanismos y medios para garantizar cumplimiento normativo en materia de protección de datos.

Para minimizar el impacto organizativo y operativo, es recomendable centralizar la gestión de la privacidad y automatizar los procesos, disponer de un repositorio central con los documentos más relevantes de su Modelo de Gobierno de la Privacidad, asignar las tareas a los diferentes responsables, automatizar la carga de información del RAT o disponer de un mecanismo de visualización del mapa de riesgos actualizado.

Para poder supervisar y gestionar de forma eficiente la protección de datos resultará crucial la aplicación de la tecnología. Por ello, contar con una herramienta de gestión de la privacidad que facilite la centralización y automatización de los procesos puede resultar clave para optimizar los recursos dedicados al cumplimiento.

Han participado en este Breves:

Assumpta Zorraquino
Socia responsable de Regulación Digital - New Law Department
assumpta.zorraquino@pwc.com

Alejandra Matas Brancós
Directora de Regulación Digital - New Law Department
alejandra.matas.brancos@pwc.com

Galindo Pérez Sánchez
Manager de Regulación Digital - New Law Department
galindo.perez.sanchez@pwc.com