EDICIÓN CONSEJEROS
MAYO 2018

LA FÁBRICA DE PENSAMIENTO
INSTITUTO DE AUDITORES INTERNOS DE ESPAÑA

SUPERVISIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

7 preguntas que un Consejero debe plantear

A partir del 25 de mayo de 2018 será obligatorio implantar el Reglamento General de Protección de Datos (RGPD) para todas las organizaciones establecidas o con relaciones comerciales con la Unión Europea.

Las exigencias de cumplimiento, y las penalizaciones en caso contrario (que podrían llegar a alcanzar hasta 20 millones de euros o el 4 % de la facturación anual), pueden tener consecuencias económicas, legales y reputacionales muy importantes.

El Reglamento no solo es de aplicación a las organizaciones ubicadas en la Unión Europea, sino también a otras que, encontrándose fuera de ella, ofrezcan productos o servicios, o monitoricen el comportamiento de ciudadanos de la Unión Europea.

Las comunicaciones de datos transfronterizas podrán llevarse a cabo siempre que las normas de protección de datos de los países de destino sean similares a la norma RGPD.

Los Consejos de Administración tienen un papel fundamental en sus organizaciones para supervisar que el cumplimiento del nuevo Reglamento tiene un enfoque de privacidad basado en riesgos y proporciona una seguridad razonable de que se han destinado los recusos necesario para proteger los derechos y libertades de las personas físicas.

Este documento aborda 7 cuestiones clave que un consejero debe tener en cuenta para garantizar que su organización alcanza la conformidad con el nuevo Reglamento.

The Institute of Internal Auditors

Instituto de Auditores Internos de España

1 ¿La entidad es consciente de que la conformidad con el nuevo reglamento va más allá de la adaptación de los controles actuales de ciberseguridad?

El RGPD no es solo una cuestión de ciberseguridad. Aunque afecta a la protección de datos personales frente a la piratería y las filtraciones o fugas de datos, el reglamento se ocupa de igual forma de los procesos de recogida, almacenamiento, uso y divulgación de estos datos por parte de las organizaciones, garantizando, con ello, los derechos y libertades de las personas físicas (empleados, clientes, etc.) en esta materia. Esta norma es más estricta con respecto al consentimiento, siendo necesario que sea "expreso" en los procesos de recogida de datos y, en muchos casos, ampliará la propia definición de los datos personales, incluyendo posibles identificadores *online* como las direcciones IP.

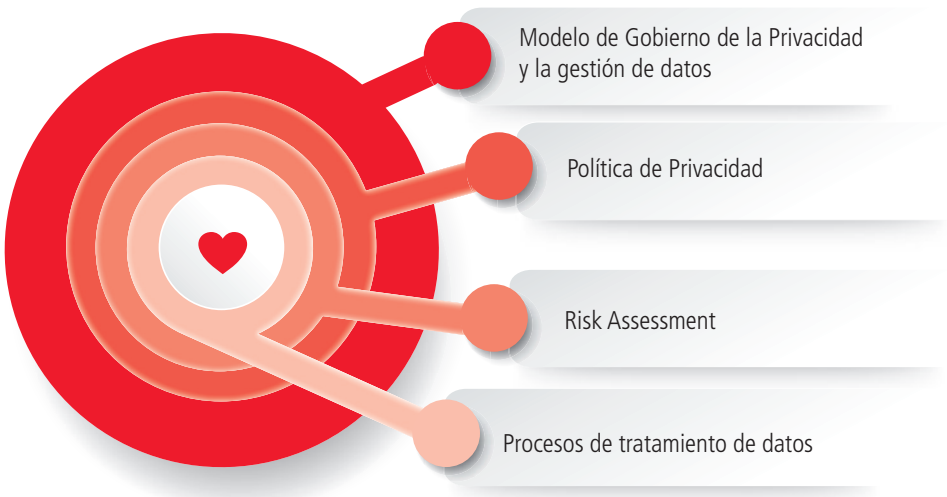
2 ¿La organización tiene diseñado e implantado un Modelo de Gobierno de la Privacidad?

La formalización de un Modelo de Gobierno de la Privacidad es un factor crítico de éxito. Se espera que las organizaciones puedan, a través de este Modelo, garantizar la privacidad y protección de los datos personales (responsabilidad proactiva), alcanzando la definición e implantación de criterios homogéneos de actuación en el contexto del tratamiento de datos: creación de códigos de conducta, mecanismos de certificación, marcas y sellos como forma de facilitar el cumplimiento del Reglamento, son algunos ejemplos de responsabilidad proactiva.

La implantación de este Modelo de Gobierno bajo un enfoque *Top-Down* trae consigo la necesidad de articular una Política de Privacidad y Protección de Datos como componente prioritario para trasladar al conjunto de la organización las directrices estratégicas consideradas por el propio Modelo. Por otro lado, la definición de este Modelo de Gobierno presentará el detalle de las funciones y obligaciones de las distintas partes interesadas para garantizar el cumplimiento de los principios, derechos y obligaciones recogidos en la norma RGPD y, con ello, respetar la privacidad como derecho fundamental de las personas físicas.

Desde el punto de vista de la gestión, estas directrices de privacidad recogidas en la Política serán desarrolladas en procedimientos de actuación que permitan la convivencia de la propia operativa de los procesos de negocio con las actividades de control precisas, de tal forma que los riesgos para la privacidad se encuentren por debajo de ciertos umbrales de aceptabilidad formalizados.

ENFOQUE TOP DOWN PARA EL CUMPLIENTO DEL RGPD



3 ¿Se ha asignado un Delegado de Protección de Datos que reporte directamente al consejo u otros miembros de la alta dirección?

Organizaciones cuya actividad principal sea la monitorización de datos y el procesamiento de grandes volúmenes de datos sensibles, se verán obligadas a la designación formal de un Delegado de Protección de Datos *(Data Protection Officer* - DPO), que rendirá cuentas al nivel jerárquico apropiado para asegurar que cuenta con la independencia necesaria para el cumplimiento de sus funciones.

Se trata de una función que, en la práctica, puede compartirse entre varias personas clave mientras queden debidamente identificadas las obligaciones, siendo posible el desempeño de otras funciones y cometidos siempre que no dé lugar a conflicto de intereses.

El Delegado de Protección de Datos deberá tener recursos suficientes para el correcto desempeño de sus obligaciones, así como otorgarle la potestad de actuación y condiciones de liderazgo necesarias para aumentar la efectividad del proceso de monitorización ejecutado por el mismo.

4 ¿La entidad realiza Evaluaciones de Impacto de Privacidad *(Privacy Impact Assessment* - PIA) para los procesos de tratamiento de datos?

Uno de los principios fundamentales recogidos en el Reglamento se centra en las Evaluaciones de Impacto de Privacidad *(Privacy Impact Assessment* - PIA).

Esta evaluación debe ser realizada tanto para los procesos existentes (cualquier iniciativa de tratamiento de datos) como para las nuevas iniciativas de tratamiento de datos *(Privacy by design)* siempre que pudiera derivarse un alto riesgo para los derechos y libertades de las personas físicas. De esta forma –desde una perspectiva de privacidad– podrán ser adoptadas las medidas técnicas y organizativas oportunas para mitigar tales riesgos.

5 ¿Se ha establecido un procedimiento de actuación en caso de fugas de información?

La regulación prevé un papel prioritario al proceso de implantación de medidas técnicas que eviten cualquier escenario de fuga de datos (fundamentalmente, el cifrado de los datos), y obliga a las compañías –responsables del tratamiento– a notificar al Órgano de Control español cualquier incidente de seguridad *(data breach)* que se presente en materia de protección de datos en un periodo máximo de 72 horas.

Estas notificaciones de incidentes de seguridad también deberán ser comunicadas en el caso de que se hayan presentado con relación a la información almacenada en proveedores de servicios (incluyendo la nube). Es prioritario, por tanto, la obtención de garantías de cumplimiento de la privacidad de los servicios externalizados (mediante la monitorización o auditoría de los servicios prestados por los proveedores externos).

6 ¿Ha implantado la organización un programa de concienciación sobre la protección de datos dirigido a empleados?

En última instancia, son los empleados los que llevan a cabo el tratamiento de los datos de carácter personal en el desempeño de sus actividades cotidianas.

En este sentido, todo Modelo de Gobierno de la Privacidad debe quedar sustentado por la correcta planificación de un programa de concienciación de los empleados, a través del cual, se puedan presentar los escenarios de riesgos a los que expone a la entidad en el caso de que se efectúe un tratamiento incorrecto de los datos de carácter personal.

7 ¿Se ha definido formalmente un modelo de relación entre el DPO y el área de Auditoría interna?

La necesidad de formalizar un modelo de colaboración entre el DPO y la función de auditoría interna es fundamental para la optimización de las labores de aseguramiento (Modelo de *Combined Assurance).*

Con las funciones de aseguramiento definidas, mejorará la eficiencia y efectividad del Modelo de Gobierno de la Privacidad, y será posible compartir las sinergias entre los procesos de monitorización (DPO) y Auditoría Interna.

El papel de Auditoría Interna

Auditoría Interna es una función clave de buen gobierno y apoyo fundamental de la Comisión de Auditoría y por ende del Consejo de Administración. Su independencia y la labor de aseguramiento que desarrolla hacen que sea un instrumento imprescindible para que los consejeros puedan supervisar la adecuada gestión y control de los riesgos derivados de la entrada en vigor del RGPD. Auditoría Interna deberá contar con los medios y recursos adecuados para cumplir estos objetivos.

En esta fase inicial de implantación, Auditoría interna, por sus conocimientos transversales de la organización y del sistema de control puede utilizar técnicas de gap analisis para revisar los controles existentes e identificar las áreas clave que necesitan mejora, y puede ofrecer asesoramiento sobre la implementación práctica de nuevos controles y procesos.

En el corto plazo, los equipos de Auditoría Interna deberían focalizar el esfuerzo en la planificación de auditorías orientadas a garantizar el alineamiento del Modelo de Gobierno de la Privacidad con las buenas prácticas de referencia en esta materia, así como la atención de los principios, derechos y obligaciones recogidas en la norma RGPD.

Con posterioridad, y una vez se pueda mantener el Modelo de Gobierno como estándar de referencia, se deben planificar las auditorías internas específicas que se estimen convenientes y con múltiples enfoques basados en los distintos procesos de tratamiento de datos personales existentes, así como un criterio de priorización del trabajo de campo en términos de los riesgos existentes para los derechos y libertades de los afectados por la ejecución de tales procesos de tratamiento.

Este documento recoge parte del estudio: "Risk in Focus – Hot Topics for Internal Audit 2018", elaborado por los Institutos de Auditores Internos de 6 países europeos, que describe los principales riesgos que deben tener en cuenta los Directores de Auditoría Interna en la preparación de sus planes de auditoria 2018, complementada por Pablo González Melgar, colaborador habitual del IAI en materia de privacidad y protección de datos.

Instituto de Auditores Internos de España

El Instituto de Auditores Internos de España es una asociación profesional fundada en 1983, cuya misión es contribuir al éxito de las organizaciones impulsando la auditoría Interna como función clave del buen gobierno. En España cuenta con más de 3.500 socios, auditores internos en las principales empresas e instituciones de todos los sectores económicos del país.