6ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Evaluación de Impacto en la Privacidad

Emilio Aced Félez
Jefe de Área – Unidad de Apoyo

Guía para una Evaluación del Impacto en la Protección de Datos Personales (EIPD)

Agencia Española de Protección de Datos
Marzo de 2014

Conceptos

- **Va más allá del cumplimiento normativo**
  - **Expectativas de privacidad de las personas ante tratamientos de datos personales que las afecten**
  - **Percepciones generales de la sociedad o de los colectivos más afectados por el tratamiento**
- **Análisis e identificación de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para la protección de datos**
- **Gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos**
- **Riesgo**
  - **Probabilidad de que suceda un hecho que produzca un daño a la privacidad de las personas cuyos datos se tratan o a la reputación de la organización que realiza esta actividad**

Definiciones

- **Proceso consciente y sistemático para evaluar efectos actuales o potenciales que un determinado proyecto podría tener en la privacidad individual y la forma en que estos efectos adversos se pueden mitigar**
- **Un proceso que ayuda a evaluar los riesgos existentes para la privacidad de las personas en la recogida, uso y comunicación de información, ayudando a identificar riesgos para la privacidad, prever problemas y proponer soluciones**

Elementos esenciales

- **Proceso más amplio que la comprobación del cumplimiento normativo**
- **Debe**
  - **Llevarse a cabo con anterioridad a la implantación de un nuevo producto, servicio o sistema**
  - **Ser sistemático y reproducible y estar orientado a revisar procesos y no a producir un informe final**
  - **Permitir una identificación clara de los responsables de las distintas tareas**
  - **Identificar y clasificar la información para determinar los datos personales que se tratan y sus características**
  - **Identificar quién y cómo tendrá acceso y tratará los datos personales**

Elementos esenciales

- **Participación de todos los afectados por el proyecto (departamentos internos, socios o entidades externas, afectados u otros agentes sociales**
- **Descripción de los controles que se implantarán para asegurar**
  - **Que solo se tratan los datos personales necesarios**
  - **Para las finalidades legítimas previstas y definidas**
- **El resultado final debe ser un documento con un contenido mínimo y una estructura definidos previamente**
  - **Debe tener un cierto grado de publicidad a cargo de la organización que ha realizado la evaluación**
  - **No contiene información confidencial o sensible**

Fases

- **Análisis necesidad evaluación**
  - **Reflexión previa sobre las situaciones que aconsejarían realizar EIPD**
  - **Pequeños cambios o proyectos pueden no justificarla, por su sencillez y escasos riesgos**
  - **No todas las EIPD tienen la misma intensidad ni el mismo grado de profundidad**
  - **El tipo y tamaño de la organización juegan un papel importante en la decisión**
    - **Pequeñas o medianas organizaciones**
    - **O aquellas cuya actividad principal no sea el tratamiento de datos**

    podrían optar por un proceso menos formal

Fases

- **Equipo trabajo y términos de referencia**
  - **Grupo de trabajo interdisciplinar que se encargue de obtener la información**
  - **Asuma la interlocución con los responsables del proyecto y con la dirección de la organización**
  - **Planifique las tareas, realice las consultas necesarias, evalúe los resultados y elabore el informe final**
  - **Requiere el apoyo y el compromiso de la dirección**
  - **Representantes áreas de negocio afectadas, TIC y Delegado de Protección de Datos**

Fases

- **Descripción proyecto y flujos de información**
  - **Paso crucial para realizar una correcta identificación de los riesgos**
  - **Objetivos**
  - **Actores implicados**
  - **Categorías de datos que se tratarán**
  - **Tecnologías utilizadas**
  - **Flujos internos y comunicaciones a terceros**
  - **Necesidad de utilizar o no todos los datos previstos**
  - **Necesidad de los participantes de acceder y utilizar datos personales o categorías de datos personales específicas**

Fases

- **Identificación y evaluación de riesgos**
  - **Es la parte esencial de la EIPD**
  - **Análisis de toda la documentación generada:**
    - **Ciclo de vida de los datos personales**
    - **Usos previstos**
    - **Finalidades**
    - **Tecnologías utilizadas**
    - **Identificación de los usuarios que accederán a los datos**

  para identificar los riesgos, reales y percibidos, existentes para la privacidad

Fases

- **Consulta con partes afectadas (internas/externas)**
  - **Fundamental para el correcto desarrollo EIPD**
  - **Visión de personas u organizaciones que no están implicadas en el proyecto y que, por ello, lo pueden observar desde una perspectiva más amplia**
  - **Pueden poner de manifiesto riesgos que hayan pasado desapercibidos para el equipo del proyecto**
  - **Incluyen a organizaciones externas con las que se va a compartir datos personales y representantes de los colectivos cuyos datos van a ser tratados**
  - **No es necesario hacer públicos los planes detallados sobre los nuevos productos o servicios o revelar secretos comerciales o tecnológicos**

Fases

- **Gestión de riesgos identificados**
  - **Los riesgos se pueden evitar o eliminar, mitigar, transferir o aceptar**
  - **Los que impliquen incumplimientos normativos deben ser eliminados o evitados**
  - **En la Guía se incluyen algunas medidas que podrían ayudar a esta gestión**

- **Análisis de cumplimiento normativo**
  - **Se aporta una guía indicativa**
  - **EVALÚA**

Fases

- **Informe final**
  - **Estructura definida previamente**
  - **Publicado (de forma completa o parcial si existen apartados que no pueden ser divulgados por restricciones legales, comerciales o de seguridad**
  - **Contenido y modelos incluidos en la Guía**

- **Implantación de las recomendaciones**
  - **Decisión de la dirección**
  - **Nombramiento persona o unidad encargada de ello con la necesaria autoridad**

Fases

- **Revisión de los resultados y realimentación**
  - **Revisión y comprobación de la implantación real y de la eficacia de las medidas correctoras**
  - **Examen del proyecto una vez operativo para verificar que los riesgos detectados se han abordado correctamente y que no existen otros nuevos**
  - **Auditorías que realimentan la EIPD**
  - **La modificación del proyecto o la incorporación de nuevas funcionalidades llevan consigo la necesidad de revisar la EIPD**

Conclusiones

- **Las EIPD son instrumentos que pueden jugar un papel fundamental en la mejora de la protección de datos**
- **Parte esencial de una nueva generación de herramientas y metodologías (PbD)**
  - **Que buscan una aproximación proactiva a los retos de implantar garantías para la privacidad**
- **Desarrollada con seriedad es un instrumento ideal para que los responsables puedan mostrar su compromiso y diligencia con los derechos de los ciudadanos y el cumplimiento de sus obligaciones**
- **La AEPD desea que esta Guía**
  - **Promueva la concienciación de las organizaciones**
  - **Impulse la utilización de esta herramienta**

para contribuir a la creación de confianza entre los ciudadanos en un tratamiento leal, lícito y transparente de sus datos personales

Consulta pública

En el portal de la AEPD

www.agpd.es

Plazo

Desde: 17/03/2014

Hasta: 25/04/2014

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es