Citibank

La función del Compliance Officer en la protección de datos personales

Citibank España S.A.
Teresa Serrano – Business Compliance Officer
Arturo Cuerda – Data Privacy Officer

Introducción

- La función de Compliance en la gestión global de riesgos
  - El concepto de “Cumplimiento”
    - Qué NO es Compliance: “Servicio de Inteligencia” de la entidad;Freno al negocio; Cortapisa a las relaciones interdepantamentales
    - Qué ES Compliance: Cumplimiento con el entorno normativo externo e interno (Legislación sectorial, políticas corporativas, Reglamento Interno de Conducta, Código deontológico)
  - Qué riesgos gestiona la función de Compliance: regulatorio, reputacional, de franquicia.

Introducción (Continuación)

-Aspectos derivados del incumplimiento con el el entorno normativo

- sanciones legales
- pérdidas económicas
- daño reputacional o de imagen

-La prevención como solución

-La colaboración entre áreas complementarias:

- Compliance,
- Auditoría,
- Gestión de riesgos

Principios

- Los principios que deben regir un programa de gestión de riesgos de Compliance y de prevención son:
  - La Independencia de la función respecto del “negocio”
  - Involucración de la Alta Dirección
  - Estructura organizativa bien definida y medios adecuados
  - Políticas y procedimientos escritos
  - Formación mínima que garantice un adecuado nivel de conocimiento de la organización y de las normas aplicables
  - Programas de Verificación y Vigilancia (Monitoring &Testing)
  - Acceso a la información y a todas las funciones y procesos
  - Interacción con Auditoría, Control Interno y Gestión de riesgos

El programa de prevención (I) Nuestra experiencia

Desarrollo y definición de un programa efectivo que implica:

1. Identificación de la **norma aplicable**. Especial referencia a entidades con actividad multijurisdiccional
2. Definición de **políticas internas** (políticas de privacidad) que desarrollen la norma. El problema de la coexistencia de diferentes políticas y el potencial conflicto normativo
3. Identificación de productos, servicios y **procesos afectados**. El mapa de riesgos o risk assessment (ej.flujos de datos personales)
4. Identificación de los **requerimientos legales** y corporativos exigibles en cada proceso
5. Elaboración de una **matriz normativa**

El programa de prevención (II)

6. Transmisión de los requerimientos legales y/o corporativos a los procesos concretos
7. Elaboración de **manuales de procedimientos** que contemplen los requerimientos plasmados en la Matriz de Riesgo Normativo
8. Elaboración y aprobación de un **Plan anual de Cumplimiento** que garantice un adecuado nivel de control y supervisión sobre la actividad de la entidad, asegurando la identificación temprana de debilidades y su posterior elevación a la Alta Dirección.

La gestión del riesgo de protección de datos en la entidad

- Actividades dirigidas a **velar** por el cumplimiento de las leyes locales, europeas y políticas corporativas que se refieren a protección de datos y privacidad, dentro de la entidad financiera.

- Asegurar que todos los riesgos legales y de Compliance relacionados con protección de datos personales, derivados de la actividad de negocio, están adecuadamente **identificados**, **evaluados** y **controlados**.

- La gestión del riesgo de Privacidad y Protección de Datos en la actividad de negocio, es realizada principalmente por el Data Privacy Officer en **coordinación** con **Asesoría Jurídica** y del responsable de la **Seguridad de la Información**.

Herramientas de gestión del riesgo de protección de datos y seguridad de la información (I)

- El Compliance Officer de Protección de Datos trata diferente información, para la adecuada gestión del riesgo reputacional y de imposición de sanciones de la AEPD:

  - ✓ **Matriz normativa** : Identificación de normas de protección de datos aplicables. Proyectos de implementación de normas y políticas.
  - ✓ **Procesos de autoevaluación** (RCSA): Permiten llevar a cabo revisiones periódicas de controles sobre procesos críticos y corregir posibles debilidades.
  - ✓ **Monitoring &Testing**: Llevados a cabo por la propia Unidad de Compliance. El Plan Anual debe contemplar aplicando criterios de riesgo (Risk Based Approach) revisiones “end-to-end” de procesos de alto riesgo.
  - ✓ **Informes de auditores internos**, en los que la Unidad de Compliance debe participar (directa o indirectamente). Necesidad de que Compliance apruebe los programas de auditoría.

Herramientas de gestión del riesgo de protección de datos y seguridad de la información (II)

- ✓ **Informes de auditoría externa** de medidas de seguridad. Coordinación de Compliance. Escalación de incidencias.
- ✓ **Análisis de Reclamaciones de clientes**: Detección de debilidades de procesos.
- ✓ **Tramitación de expedientes disciplinarios de la AEPD**: Coordinación conjunta de Compliance y Asesoría Jurídica
- ✓ **Demandas judiciales**: Responsabilidad de Asesoría Jurídica. Compliance debe recibir periódicamente información sobre litigios relacionados con protección de datos.
- ✓ **Incidentes de seguridad:** Procedimiento de escalación de incidentes. Comités de segumiento con participación de todas las áreas involucradas en un incidente de seguridad.
- ✓ **Foros especializados** en seguridad de la Información y protección de datos, **Noticias en buscadores, medios de comunicación**, etc.

Areas de especial riesgo en una entidad financiera (I)

- **Encargados del tratamiento:** Deber de velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en la normativa de protección de datos.
  - ✓ Deber de diligencia previa a la contratación.
  - ✓ Claúsula contractual de protección de datos (art.12 LOPD):
  - ✓ Asegurar la devolución o destrucción de los datos una vez cumplida la prestación contractual.
- **Transferencias internacionales de datos:** Especial complejidad en entidades multinacionales.
- Altas, bajas y actualizaciones de **ficheros declarados** a la **AEPD.**
- **Formación** en protección de datos y seguridad de la información.

Areas de especial riesgo en una entidad financiera (II)

- **Cancelación de Datos**
  - ✓ Concepto
  - ✓ Acceso a datos cancelados de acuerdo con la normativa de protección de datos
- **Listas Robinson**
  - ✓ Sensibilidad del cliente que ejercita el “opt-out”
- **Servicio de Atención al Cliente**
  - ✓ Ejercicio de derechos ARCO de la LOPD.
  - ✓ Puerta de entrada de clientes descontentos.
- **Ficheros de Solvencia Patrimonial**
  - ✓ Fuente de las principales sanciones.
  - ✓ Principio de calidad de datos. Requisitos de inclusión en los ficheros de solvencia patrimonial.

Conclusiones

- Riesgo gestionado de forma **independiente** por la Unidad de Compliance
- Estrecha **colaboración** con otras Areas (IS, AJ, Auditoria, etc…)
- Fuente de **riesgo legal** y **regulatorio** así como de **daños a la reputación** de la entidad
- Creciente exigibilidad de **Reguladores** y del propio mercado
- Necesidad de contar con **procesos permenentes de verificación y vigilancia** que aseguren un adecuado cumplimiento, así como una rápida detección de debilidades y su elevación a la Alta Dirección