Protección de Datos y Compliance

Centro de Gobernabilidad y Transparencia del IAE

HSBC

Regimen de Protección de Datos Personales

Eje del régimen de datos personales:

El titular de los datos es **dueño del bien intangible** que constituyen sus datos personales.

Cuando se recaban datos, **no se transfiere el derecho sobre los mismos** al receptor. **Depositario no nuevo dueño.**

Esto implica una serie de obligaciones para el receptor de los datos, al que la ley denomina responsable o usuario, y que es una suerte de depositario de ese bien intangible ajeno que son los datos personales.

Regimen de Protección de Datos Personales

Como en todo supuesto en que se recibe un bien ajeno, el mismo

debe ser preservado y cuidado para el dueño.

De esta forma la ley exige que al receptor:

Garantizar la seguridad, integridad y confidencialidad

(art.9 de la ley 25.326)

Rol de Legales y Compliance

1 - Recolección

Principales ejes de la etapa de Recolección o Captura

Bases de Datos

- **<u>Condición para la licitud</u>**: Inscripción en el Registro Nacional de Bases de Datos.
- **¿Qué bases deben inscribirse?** Todas aquellas que <u>describen algo sobre una persona determinada o determinable</u>.

Rol de Compliance

1) Definición políticas de protección de datos.
2) Asegurar la inscripción de las bases que aplican a la compañía y su actualización

Principio de calidad de los datos

- Ciertos.
- Adecuados
- Pertinentes
- No excesivos
- Exactos /actualizados.

Rol de Compliance

Asegurar que:

1) Los datos solicitados al titular sean sólo los necesarios para la finalidad informada.
2) Los datos solicitados sean consistentes con la regulación que aplica a la materia (ej: norma de apertura de cuentas del BCRA)

Consentimiento del titular del dato / Finalidad

<u>Consentimiento del "Titular del Dato":</u> Libre; Expreso; Informado

<u>Finalidad:</u> Comunicada al titular del dato al momento de la recolección (Resolución AAIP 14/2018).

Rol de Compliance

Asegurar que:

1) El consentimiento es acorde con los requisitos de la Ley.
2) Se encuentren disponibles las leyendas de la AAIP 14/2018 en la página web y formularios de recolección de datos.

1 – Recolección (cont.)

Principales ejes de la etapa de Recolección o Captura

Bases de datos	Fuente de los datos	Consentimiento
Clientes	Información proporcionada directamente por los clientes en los formularios de apertura de productos / servicios / contratos, etc.	Suscripción de la autorización que se incluye en las solicitudes y reglamentos de los productos y servicios contratados por los clientes.
Proveedores	Información presentada por los proveedores de bienes y servicios en oportunidad de su evaluación / contratación.	Clausulas específicas sobre Tratamiento de Datos incorporadas en los acuerdos de los proveedores de bienes y servicios.
Recursos Humanos	- CV cargado por el aplicante en la página - Nota de solicitud de empleo que completan los aplicantes - Documentación presentada por los individuos en oportunidad de su contratación.	Suscripción de las autorizaciones por parte de los aplicantes (Cuando cargan su CV en la página de la Entidad/ nota de solicitud de empleo) o empleados de la entidad (nota de tratamiento de datos).
Videovigilancia	Imágenes capturadas por las Video cámaras de filmación contínua.	Carteles que indican al público la existencia de cámaras de seguridad.

2 - Uso y Conservación
Principales ejes

Seguridad de los datos

Principio rector

Se deben adoptar las medidas técnicas y organizativas que permitan garantizar la seguridad y confidencialidad de los datos.

Medidas de seguridad (Resolución AAIP 47/2018) :

Catálogo técnico de **medidas recomendadas para medios informatizados/ no informatizados**

Rol de Compliance

Asegurar que el Documento de Seguridad se encuentre definido e implementado por las áreas especialistas en la materia.

Confidencialidad / Secreto Profesional

- Aplica a **todas** las personas que intervienen en cualquier fase del tratamiento de datos.
- Subsiste aún después de finalizada la relación con el titular del archivo de los datos.

Rol de Compliance

Asegurar que el Deber de Confidencialidad se informe y exija a los empleados y proveedores (Código de Conducta Empleados; Cláusulas de Confidencialidad incluidas en los contratos marco con proveedores, etc)

Asegurar el ejercicio de derechos

Derechos del titular del dato

- De acceso.
- De rectificación, actualización o supresión

Rol de Compliance

Definición de la política y responsables para asegurar el cumplimiento de los derechos del titular de los datos en los plazos y forma establecidos por la Ley de PDP.

2 - Uso y Conservación (cont.)

Principales ejes

Cesión / Transferencia Internacional de datos - ¿Qué evalúa Compliance?	
Tema	**Descripción**
Marco	Cesión o Prestación de Servicios Nacional o Internacional (Jurisdicciones involucradas)
Finalidad / Consentimiento	Consistencia con la actividad de la compañía y el consentimiento brindado por el titular del dato.
Datos involucrados	Detalle de los datos personales sujetos a transferencia Análisis de factibilidad en caso de secretos especiales (secreto bancario)
Marco contractual	Clausulas de Tratamiento de Datos / Confidencialidad Clausulas definidas por la Disposición 60 - E/2016 si involucra transferencia a jurisdicciones sin adecuada protección de datos. Definición clara de la cesión /prestación de servicios.
Medio transferencia	Email / Sharepoint / Sistema /documentación física
Contraparte	Compañía del mismo grupo económico / Terceros ajeno al mismo. Subcontratación
Demás requisitos	Requisitos inherentes a la actividad de la compañía exportadora del dato. Por ejemplo: normativa específica para la descentralización y tercerización de actividades emitida por el BCRA. Requisitos a aplicar en caso de prestación de servicios de proveedores de la nube.

3 - Destrucción
Principales ejes

Destrucción de la información

- Principio rector ➡ Los datos deben destruirse cuando ya no son necesarios o pertinentes a los fines para los cuales fueron recolectados.
- A tener en cuenta:
  - Definición de procedimientos de destrucción de datos personales en medios informatizados o no informatizados.
  - Establecimiento de mecanismos / medios seguros de eliminación de la información.
  - Procedimientos de descarte de medios magnéticos / archivos físicos (ej: trituración).
  - Cumplimiento de los plazos legales de guarda para cada tipo de información almacenada.

Rol de Compliance

1) Asegurar que el Documento de Seguridad se encuentre definido e implementado por las áreas especialistas en la materia.

2) Asegurar la existencia de una política de guarda de documentación para cada tipo de registro.