

#GBM

REGULACIONES DE DATOS: NAVEGANDO POR EL LABERINTO LEGAL

DAVID HIDALGO SEQUEIRA – ASSOCIATE Counsel

Departamento Legal I GBM Corporation

-

YOSER GONZÁLEZ HERNÁNDEZ – ASSOCIATE Attorney

Cumplimiento Regulatorio I Consortium Legal





David Alfredo Hidalgo Sequeira

Abogado Asociado en GBM Corporation

David es miembro del Departamento Legal Regional de GBM Corporation.

Es Licenciado en Derecho por la Universidad de Costa Rica con énfasis en Ciencias Forenses.

Hace parte del equipo legal de GBM atendiendo temas de cumplimiento, confidencialidad, tratamiento de datos personales y asuntos comerciales en países de la región de Centro América y el Caribe.





Yoser David González Hernández

**Abogado Asociado en Consortium Legal-
Costa Rica**

Es Licenciado en Derecho por la Universidad de Costa Rica y cuenta con especialidad en Derecho Notarial y Registral por la Universidad Fidélitas.

Cuenta con 9 años de experiencia en la firma, colaborando desde el Departamento de Real Estate en temas corporativos, inmobiliarios, ambientales y de cumplimiento regulatorio.



DEFINICIONES RELEVANTES

Titular de datos personales: Persona física al que pertenece información personal con capacidad de ejercer sus derechos (Habeas Data).

Datos personales: Información relativa a una persona física identificada o identificable.

Datos personales sensibles: Información íntima, vida personal o privada de las personas físicas, como sus gustos y preferencias, condición socioeconómica, convicciones, datos médicos o biométricos, etc.

DEFINICIONES RELEVANTES

Base de datos: Conjunto estructurado de datos (personales), sea manual o automatizado, que al que se le da un tratamiento o procesamiento de datos personales.

Tratamiento de datos personales: Cualquier operación o conjunto de estas, bajo procedimiento, que se aplican sobre los datos para su recolección, orden, ajuste, transmisión y/o eliminación, entre otras acciones.

Roles de Tratamiento de datos personales: Personas que administran y dirigen la finalidad de la base de datos (Responsables) o Personas que ejecuta las acciones de tratamiento de datos personales (Encargados).

CONTEXTO INTERNACIONAL

En el contexto en que Europa reconoce “la vida privada, familiar, el hogar y las comunicaciones privadas” como un Derecho Humano como reconocimiento local de la Declaración Universal de los Derechos Humanos (1948), bajo el Convenio Europeo de Derechos Humanos (1950).

Este desarrollo se ve reflejado en América en sus Constituciones Políticas.

A partir de los procesos de búsqueda de desarrollo económico de la Unión Europea (1980's) se crea un sistema de protección de datos, privacidad y el flujo de información personal; derivando en la Directiva de Protección de Datos (1995).

CONTEXTO INTERNACIONAL

Habiéndose puesto en el radar jurídico la relevancia de legislar sobre los datos personales y su debido tratamiento, aparecen legislaciones en América inspiradas en esta regulación y sus reformas bajo leyes especiales (ejemplos: CR, PA, NI, RD, CO, entre otras).

A partir de los cambios que hemos experimentado en tecnologías de la información, transmisión / transferencia de datos y negocios internacionales, se actualiza la legislación de referencia y se emite el Reglamento General de Protección de Datos (GDPR, 2016).

Lo anterior ha generado actualización en las demás normas americanas inspiradas incluyendo las que aplican a los territorios de actividad comercial de la región.

DATOS PERSONALES EN LA REGIÓN

País	Regulación
Costa Rica	Ley No. 8968 de 2011 y su Reglamento.
Panamá	Ley No. 81 de 2019 y su Reglamento.
Nicaragua	Ley No. 787 de 2012 y su Reglamento.
Honduras	Constitución Política + Código Penal Proyecto de Ley y Tratamiento de entes públicos*
El Salvador	Constitución Política + Código Penal Proyecto de Ley y Tratamiento de entes públicos*
Guatemala	Constitución Política + Código Penal Proyecto de Ley y Tratamiento de entes públicos*
República Dominicana	Ley No. 172 de 2013 y su Reglamento.



COSTA RICA: LEY NO. 8968 DE 2011 Y SU REGLAMENTO.

Obligación general constitucional de un debido manejo de datos que pertenecen a titulares personas físicas.

Régimen especial: Enfoque en la comercialización de datos personales.

Ente regulador: Agencia de Protección de Datos de los Habitantes (PRODHAB).

Delito especial: Violación de Datos personales (Art 196 bis, Código Penal).



COSTA RICA: OTRAS DISPOSICIONES LEGALES.

Protección de datos
personales en comercio
electrónico

Adopción de medidas de
seguridad
Informar nivel de
seguridad
Cláusulas de protección

Protección de datos
personales en servicios
financieros

Consentimiento
Informado
Adopción de medidas de
seguridad técnicas



NICARAGUA: LEY NO. 787 DE 2012 Y SU REGLAMENTO

Obligación general constitucional de un debido manejo de datos que pertenecen a titulares personas físicas.

Régimen especial: Enfoque estructural aplicando a cualquier conjunto de datos personales bajo formato de base de datos.

Ente regulador: Dirección de Protección de Datos Personales (DPDP).

Delito especial: Violación a la autodeterminación informativa (Art 444, Código Penal).



PANAMÁ: LEY NO. 81 DE 2019 Y SU REGLAMENTO

Obligación general constitucional de un debido manejo de datos que pertenecen a titulares personas físicas.

Régimen especial:
Enfoque territorial de ubicación de las bases de datos o del ejercicio del tratamiento.

Ente regulador:
Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI).

Delitos especiales:
Manipulación de bases de datos y Tratamiento de datos indebido (Art 226 y 292, Código Penal).



REPÚBLICA DOMINICANA: LEY NO. 172 DE 2013 Y SU REGLAMENTO

Obligación general constitucional de un debido manejo de datos que pertenecen a titulares personas físicas.

Régimen especial: Enfoque financiero-bancario aplicando mayor severidad a las entidades del sector bancario que gestionan bases de datos (Sociedades de Información Crediticia).

Ente regulador: Superintendencia de Bancos (SB).

Delito especial: Violación del tratamiento de datos personales (Art 88, Ley No. 172-13).

BUENAS PRÁCTICAS PARA LA PROTECCIÓN DE DATOS



Las obligaciones del prestador de servicios ante un tratamiento de datos personales debe estar debidamente limitado a su aplicabilidad y estrictamente al alcance del servicio.



Implementar una Política de Tratamiento de Datos Personales de acceso público.



Implementar Políticas de Tratamiento de Datos Personales locales en caso de grupos empresariales con diferencias legislativas marcadas.



Implementar una Política de Seguridad de la Información de acceso público y una Política de uso ético de las Inteligencias Artificiales.



Implementar un Aviso de Privacidad para dar detalle a las formas de tratamiento a las que se sujeta una determinada interacción con tratamiento de datos.

BUENAS PRÁCTICAS PARA LA PROTECCIÓN DE DATOS



La información personal que sea recolectada como parte del tratamiento de datos personales debe ser solicitada con el debido consentimiento informado del titular de los datos personales.



Como operación adicional, la información personal que sea transmitida o transferida como parte de los fines del tratamiento de datos personales debe ser autorizado con el debido consentimiento informado del titular de los datos personales.



Implementar medidas de seguridad físicas, administrativas y técnicas; así como de confidencialidad para procurar el debido tratamiento de datos personales.



En caso de que en la legislación local indique el deber de registrar las bases de datos y/o registrarse como entidad que realiza tratamiento de datos personales, cumplir con esta obligación en tiempo y forma ante el ente regulador.



Ante disposiciones legales de tratamiento de datos personales en los contratos se recomienda revisar de manera conjunta con el Departamento Legal y con el Information Security Manager, o sus equivalentes funcionales.

BUENAS PRÁCTICAS PARA LA PROTECCIÓN DE DATOS



Descubrir y Clasificar

- Definir los niveles de clasificación
- Definir los criterios de clasificación
- Descubrir la información

1



Definir Políticas

- Políticas de acceso
- Políticas de cumplimiento
- Políticas del manejo de datos

2



Desarrollar un análisis

- Análisis de accesos a los datos
- Análisis de Vulnerabilidades

3

4

Implementar controles

- Privacidad
- Integridad
- Disponibilidad

5



Monitorizar el acceso a los datos y tomar acción

- Monitoreo de la actividad
- Detección de Amenazas
- Análisis de comportamiento
- Responder a amenazas

CONCLUSIONES



A pesar de que las legislaciones comparten como fuente la regulación de GDPR, y que por esto son similares entre sí, se puede evidenciar que cada una tiene sus particularidades por lo que es necesario conocerlas para aplicarlas bien.



La tecnología es un aspecto en constante cambio y avance de nuestra realidad, y con esto surge la necesidad de una actualización constante para poder proteger los datos personales, dado a que estos cambios conllevan nuevos y mejorados medios para ser vulnerados.



En la medida en que los riesgos incrementan, no solo es obligación del Estado y sus leyes, sino también de las empresas de tener sus iniciativas para colaborar en la protección de los datos personales, permitiendo el avance y uso responsable de otras herramientas



Es responsabilidad de las empresas y de los individuos conocer y actualizarse de las regulaciones aplicables en materia de protección de datos para el debido cumplimiento de sus obligaciones.



Las empresas deberán contar con una Política de Tratamiento de Datos Personales dar cumplimiento a las obligaciones como responsables de estas operaciones. Esta deberá acompañarse de otras políticas o iniciativas para reforzar los controles y velar por su cumplimiento práctico.



Cualquier consulta, duda, sugerencia, podrá realizarla a través del correo electrónico: mercadeo@gbm.net dirigido a la consulta sobre el tema de Tratamiento de Datos Personales y Privacidad de Datos.