XII ENCUENTRO IBEROAMERICANO PROTECCIÓN de DATOS PERSONALES

ifai Transparencia y Privacidad
Organismo Autónomo

RED IBEROAMERICANA DE PROTECCION DE DATOS

Ciudad de México, México
12 y 13 de noviembre de 2014

SESIÓN 4
La actividad empresarial y la privacidad.
Las transferencias internacionales de datos y la convergencia entre sistemas de protección.

DAVARA
ABOGADOS, S.C.

XII ENCUENTRO IBEROAMERICANO DE PROTECCIÓN DE DATOS
13/Noviembre/2014

Dra. Isabel Davara F. de Marcos

¿Por qué hablar de transferencia internacional de datos desde la perspectiva empresarial?

Transferencia o transmisión, pero similares reglas:
México es el 3er país en el mundo en outsourcing de tratamiento de datos (especialmente en call centers), después de India y Filipinas: **poder tratar datos de terceros países implica empleo y resultados económicos**

Implica flujo de capitales y/o personas

Implica comercio

¿Qué legislación/reglas aplica?:
Lo plantearemos dependiendo de si la transferencia sale de México o llega a México desde distintos entornos geográficos y/o regulatorios

Por lo tanto, en términos de procedencia y/o aplicación de la legislación….

1. **Desde México:**
    1. Necesario el consentimiento del titular.
    2. Salvo las excepciones previstas
2. **A México:**
    1. Desde países con legislación parecida a la UE
        1. México no es aún un país con nivel adecuado de protección
        2. Claúsulas contractuales caso por caso
        3. BCR
    2. Desde USA - Entorno APEC

Transferencias (y/o transmisiones) desde México

Régimen Mexicano

1. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra **sujeta al consentimiento** de su titular, salvo las **excepciones** previstas en el artículo 37 de la Ley.

2. Deberá ser informada a este último mediante el **aviso de privacidad** y limitarse a la finalidad que la justifique.

Las transferencias internacionales

1. Serán posibles cuando **el receptor de los datos personales asuma las mismas obligaciones** que corresponden al responsable que transfirió los datos personales. (Artículo 74 del RLFPDPPP).
2. El responsable que transfiera los datos personales podrá valerse de **cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones** a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales. (Artículo 75 de RLFPDPPP).
3. Los responsables podrán **solicitar la opinión del Instituto** respecto a si las transferencias internacionales que realicen cumplen con lo dispuesto por la Ley y el presente Reglamento. (Artículo 76 del RLFPDPPP).

Transferencias (y/o remisiones) a México

Estados Unidos de América y entorno APEC

Unión Europea

Régimen Europeo

1. Consentimiento y excepciones
2. País con nivel adecuado de protección
3. Contratos
4. Binding Corporate Rules

Régimen Europeo - Consentimiento

Artículo 36 LFPDPPP

Consentimiento

Excepciones (art. 37 LFPDPPP)

I. Esté prevista en una **Ley o Tratado**

II. necesaria para un **diagnóstico médico**

III. Efectuada a **sociedades controladoras, subsidiarias o afiliadas** bajo el control común del responsable siempre que que opere bajo los mismos procesos y políticas internas;

IV. Necesaria por virtud de un **contrato** celebrado o por celebrar en interés del titular

V. Exigida para la salvaguarda de un **interés público**, o para la procuración o administración de justicia

VI. Reconocimiento, ejercicio o defensa de un derecho en un **proceso judicial**

VII. Mantenimiento o cumplimiento de una **relación jurídica entre el responsable y el titular.**

Artículo 26.1 Directiva 95/46/CE

a) El interesado haya dado su **consentimiento** inequívocamente

Excepciones

b) Sea necesaria para la **ejecución de un contrato entre el interesado y el responsable del tratamiento**.

c) Sea necesaria para la **celebración o ejecución de un contrato celebrado o por celebrar** en interés del interesado, entre el responsable del tratamiento y un **tercero**,

d) Sea necesaria o l**egalmente exigida para la salvaguardia de un interés público** importante para el reconocimiento, ejercicio o defensa de un derecho en un **procedimiento judicial,**

e) Sea necesaria para la salvaguardia del **interés vital del interesado,**

f) La transferencia tenga lugar desde un **registro público**

Régimen Europeo - Nivel adecuado

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un **nivel de protección adecuado.**

2. **El carácter adecuado del nivel de protección** que ofrece un país tercero **se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos**; en particular, se tomará en consideración l*a naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero* de que se trate, así como las n*ormas profesionales y las medidas de seguridad en vigor* en dichos países.

3. Los **Estados miembros y la Comisión se informarán recíprocamente** de los casos en que consideren que un tercer país **no garantiza un nivel de protección adecuado** con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros **adoptarán las medidas necesarias para impedir cualquier transferencia** de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a **remediar la situación** que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un n**ivel de protección adecuado de conformidad con el apartado 2 del presente artículo**, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas. Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

ART. 25 DIRECTIVA

- La Directiva 95/46 CE **no prevé una definición** de adecuación.

- La frase "nivel adecuado de protección" brinda suficiente **flexibilidad** a efectos de su aplicación a las diferentes realidades en que dicho estándar es aplicado.

- La Unión Europea emplea el **estándar de "nivel adecuado de protección"** en relación con terceros países.

- A efectos de **calificar** a éstos, la Unión Europea tampoco usa el estándar de equivalencia como punto de referencia, en cambio, provee **otros criterios** que permiten determinar si un país ofrece un nivel de protección adecuado o no.

Interpretación de la noción de "nivel adecuado de protección"

De acuerdo al **Grupo del artículo 29 sobre Protección de Datos**, hay dos elementos esenciales en cualquier análisis relativo al "nivel adecuado de protección":

1) El contenido de las reglas aplicables y

2) Los medios para asegurar su efectiva aplicación.

La evaluación requiere constatar la **apropiada adopción y cumplimiento de las disposiciones** sobre protección de datos personales.

El "nivel adecuado de protección" requiere la existencia de disposiciones que garanticen los *derechos de los titulares de datos personales*, imponen *obligaciones a los responsables de tratamiento*, establecen *principios aplicables al procesamiento de datos*, y *responsabilidad*, en caso de infracción.

Dichos requisitos están **presentes en la mayor parte de los instrumentos internacionales** relativos a la protección de los datos personales, lo que evidencia un significativo **nivel de consenso** en torno a ellos.

Evaluación del “nivel adecuado de protección”

El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración:

- la naturaleza de los datos
- la finalidad y la duración del tratamiento o de los tratamientos previstos,
- el país de origen y el país de destino final,
- las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate,
- así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 25.2 Directiva 95/46/CE

- La Comisión ha reconocido que los siguientes países aseguran un "nivel adecuado de protección”.

AD - Andorra
AR - Argentina
AU - Australia
CA - Canada
CH - Switzerland
FO - Faeroe Islands
GG - Guernsey
IL - State of Israel
IM - Isle of Man
JE - Jersey
US - United States - Transfer of Air Passenger Name Record (PNR) Data
NZ - New Zealand
US - United States - Safe Harbor
UY - Eastern Republic of Uruguay

Régimen Europeo - Contratos

Art. 37.3 LFPDPP y 70 RLFPDPP

III. Efectuada a **sociedades controladoras, subsidiarias o afiliadas** bajo el control común del responsable que opere bajo los mismos procesos y políticas internas:

En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con normativa aplicable, podrá ser:

La existencia de **normas internas de protección de datos** personales cuya observancia sea **vinculante.**

Siempre y cuando éstas cumplan con lo establecido en la normatividad.

Art. 26.2 Directiva 95/46

Los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado cuando:

El responsable del tratamiento ofrezca **garantías suficientes** respecto de:

- La protección de la vida privada.
- Los derechos y libertades fundamentales de las personas.
- Respecto al ejercicio de los respectivos derechos.

Las garantías podrán derivarse, en particular, de **cláusulas contractuales apropiadas**

Régimen Europeo - contratos

RESPONSABLE-RESPONSABLE

- Definiciones
- Acuerdo de transferencia de datos
- Obligaciones del exportador de datos
- Obligaciones del importador de datos
- Responsabilidad y derechos de terceros
- Legislación aplicable
- Resolución de conflictos con los interesados o con la autoridad
- Resolución de las cláusulas
- Variación de las cláusulas
- Descripción de la transferencia
- ANEXO A
  PRINCIPIOS RELATIVOS AL TRATAMIENTO DE DATOS

Decisión **2001/497/CE,** de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la **transferencia** de datos personales a un tercer país; Decisión **2004/915/CE,** de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE, de 15 de junio de 2001 y Decisión 2004/915/CE, se contiene, un **régimen de responsabilidad** basado en la obligación de diligencia debida, en virtud del cual el exportador y el importador de datos responderían ante los interesados por el incumplimiento de sus obligaciones contractuales respectivas.

RESPONSABLE-ENCARGADO

- Definiciones
- Detalles de la transferencia
- Cláusula de tercero beneficiario
- Obligaciones del exportador de datos
- Obligaciones del importador de datos
- Responsabilidad
- Cooperación con las autoridades de control
- Legislación aplicable
- Mediación y jurisdicción
- Variación del contrato
- Obligaciones una vez finalizada la prestación de servicios de tratamiento de datos personales
- Subtratamiento de datos

Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los **encargados** del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

Régimen europeo - Binding Corporate Rules (BCR)

- Las **BCR**, desarrolladas por el Grupo de Trabajo de Protección de Datos del Articulo 29, son un mecanismo adecuado que permite la transmisión de información de los titulares a países que no garantizan un nivel “adecuado” o “equiparable” de protección de datos.

- Se trata de una forma de avalar la libre circulación de información sin poner en peligro el nivel de protección de datos de los sujetos previsto en el país exportador.

BCR

Definición y Características

- Normas internas adoptadas por un grupo multinacional de empresas, que definen una política común, **en lo que respecta a transferencias internacionales** de datos entre compañías del grupo ubicadas en países que no proporcionan un nivel adecuado de protección
- Naturaleza **vinculante** o exigibles legalmente.
- Aplicación a un grupo de empresas o entidades **sometidas al control de la entidad matriz**.
- Su cumplimiento puede ser **exigido de forma externa por parte de terceras entidades oficiales** e independientes.
- Dotan a las organizaciones multinacionales de un **marco común** para realizar transferencias internacionales de datos de forma ágil, sencilla y cumpliendo el marco normativo comunitario.

Ventajas

1. Lograr dar cumplimiento a los principios de los arts. 25 y 26 Directiva Europea 95/46/CE.
2. Lograr **armonizar** prácticas y procedimientos en materia de protección de datos.
3. **Reducir y prevenir riesgos** derivados de las Transferencias Internacionales a terceros países.
4. **Evitar soporte contractual por cada transferencia individual**.
5. **Comunicación externa de la política** del Grupo .

Recomendaciones para incorporar las BCR

1. Definir procedimientos de aplicación y cumplimiento
2. Definir procedimientos de aplicación y cumplimiento
3. Definir el flujo de datos, especialmente aquellos transnacionales
4. Incluir en todo caso cláusulas que garanticen un nivel de cumplimiento alto
5. Redactarlas con un enfoque adaptado y adecuado a las particularidades del sector
6. Programar y realizar auditorías periódicas de los sistemas
7. Procedimiento estándar de reclamaciones ágil, sencillo y ajustado a los plazos
8. Procedimientos ágiles, estándares y sencillos para lograr la cooperación con las autoridades
9. Regular específicamente la reparación e indemnización adecuada de los titulares
10. Elegir adecuadamente la autoridad de protección de datos que gestionará el procedimiento de autorización con el resto de autoridades.

USA y ENTORNO APEC

USA

La regulación en USA es inexistente respecto de las transferencias de datos que se pueden realizar a México.

La regulación en USA más bien pretende muchas veces que se realicen transferencias (por blanqueo de capitales o por terrorismo por ejemplo) que en la legislación mexicana no están permitidas.

La legislación en USA sobre privacidad es diversa y dispersa, sectorial y estatal, complicada de conocer y de cumplir, pero en transferencias internacionales no se preven reglas de carácter general.

APEC - Cross Border Privacy Rules (CBPR)

1. Las Reglas de Privacidad Transfronteriza tienen como objetivo asegurar que los datos personales que se comunican o intercambian entre las economías de la región Asia-Pacífico estén debidamente protegidos.

2. Este sistema facilita a los responsables ubicados en distintas Economías de Asia Pacífico transferir DP entre ellos, siempre y cuando las transferencias sean seguras de conformidad con el Marco de Privacidad de APEC .

3. Actualmente hay 3 economías participantes en el sistema Estados Unidos, México y Japón. Canadá y algunos otros están en proceso…

Sistema APEC-CBPR

El Sistema de Reglas de Privacidad Transfronteriza (CBPR) Tiene 4 componentes principales:

- **Reconocimiento de criterios** para las organizaciones dispuestas a convertirse en un Agente Responsable certificado por el sistema APEC CBPR.

- Un **cuestionario de entrada para organizaciones** que deseen estar certificadas como compatibles con el sistema APEC CBPR por un **Agente Responsable.**

- **Criterios de evaluación para su uso** por Agentes Responsables certificados por el sistema APEC CBPR cuando revisen las respuestas de una organización para el cuestionario de entrada.

- Un **Acuerdo de Cooperación Transfronteriza en Materia de Privacidad** (**CPEA**) para asegurar que cada uno de los requerimientos del programa APEC CBPR se pueden hacer cumplir por las economías participantes en APEC.

El Sistema se basa en la validación de las políticas y prácticas de privacidad y protección de datos personales de las empresas u organizaciones que pretendan tratar datos personales provenientes de algún país miembro del Foro APEC, a fin de garantizar un tratamiento seguro de la información personal.

Agente Responsable

Hasta ahora, solamente Estados Unidos cuenta con un agente responsable: TRUSTe. Por su parte Japón y México no han identificado a sus Agentes Responsables..

Una Autoridad PE es cualquier organismo público que se encarga de hacer cumplir las Leyes de privacidad y que tiene facultades para realizar investigaciones o proseguir los procedimientos de ejecución, **en México esta autoridad es el IFAI.**

Sistema APEC-CBPR

Este sistema refiere las bases para el desarrollo de regional de transferencias seguras y confiables de datos personales entre las Economías APEC.

Marco de Privacidad APEC

- Mejora el intercambio de información entre agencias de gobierno y reguladores
- Facilita la transferencia segura de información entre economías.
- Establece un conjunto común de principios de privacidad.
- Motiva el uso de datos electrónicos como medios para perfeccionar y expandir los negocios.
- Provee asistencia técnica para aquellas economías que aun tienen que hacer frente a políticas de regulación en privacidad.

Principios

Prevención de Daño, Aviso, Limitaciones de la Recolección, Usos de la Información Personal Elección, Integridad de la Información Personal., Medidas de Seguridad, Acceso y Corrección y de Responsabilidad.

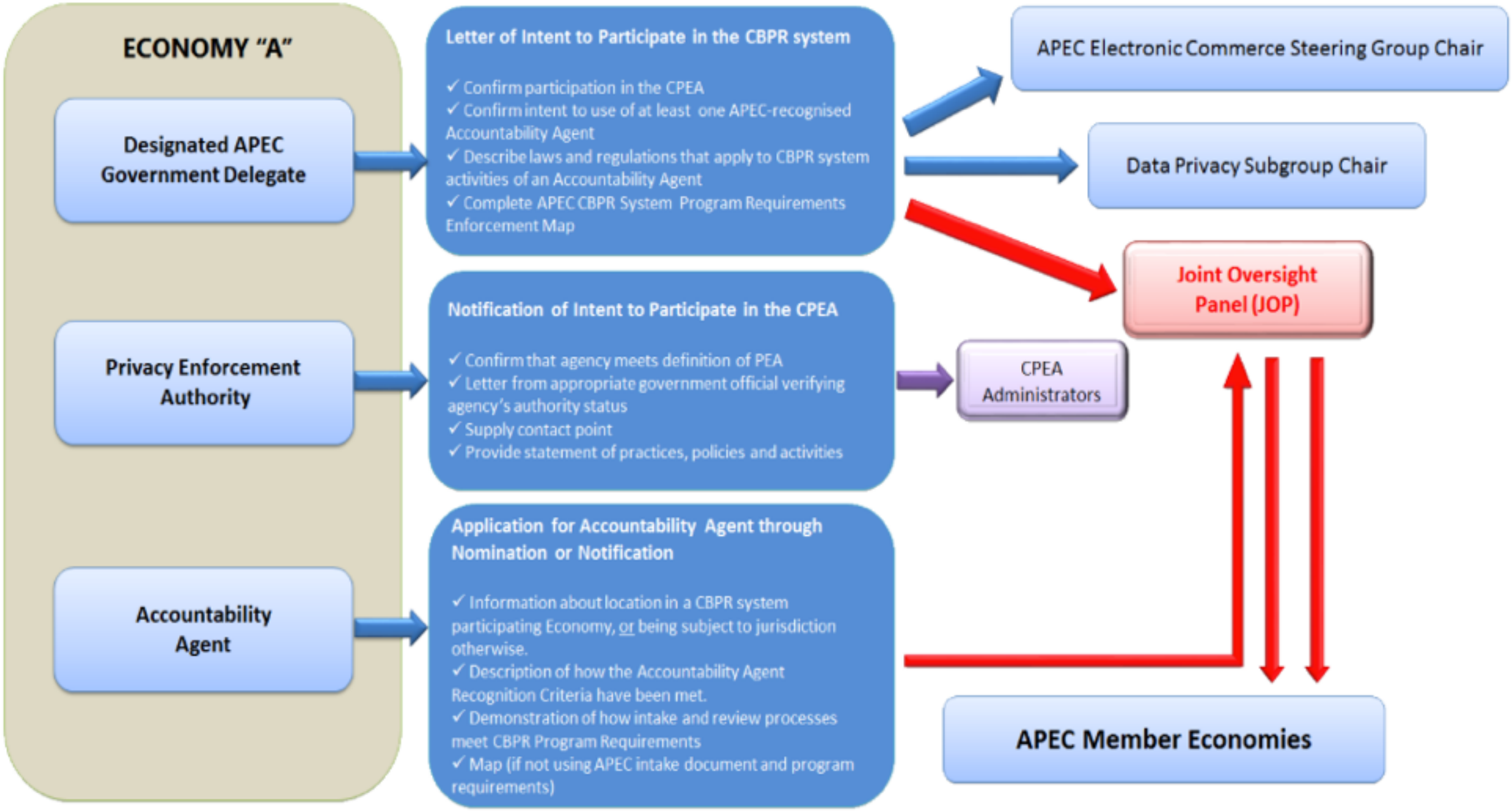
Acuerdo de Cooperación Transfronteriza en Materia de Privacidad (CPEA)

Crea un marco jurídico para la cooperación regional en el cumplimiento de las Leyes de Privacidad. Cualquier Autoridad de Privacidad en una economía APEC puede participar.

El CPEA tiene como propósito:

- Facilitar la transferencia de información entre Autoridades de Privacidad APEC.
- Proporcionar mecanismos para promover la cooperación transfronteriza entre autoridades en el cumplimiento de la legislación en materia de privacidad.
- Alentar el intercambio de información y cooperación en investigación sobre privacidad y su cumplimiento con Autoridades de Privacidad fuera de APEC.

Structure of the APEC Cross Border Privacy Rules (CBPR) system



Unión de México al sistema APEC-CBPR

28 de septiembre de 2012

Solicitud presentada por la Secretaría de Economía, ante el Comité Ejecutivo de Comercio Electrónico de APEC (ECSG), para que México forme parte del Sistema.

Enero de 2013

APEC emite un reporte de resultados en el que declara que México satisface los requisitos establecidos para ser parte del sistema de CBPRs. México se convierte en el segundo participante del Sistema CBPR.

Febrero de 2013

Integración de México como parte del Sistema de Reglas de Privacidad Transfronteriza

Implicaciones

Una vez que la organización ha sido certificada para participar en el sistema CBPR, sus políticas de privacidad y practicas será obligatorias para la entidad participante y serán ejecutables por la autoridad reguladora correspondiente del país en el que se encuentra.

Contar con terceros certificadores reconocidos ante APEC que validen las políticas y prácticas de privacidad y protección de datos personales de empresas mexicanas que busquen ofrecer servicios en APEC.

Beneficios económicos a través de la atracción de inversiones, al ser una economía que ofrece garantías suficientes para la protección de los datos personales

Ventajas de las CBPR

- **Favorecen el cumplimiento con el marco legal:** Los negocios que están certificados con CBPR pueden tener un amplio grado de cumplimiento con respecto a los requerimiento de varas jurisdicciones participantes.

- **Facilitan las comunicaciones transfronterizas de datos:** Las CPBR fueron diseñadas ara funcionar como una mecanismo de transferencia transfronteriza de datos que tienen restricciones de exportación de datos pero que permiten excepciones, como cuando una compañía participa en un determinado código de conducta transfronterizo.

- **Demuestran responsabilidad organizacional:** Tener un cumplimiento interno en materia de privacidad ayudará a las organizaciones a demostrar responsabilidad y esfuerzos de buena fe para cumplir con las obligaciones en materia de privacidad en el caso de una investigación o ejecución de una acción legal.

- **Generan confianza en el consumidor:** Participar en las CBPR crea confianza en el consumidor lo que representa una ventaja competitiva.

- **Uniformidad a los mecanismos de protección a la privacidad en la organización**: participar en el sistema CPBR perfecciona una habilidad de la organización internacional para estandarizar sus marcos de protección a la privacidad.

- **Demuestran la efectividad de mecanismos de co-regulación**: En el largo plazo, participar en el sistema y en códigos de conducta obligatorios puede ayudar a demostrar la viabilidad de implementar medidas de protección a la privacidad a través de la adopción de esquemas de responsabilidad flexibles.

Algunas conclusiones…

- Perspectiva empresarial: transferencias internacionales suponen comercio. Hay que encontrar el equilibrio
- Transferencias **a** terceros países: artículos Ley y reglamento mexicanos
- Transferencias **de** terceros países: México es el tercer país en compañías de outsourcing de tratamiento de datos, en concreto de “call centers”.
- Necesidad de que haya otra base, además del consentimiento, para facilitar los flujos e intercambios, sin desproteger al titular.
  - Nivel adecuado: Siempre y cuando un país cumpla con los estándares de privacidad y tenga el reconocimiento de la Comisión se podrá realizar transferencias internacionales de datos.
  - Cláusulas contractuales: En el ámbito europeo se ha previsto la posibilidad de transferir datos a terceros Estados que no cuenten con un nivel adecuado de protección mediante la incorporación de cláusulas tipo que regulen la transferencia a Responsables y/o Encargados.
  - BCR: Se prevén la transmisión de información a empresas transnacioanles del mismo grupo que tienen los mismos estándares de protección.
  - USA: Se pueden realizar transferencias internacionales en general. No normatividad comprehensiva.
  - En el entorno de APEC se pueden realizar transferencias internacionales con respeto a las leyes de privacidad y estándares internacionales

Muchas gracias

XII ENCUENTRO
IBEROAMERICANO DE
PROTECCIÓN DE DATOS

Twitter: @DavaraAbogados