XI ENCUENTRO IBEROAMERICANO DE PROTECCION DE DATOS

15, 16 Y 17 OCTUBRE 2013

CARTAGENA DE INDIAS, COLOMBIA

CLOUD COMPUTING

Las garantías de los datos personales en la nube, ley aplicable, transferencias internaciones de datos y requerimientos de información por autoridades de terceros países

Jesús Rubí Navarrete

Adjunto al Director

Agencia Española de Protección de Datos

CLOUD COMPUTING

- **Modalidades de computación en nube:**
  - **Privada**
  - **Pública**
  - **Híbrida**
  - **Comunitaria**
- **Modalidades de servicios:**
  - **Infraestructura como servicio (IAAS)**
  - **Plataforma como servicio (PAAS)**
  - **Software como servicio (SAAS)**
- **Las modalidades de computación y las modalidades de servicios condicionan la aplicación de la LOPD**
- **Formular reflexiones generales que han de adaptarse a dichas modalidades**

POSICIÓN JURÍDICA DE LOS INTERVINIENTES

- **El cliente como responsable del tratamiento:**
  - **Decisión sobre la finalidad, contenido y uso del tratamiento (Art. 3.d) LOPD)**
    - **Decisión sobre optar por la computación en nube (total o parcial)**
    - **Decisión sobre la modalidad de computación en nube (en particular sobre TID)**
    - **Decisión sobre las modalidades de servicios de computación en nube**
  - **Responsabilidad sobre el tratamiento de los datos personales (no se desplaza la responsabilidad)**
  - **El CCP como encargado de tratamiento**

POSICIÓN JURÍDICA DE LOS INTERVINIENTES

- **Consecuencias de la posición jurídica de los intervinientes:**
  - **Ley aplicable: La ley nacional del responsable/cliente (art. 2.1.a) LOPD)**
  - **La fragmentación y encriptación de los datos**
  - **Garantías contractuales ex art. 12 LOPD**

CAMBIO DE PARADIGMA

- **La relación tradicional responsable/encargado (art. 12 LOPD) no responde al modelo cloud computing**
  - **Instrucciones del responsable al encargado**
  - **No comunicación a terceros ni siquiera para su conservación**
  - **Estipulación de las medidas de seguridad a implementar por el encargado**
  - **Destrucción o devolución de datos al término de la prestación**

CAMBIO DE PARADIGMA: SUBCONTRATACIÓN

- **Los criterios tradicionales en la subcontratación (art. 21.2 RLOPD y STS de 15 de julio de 2010) no responden al modelo cloud computing**
  - **Especificación de los servicios a subcontratar**
  - **Indicación de las empresas subencargadas**
  - **Autorización del responsable/cliente sobre los subencargados**
  - **Contrato entre encargados y subencargados**

CAMBIO DE PARADIGMA

- **Autonomía del CCP**
- **Contratos de adhesión**
- **Selección subencargados (proceso dinámico)**
- **Oferta de medidas de seguridad**
- **Opción sobre TID**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Diligencia exigible al responsable:**
  - **Velar por que el encargado reúna las garantías exigibles (art. 20.2 RLOPD)**
    - **Obtener información sobre las garantías del contrato conforme al art. 12 LOPD**
    - **Ejercer diligentemente su posición de responsable sobre el tratamiento de los datos de los interesados**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Diligencia exigible al encargado (de oficio):**
  - **Información detallada sobre la tipología de computación en nube y de servicios que ofrece (tipología de nube, tipología de servicios, participantes en la prestación de servicios, TID)**
  - **Información sobre medidas de seguridad (niveles de seguridad, auditoría, encriptación, incidencias de seguridad). Análisis funcional, no estrictamente formal**
  - **Información sobre portabilidad**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Instrucciones del responsable:**
  - **Selección del tipo de computación en nube y de los servicios a contratar**
  - **Decisión sobre los tratamientos que no se contratan al CCP (naturaleza de la información, posible pérdida de control,…)**
  - **Decisión sobre la información solicitada y/o ofrecida por el CCP**

MODULAR LA NORMATIVA APLICABLE: TRANSPARENCIA

- **Medidas de seguridad:**
  - **Auditoria externa e independiente (incluso cuando no se exijan medidas de seguridad de nivel medio)**
  - **Comunicación de las incidencias de seguridad que afecten al cliente/responsable (Notificación brechas de seguridad)**
- **Portabilidad (art. 20.3 RLOPD)**

MODULAR LA NORMATIVA APLICABLE: SUBENCARGADO

- **Autorización previa sobre empresas subencargadas**
  - **Especificación funcional de los servicios susceptibles de subcontratación (p.ej. hosting)**
  - **Relación actualizada de entidades subencargadas (p.ej. Accesible en sitio web con indicación de países en que opera)**
  - **Tipología de garantías a exigir (incluidas TID)**
- **Contratos jurídicamente vinculante en todos los procesos de tratamiento, conforme a la ley aplicable (responsable/encargado. Encargado/subencargado)**
- **Posibilidad de actuación de la AEPD**

ESCENARIOS DE TRANSFERENCIAS INTERNACIONALES

- **NIVEL ADECUADO DE PROTECCIÓN**

  - establecido por Decisión de la Comisión Europea

  - Suiza, Argentina, Canadá, Guernsey, Isla de Man,

  Jersey, Andorra, Israel y Uruguay

  ENTIDADES DE EEUU ADHERIDAS A PUERTO SEGURO/SAFE HARBOR

- **TERCEROS PAÍSES (Clausulas contractuales, BCR,s)**

SITUACIÓN EN ESPAÑA

- Consulta pública
- Consejo General Abogacía Española
  - Recomendaciones prácticas
  - Síntesis
- Sector financiero
  - Sugerencias
- Universidades
  - Informe con recomendaciones

Guía y Orientaciones sobre Cloud Computing

- Introducción sobre cloud computing
- Tipos de cloud computing (neutralidad)
- Portabilidad (facilidad para transferir datos y aplicaciones de un proveedor a otro)
- Localización
  - Subcontratación
  - Localización de los recursos para la prestación del servicio (TID)

Aspectos destacados

- **Transparencia**
  - **Oferta de información sobre donde, cuando y quien procesa datos**

- **RIESGOS**
  - **Falta de transparencia**
  - **Falta de control**

Aspectos destacados

- **ESTRATEGIA PARA EL CLIENTE**
  - **Evaluar los tratamientos y la sensibilidad de los datos:**
    - **Análisis de los tratamientos a transferir a la nube**
  - **Verificación de las condiciones de prestación del servicio (aspectos tecnológicos, económicos y legales)**
    - **Lista de control (12 preguntas)**

Orientaciones para prestadores de servicios

- **Desequilibrio entre las partes**

- **Posición jurídica de las partes**
  - **Responsable**
  - **Encargado**
  - **Ley aplicable (LOPD)**

- **Diligencia**

- **Transparencia**
  - **Atender solicitudes de información del cliente (remisión a preguntas de la guía)**
  - **Ofrecer información "de oficio"**
  - **Valoración por AEPD**

Orientaciones para prestadores de servicios

- Garantías exigibles a los “partners”
- Modulación de las garantías tradicionales
- Portabilidad
- TID
- Ejercicio de derechos ARCO
- Administraciones públicas

- ORIENTACIONES A TENER EN CUENTA
  - Revisar sus contratos
  - Adaptarlos, en su caso, informando a sus clientes
  - Ser conscientes de que pueden ser responsables por incumplimiento

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es