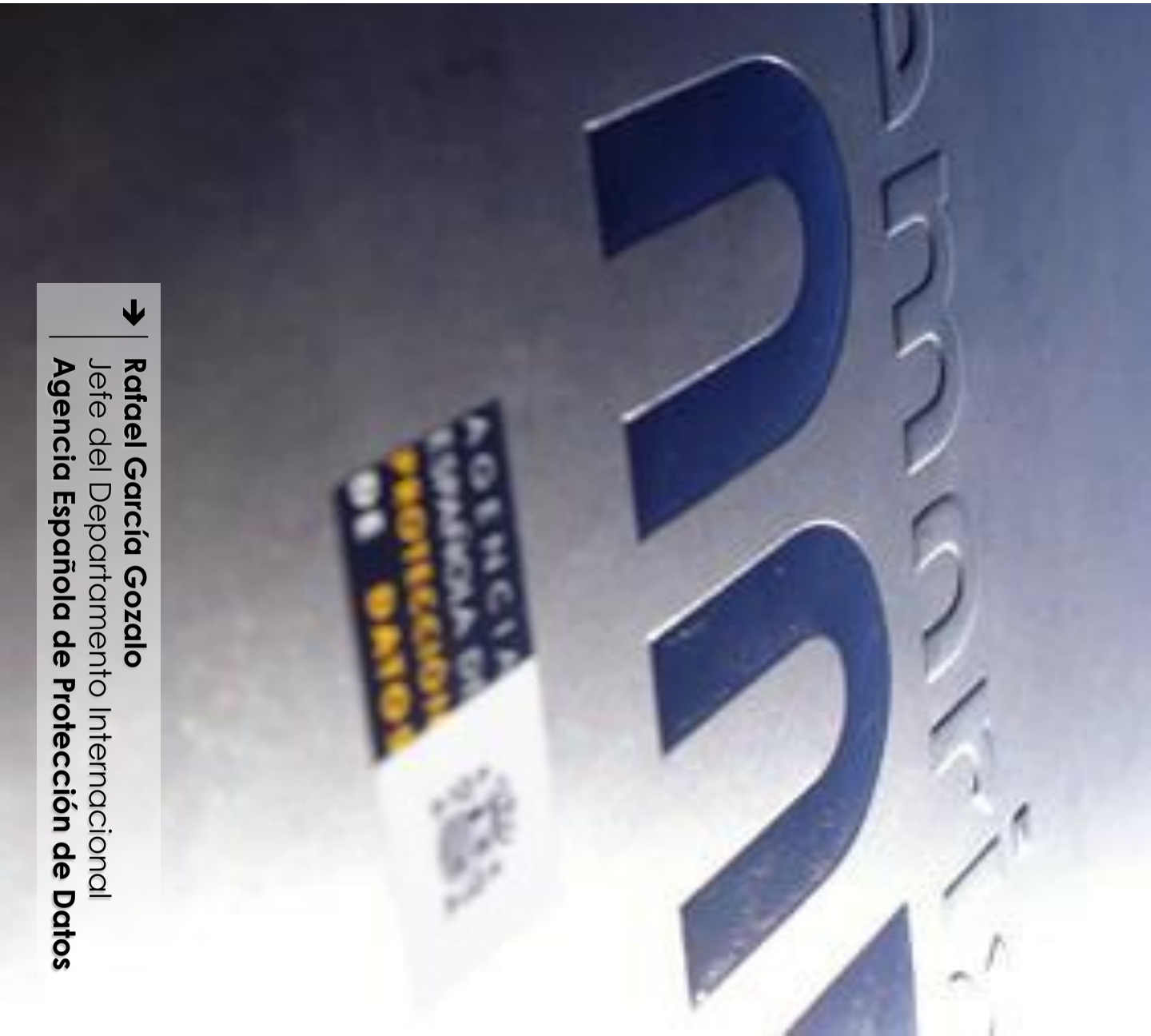
Computación en la Nube y Redes Sociales

Aspectos de Protección de Datos



Rafael García Gozalo
Jefe del Departamento Internacional
Agencia Española de Protección de Datos

Computación en Nube

- **Modalidades de computación en nube:**
  - **Privada**
  - **Pública**
  - **Híbrida**
  - **Comunitaria**
- **Modalidades de servicio:**
  - **Infraestructura como servicio (IAAS)**
  - **Plataforma como servicio (PAAS)**
  - **Software como servicio (SAAS)**
- **Las modalidades de computación y las modalidades de servicio condicionan la aplicación de la LOPD**

Posición jurídica de los participantes

- El cliente como responsable del tratamiento
  - Decisión sobre la finalidad, contenido y uso del tratamiento
    - 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
- El prestador como encargado de tratamiento

Consecuencias de la posición jurídica de los participantes

- Ley aplicable: Ley nacional del responsable/cliente (Salvo medidas de seguridad en otro EM UE)
- Inexistencia de obligación de informar a los interesados
- Garantías contractuales ex art. 12 LOPD

Conceptos clásicos

La relación tradicional responsable/encargado (art. 12 LOPD)

- 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

Criterios tradicionales en la subcontratación

- Especificación de los servicios a subcontratar
- Indicación de las empresas subencargadas
- Autorización del responsable/cliente sobre los subencargados
- Contrato entre encargados y subencargados

Nuevas condiciones

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

Nuevas interpretaciones

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
    - Ejercicio de derechos ARCO
    - Responsabilidad por daños

Nuevas interpretaciones

Diligencia exigible al encargado (por defecto)

- **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**

Nuevas interpretaciones

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 prestador (naturaleza de la información, posible pérdida de control,…)
- Decisión sobre la información solicitada y/o ofrecida por el prestador
- Selección del prestador

Nuevas interpretaciones

- **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
- **Portabilidad (art. 20.3 RLOPD)**
  - **Devolución o migración** a un nuevo prestador de servicios designado por el responsable

Nuevas interpretaciones

- **Autorización "previa" sobre empresas subencargadas**
  - Especificación funcional de los servicios susceptibles de subcontratación
  - Especificación de los niveles de calidad exigibles
  - 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 vinculantes en todos los procesos de tratamiento, conforme a la ley aplicable (Responsable/Encargado. Encargado/Subencargado)**
- **Posibilidad de actuación de la AEPD**

Transferencias Internacionales

- País adecuado → Contrato de prestación de servicios
- Contrato basado en Decisión 2010/87/UE – cláusulas contractuales tipo de responsable (cliente CC) a encargado (prestador SCC)
  - Ofrecen garantías en la transferencia de EEE al tercer país
  - Cláusula 11, subcontratación del encargado – importador
  - Encadenamiento de garantías de protección de datos
  - Autorización y conocimiento de la subcontratación por parte del Responsable
  - Información de los subencargados disponible para la AEPD
- BCR → válidas para movimiento intra-grupo → Nube privada
- BPR para encargados → En desarrollo

Redes sociales

¿Quién es el responsable del tratamiento?

- Los **proveedores de SRS son responsables del tratamiento** de datos en virtud de la Directiva relativa a la protección de datos
- Los **proveedores de aplicaciones también pueden ser** responsables del tratamiento de datos
- En la mayoría de los casos, los **usuarios se consideran personas interesadas**
- La Directiva no impone las obligaciones de un responsable del tratamiento de datos a una persona que trata datos personales «en el ejercicio de actividades exclusivamente personales o domésticas»

Redes sociales

¿Quién es el responsable del tratamiento?

- En algunos casos, la exención doméstica puede no cubrir las actividades de un usuario de SRS
  - Si actúa en nombre de una empresa o de una asociación o como una plataforma con fines comerciales, políticos o sociales
  - Un gran número de contactos puede indicar que no se aplica la excepción doméstica
  - Si un usuario decide ampliar el acceso más allá de los «amigos» elegidos, asume las responsabilidades de un responsable del tratamiento de datos

Redes sociales

¿Quién es el responsable del tratamiento?

"Si un usuario de SRS actúa en nombre de una empresa o de una asociación o utiliza el SRS principalmente como una plataforma con fines comerciales, políticos o sociales, la exención (domestica) no se aplica. En este caso, el usuario asume la plena responsabilidad de un responsable del tratamiento de datos que revela datos personales a otro responsable del tratamiento de datos (SRS) y a terceros (otros usuarios de SRS o incluso, potencialmente, a otros responsables del tratamiento de datos que tienen acceso a ellos). En tales circunstancias, el usuario necesita el consentimiento de las personas interesadas u otra base legítima que figure en la Directiva relativa a la protección de datos" (WP 163)

Un responsable "especial"

- El uso se limita exclusivamente al alta en la red social y al empleo de las herramientas que en ella existen
- No existe ninguna capacidad de decisión sobre la estructura, ordenación o gestión material de los datos distinta de la propia de la red social
- No se incorporan datos personales a recursos propios
- No se utiliza ningún recurso de indexación o se integra una aplicación propia
- No se contrata ninguna prestación de servicios para el desarrollo o mantenimiento del espacio con el proveedor de la red social
- No se pactan condiciones específicas de uso con el proveedor: como análisis del comportamiento, seguimiento o elaboración de perfiles de usuario, o publicidad comportamental

Tratamiento → Principios y obligaciones derivados del artículo 5 LOPD

- Ubicar una información básica en el espacio de la cuenta que facilite la red social con detalles sobre la identidad y localización del responsable, finalidad que se persigue, formas de ejercicio de los derechos…
- Procedimiento de bienvenida a nuevos amigos con un mensaje de correo-e que incluya esta información
- Enlazar a políticas de privacidad corporativas
- Informar en particular sobre posible
  - Utilización de los datos con fines de comercialización directa
  - Distribución de datos a categorías específicas de terceros
  - Uso de datos sensibles

Consentimiento

- En principio el consentimiento se manifiesta cuando se solicita “hacerse amigo de”
- El consentimiento únicamente afecta a los datos de la persona que se agrega nunca a otros relacionados con él
- La posible existencia de excepciones a la regla
- del consentimiento deberán examinarse caso por caso y con pleno respeto a la regulación
- Un perfil abierto “no implica consentimiento”

Derechos

Rigen los derechos de acceso, rectificación, cancelación y oposición. No obstante

- El contenido del derecho de acceso vendrá definido por las posibilidades que ofrezca la red
- El derecho de oposición, rectificación y cancelación se encontrará modulado

  El responsable del tratamiento debería satisfacerlo sobre aquellos aspectos de la aplicación que se encuentren bajo su control (modificar o eliminar datos un comentario del propio muro)
- La rectificación de aspectos relativos al perfil del usuario normalmente se ejercen ante el SRS
- La cancelación u oposición cuando consiste en "dejar de ser amigos" podría ser ejercida por ambas partes

Límites

- **Principio de finalidad como límite infranqueable** definido por
  - Condiciones de uso de la red social.
  - Información disponible y efectivamente facilitada "al hacerse amigos"
- La **incorporación de datos**, como la dirección de e-mail, a los propios sistemas constituye un **nuevo tratamiento** sujeto a la LOPD
- El uso de aplicaciones de terceros o propias insertas en el entorno de la red social obliga al cumplimiento de la legislación vigente cuando dé lugar al tratamiento de datos
- **Rigen los principios de seguridad y secreto** para cualquier usuario del responsable del tratamiento pero deberán adaptarse a las condiciones propias del entorno y afectarán únicamente a los tratamientos efectivamente realizados
- El estímulo a los usuarios para "difundir" mediante la estrategia de "enviar a un amigo" o "invitar a más amigos", en particular cuando opere algún tipo de bonificación **puede constituir una actividad sujeta a las reglas vigentes en materia de protección de datos personales**

¡Gracias por su atención!

rgarciag@agpd.es
www.agpd.es

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS