Segunda Parte:
Principios aplicables al tratamiento de datos personales

Marcos A. López Suárez

El tratamiento de datos de carácter personal ha de realizarse de acuerdo con unas reglas o principios que se plasman en diversos preceptos del Reglamento de la Unión Europea (arts. 5 y concordantes):

- Calidad
- Licitud [consentimiento]
- Lealtad
- Transparencia [información]
- Responsabilidad proactiva [Seguridad]
- Secreto

1. Calidad de los datos

- **Finalidad**: los datos sólo pueden ser recogidos para el cumplimiento de una finalidad determinada, explícita y legítima
  - Los datos que se recogen deben ser "adecuados, pertinentes y no excesivos" en relación con la finalidad ("minimización de datos")
  - Los datos deben cancelarse cuando dejen de ser necesarios o pertinentes para la finalidad elegida; no obstante, podrán conservarse durante períodos más largos siempre que se traten **exclusivamente** con fines de archivo en interés público, fines de investigación –científica o histórica- o fines estadísticos
- **Utilización no abusiva**: no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos
  - El tratamiento con fines de archivo en interés público, fines de investigación –científica o histórica- o fines estadísticos no se considerará incompatible con los fines iniciales ("limitación de la finalidad")
- **Exactitud**: Los datos de carácter personal serán exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado
  - Cuando los datos los facilita el interesado, se consideran veraces
  - La inexactitud de los datos obliga al responsable a cancelarlos (o rectificarlos)

2. Licitud (I)

- Como regla general, el tratamiento de los datos de carácter personal requerirá el **consentimiento** "inequívoco" de su titular.
- En su defecto, se considera que el tratamiento es igualmente lícito si es necesario para:
  1. La ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales
  2. **El cumplimiento de una obligación legal aplicable al responsable**
  3. Proteger intereses vitales (del interesado u otra persona)
  4. **El cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento**
  5. La satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero, siempre que no prevalezcan derechos y libertades fundamentales del interesado ("expectativas razonables").

  La base del tratamiento indicado en 2 y 4 deberá ser establecida por "ley" (cfr. art. 6.3 Reglamento UE). Con todo, no se exige un acto legislativo adoptado por un parlamento, pero la base jurídica o medida legislativa ha de ser clara y precisa y su aplicación previsible para sus destinatarios.

2. Licitud II

- Datos obtenidos de “fuentes de acceso público”
  - No es necesario consentimiento
  - Información: remisión

*****

El responsable debe ser capaz de demostrar que el interesado ha dado su consentimiento a la operación de tratamiento. De ahí que deba proporcionarle un **modelo de declaración** de consentimiento elaborado previamente con una **formulación inteligible y de fácil acceso** que emplee un **lenguaje claro y sencillo**, y que no contenga cláusulas abusivas.

El consentimiento no puede considerarse libremente prestado si el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

Se presume que el consentimiento no es libre cuando no permite autorizar por separado las distintas operaciones de tratamiento pese a ser adecuado al caso concreto o cuando el cumplimiento de un contrato sea dependiente del consentimiento, aun cuando éste no sea necesario para dicho cumplimiento.

3. Lealtad

- El Reglamento U.E. se limita a señalar que los datos serán tratados de manera “leal”, sin concretar en qué consiste la lealtad.

- Con todo, atendiendo a lo previsto en el art. 4 LOPD, atinente a la calidad de los datos, cabría entender que el contenido de dicho principio se concreta en la prohibición de la recogida de datos por medios fraudulentos, desleales o ilícitos.

4. Transparencia (I)

- El responsable del tratamiento deberá facilitar al interesado, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, la información sobre las condiciones de los tratamientos.
- **Forma:** Por escrito u otros medios (v. gr. los electrónicos o iconos normalizados) en el momento de la recogida.
  - Si el interesado lo solicita, también podrá facilitarse verbalmente, siempre que se demuestre la identidad del interesado por otros medios.
- **Contenido mínimo común,** con independencia del origen de los datos [similar, en parte, al previsto en el art. 5 LOPD]:
  - Identidad y datos de contacto del responsable del tratamiento
  - Datos de contacto del delegado de protección de datos, en su caso
  - Los intereses legítimos del responsable o de un tercero, en su caso
  - Finalidad del tratamiento y base jurídica de éste
  - Los destinatarios de los datos
  - La intención de realizar transferencias internacionales
  - Plazo de conservación de los datos o criterios para determinarlo
  - Derechos (acceso, rectificación, "supresión", oposición, "limitación del tratamiento" y "portabilidad de los datos")

4. Transparencia (II)

- Derecho a revocar el consentimiento
- Derecho a presentar una reclamación ante la autoridad de control
- La existencia de decisiones automatizadas y en tal caso información sobre la lógica aplicada, importancia y consecuencias del tratamiento para el interesado
- En caso de tratamientos ulteriores, información previa sobre los fines si fueran distintos de aquellos para los que se obtuvieron los datos

Contenido adicional…

si los datos han sido facilitados por el propio interesado

- Si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato y si el interesado está obligado a facilitar los datos y está informado de las consecuencias de no facilitarlos

si los datos no han sido obtenidos del propio interesado

- Las categorías de datos personales de que se trate
- La fuente de la que proceden los datos y, en su caso, si proceden de fuentes de acceso público
  - **Plazo:**
  - "Razonable"; a más tardar dentro de un mes de haber sido obtenidos los datos
  - Si los datos se utilizan para comunicación ya sea con el interesado ya sea con un tercero: a más tardar en el momento de la primera comunicación

4. Transparencia (III)

- **Excepciones a la obligación de informar**
  - **En todo caso** cuando el interesado ya disponga de la información
  - **Además,** si los datos no han sido obtenidos del propio interesado, cuando:
    - La comunicación de la información resulte imposible o suponga un esfuerzo desproporcionado o pueda imposibilitar u obstaculizar gravemente el logro de los objetivos del tratamiento
    - La obtención o comunicación está expresamente establecida en la "ley"
    - Los datos deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional
- **Información "por capas"**
  - **Primera capa:** Información resumida sobre Responsable, Finalidad, Legitimación, Derechos, y, en su caso, Procedencia
  - **Segunda capa**: Información detallada susceptible de ser consultada en un hipervínculo

5. Seguridad de los datos (I)

- El responsable del tratamiento (o, en su caso, los encargados) deberán adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.
  - Infracciones flagrantes: historias clínicas en la basura, pérdida disco con datos contribuyentes británicos,…
- Enumeración ilustrativa:
  - Seudonimización y cifrado
  - Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento
  - Capacidad de restaurar la disponibilidad y el acceso a los datos en caso de incidente físico o técnico
  - Proceso de verificación, evaluación y valoración regulares de las medidas adoptadas
- A la hora de establecer las concretas medidas de seguridad deben tenerse en cuenta diversas variables:
  - El coste de la técnica
  - Los costes de aplicación
  - La naturaleza, el alcance, el contexto y los fines del tratamiento
  - Los riesgos para los derechos y libertades

5. Seguridad de los datos (II)

- Notificación de las violaciones de seguridad
  - A la autoridad de control: sin dilación y a más tardar 72 h. después de que se haya constatado la violación.
  - Al interesado: alto riesgo para sus derechos y libertades y sin dilación, salvo si el responsable ha adoptado...
    - medidas de protección técnicas y organizativas apropiadas (*v. gr.*, el cifrado, que haría ininteligible los datos personales para cualquier persona que no esté autorizada a acceder a ellos)
    - o medidas ulteriores que garanticen que ya no existe la probabilidad de que de "concretice" el riesgo…
    - o suponga un **esfuerzo desproporcionado** (comunicación pública).
- Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal
  - Nivel básico (datos de carácter personal)
  - Nivel medio (infracciones administrativas o penales, Hacienda Pública, servicios financieros y servicios de solvencia y crédito -registros de morosos-)
  - Nivel alto (datos especialmente protegidos -ideología, religión, creencias, origen racial, salud o vida sexual- y fines policiales)

6. Deber de secreto

- El responsable del fichero y quienes intervengan en el tratamiento de los datos están obligados al secreto profesional
- La obligación de secreto se refuerza en el Código Penal al penalizarse algunas conductas relativas a la protección de datos (arts. 197 a 200).