10ª sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

ORIENTACIONES DEL GT29 EN RELACIÓN CON EL RGPD
EL PAPEL DEL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

Rafael García Gozalo
Jefe del Departamento Internacional

Directrices y documentos de trabajo adoptados

Adoptados por GT29 y ratificados por CEPD

- Delegados de Protección de Datos
- EIPD y Tratamientos de Alto Riesgo
- Identificación de la Autoridad Principal
- Portabilidad

- Consentimiento
- Transparencia
- Decisiones individuales automatizadas y perfilado
- Notificación de quiebras de seguridad
- Elementos y Principios para BCR de responsables y encargados
- Adecuación
- Aplicación y determinación de multas administrativas
- Interpretación art. 30.5 RGPD

Adoptadas por CEPD

- Certificación (Pendiente de Consulta Pública)
- Excepciones para Transferencias Internacionales

Directrices CONSENTIMIENTO

- El consentimiento como una más de las bases jurídicas
- Necesidad de respetar principios del tratamiento, especialmente los de lealtad, necesidad y proporcionalidad
- Presunción de consentimiento no libre si se vincula a ejecución de un contrato o prestación de servicio →
  Tratamiento necesario para ejecución de un contrato no requiere consentimiento
- Validez del consentimiento en situaciones en que no puede rechazarse sin perjuicio
- Relación con Directiva ePrivacy

Directrices CONSENTIMIENTO

- Consentimiento granular (específico para finalidades específicas)
- Información mínima →
  - Identidad del responsable
  - Finalidad
  - Derecho a retirar consentimiento
  - Existencia de decisiones automatizadas
  - Posible riesgo por TI sin garantías adecuadas
- Distinción de "inequívoco" y "explícito"
- Retirar consentimiento debe ser tan sencillo como darlo
- Consentimiento de niños y para finalidades de investigación científica
- Consentimientos obtenidos en el marco de la Directiva 95/46

Directrices TRANSPARENCIA

- Transparencia incluye tres áreas →
  - Cómo se proporciona información sobre tratamiento a interesados
  - Cómo facilitan responsables ejercicio de derechos
  - Cómo se comunican los responsables con interesados sobre el ejercicio de derechos
- Importancia de objetivo de transparencia y relación con principio de "accountability" → el interesado debe ser capaz de determinar el alcance y las consecuencias de un tratamiento, incluidos sus riesgos, las salvaguardas implantadas y sus derechos
- Importancia de concisión, accesibilidad e inteligibilidad de la información. Uso de "lenguaje claro y sencillo" → Evitar uso de expresiones como →
  - "Podemos tratar sus datos para…"
  - "Entre otras finalidades…"
  - "Usamos sus datos para ofrecerle servicios personalizados"

Directrices TRANSPARENCIA

- Posibilidad de proporcionar información por escrito "o por otros medios"
- Formatos → Resolviendo la tensión entre cantidad y concisión de la información
  - Capas
  - Cuadros de mandos de privacidad
  - Avisos sucesivos…
- Información para tratamientos ulteriores
- Análisis de excepciones art. 14 →
  - Proporcionar información es imposible o requiere esfuerzo desproporcionado
  - Tratamiento recogido en ley nacional o EU
  - Secreto profesional → Un médico recibe información de un paciente sobre otras personas. No está obligado a informar a esas personas de que va a tratar sus datos, dado que le vincula el secreto profesional respecto a su paciente

Directrices DECISIONES AUTOMATIZADAS Y PERFILADO

- Distinción y análisis de conceptos →
  - Perfilado → importancia del objetivo de "evaluar" ciertos aspectos
  - Decisiones automatizadas
  - Decisiones basadas únicamente en tratamiento automatizado, incluidos perfiles, que producen efectos legales o que afectan significativamente de forma similar a los interesados
- Aplicación de principios generales a perfilado y decisiones automatizadas
  - Principio de lealtad y transparencia → importancia de información en perfilado
  - Tratamientos para finalidades ulteriores
  - Principio de minimización
  - Exactitud
  - Conservación
- Bases jurídicas →
  - Dependiendo de las circunstancias, todas las bases jurídicas son posibles
  - Importancia de ponderación en aplicación de "interés legítimo" → detalle del perfilado, amplitud, impacto, salvaguardas

Directrices DECISIONES AUTOMATIZADAS Y PERFILADO

- Derechos →
  - Acceso a datos y perfiles
  - Posibilidad de rectificar perfiles (además de datos originales) si datos de partida o algoritmos se prueban erróneos
  - Derecho de oposición incluye específicamente perfilado
- Decisiones individuales basadas solamente en tratamiento automatizado, incluidos perfiles (art. 22)
  - Art. 22 debe interpretarse como prohibición de tomar ese tipo de decisiones
  - Existen excepciones, que incluyen la necesidad de salvaguardas
  - "Que afectan significativamente de modo similar" →
    - Afectan significativamente a las circunstancias, comportamiento o elecciones del individuo
    - Tienen un impacto permanente o prolongado en el interesado
    - Conducen a la discriminación o exclusión
    - Incluso en el terreno publicitario
- Prohibición, con excepciones, de decisiones art. 22 en relación con niños

Directrices NOTIFICACION DE QUIEBRAS

- Análisis de la definición de quiebra →
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Importancia de protección tecnológica adecuada y de medidas organizativas para establecer inmediatamente si se ha producido una quiebra de seguridad
- El responsable "tiene constancia" de que se ha producido una quiebra cuando tiene "razonable grado de certeza de que ha ocurrido un incidente de seguridad que conduzca a que datos personales se hayan visto comprometidos" → Distinción entre notificar quiebra y proporcionar información sobre la quiebra
- Notificación a "autoridad líder" en quiebras que afectan a tratamientos transfronterizos, en el sentido del RGPD

Directrices NOTIFICACION DE QUIEBRAS

- Notificación de quiebras →
  - A AC No es necesaria si es improbable que exista riesgo para derechos y libertades
  - A interesados si es probable que entrañe un alto riesgo para derechos y libertades
- Daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como
  - Pérdida de control sobre sus datos personales o restricción de sus derechos
  - Discriminación, usurpación de identidad, pérdidas financieras
  - Daño para la reputación,
  - Cualquier otro perjuicio económico o social significativo…
- Factores para evaluar el riesgo →
  - Tipo de quiebra
  - Naturaleza, sensibilidad y volumen de datos afectados
  - Facilidad de identificación de las personas afectadas
  - Gravedad de las consecuencias de la quiebra
  - Características específicas de personas afectadas
  - Características de responsable
- Excepción de notificación a AC si datos son ininteligibles para terceros, bajo determinadas condiciones que afectan al nivel de riesgo para interesados
- Necesidad de que notificación a interesados sea efectiva

Directrices de aplicación de multas administrativas

- Documento dirigido a guiar a AC
- No es una guía sobre fijación de cuantías
- Analiza factores atenuantes y agravantes de art. 83.2 RGPD para establecer si la medida correctiva a aplicar ante una infracción ha de ser la multa, otra medida correctiva o ambas
- Las medidas correctivas previstas son →
  - Advertencias
  - Apercibimientos
  - Ordenes de atender derechos de interesados o de realizar tratamientos de acuerdo con RGPD, de una manera y en plazos determinados
  - Ordenar comunicación de quiebras a interesados
  - Imponer limitaciones temporales o definitivas de un tratamiento
  - Retirar certificaciones
  - Ordenar suspensión de TI
- Infracciones al RGPD deberían conducir a la imposición de "sanciones equivalentes"
- Necesario en contexto de falta de experiencia de muchas AC y de diferentes aproximaciones de acuerdo a ordenamientos y tradiciones nacionales
- Criterios aplicables tanto interna como externamente
- Reacción ante infracción ha de ser "eficaz, proporcionada y disuasoria"
- Multas no deben considerarse una solución para casos extremos, pero tampoco usarse de una forma que devalúe su eficacia como herramienta en manos de AC

El Comité Europeo de Protección de Datos

- Establecido y funcional el 25 de mayo de 2018
- Relevancia de funciones del Comité
  - Recomendaciones, directrices y buenas prácticas
  - Dictámenes autorizando decisiones de AC (art. 64)
  - Decisiones vinculantes resolviendo conflictos entre AC (art. 65)
- Documentos en preparación →
  - Directrices sobre aplicación territorial del RGPD (art. 3)
  - Documento sobre límites al uso de la base jurídica 6.1.b RGPD
- Página web → edpb.europa.eu

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS

www.aepd.es

@AEPD_es #10SesiónAEPD

10 sesión anual abierta de la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS