SEMINARIO

LOS NUEVOS RETOS DE LA PRIVACIDAD.

EL TRATAMIENTO MASIVO DE LOS DATOS PERSONALES.

PANEL 5

GESTIÓN DE LOS RIESGOS.

NUEVOS ENFOQUES PROACTIVOS

JESÚS RUBÍ NAVARRETE

ADJUNTO A LA DIRECCIÓN

3-5 NOVIEMBRE 2015

MONTEVIDEO (URUGUAY)

RGTP/UE Motivos/objetivos para la reforma

- Evolución tecnológica, especialmente Internet, plantea nuevos retos para la proteción de datos
- Gobalización: problemas de determinación de ley aplicable y de competencia
- El marco actual ha dado lugar a fragmentación de regímenes jurídicos dentro de la UE
- Necesidad de mayor seguridad jurídica
- Desaparición de antiguos "pilares" hace necesario integrar protección de datos en los ámbitos policia y justicia

Características

El instrumento principal es un Reglamento

- Directamente aplicable
- Extenso y detallado (91 artículos, frente a 34 de actual Directiva)
- Marco uniforme para toda la UE
- Limitado margen de desarrollo para EEMM
- Gran capacidad de desarrollo y aplicación para COM

Responsabilidad activa del Responsable ("Accountability")

- El Reglamento prevé que los responsables adoptarán políticas y pondrán en práctica medidas para asegurar y estar en condiciones de demostrar que los tratamientos que realizan son conformes al Reglamento
- En otros términos → el Reglamento
  - Considera insuficiente "no incumplir"
  - Incluye obligaciones de "cumplir" dirigidas a evitar o paliar infracciones
- Es el enfoque de la "accountability", aunque el listado de medidas incluye algunas típicas de accountability y otras que son más propias del enfoque prescriptivo clásico
- La no existencia de estas medidas es sancionable

Responsabilidad activa del Responsable ("Accountability")

Tipos de medidas (Art. 22)

- Mantener la documentación prevista en artículo 28 (obligación que sustituye a notificación)
- Aplicar medidas de seguridad adecuadas
- Medidas de Protección de Datos en el Diseño
- Medidas de Protección de Datos por Defecto
- Llevar a cabo Evaluaciones de Impacto de Protección de Datos (PIA)
- Solicitar autorización previa o realizar consultas previas con APD en los casos previstos
- Designación Delegado Protección de Datos (DPD)
- Verificación de la eficacia de esas medidas por parte, salvo que sea desproporcionado, de auditores independientes, externos o internos

Documentación

Art. 28

"2. La documentación deberá contener, como mínimo, la información siguiente:

a) el nombre y los datos de contacto del responsable del tratamiento, o de cualquier corresponsable o coencargado del tratamiento, y del representante, si lo hubiera;

b) el nombre y los datos de contacto del delegado de protección de datos, si lo hubiera;

c) los fines del tratamiento, en particular los intereses legítimos perseguidos por el responsable del tratamiento, cuando el tratamiento se base en el artículo 6, apartado 1, letra f);

d) una descripción de las categorías de interesados y de las categorías de datos personales que les conciernen;

e) los destinatarios o las categorías de destinatarios de los datos personales, incluidos los responsables del tratamiento a quienes se comuniquen datos personales por el interés legítimo que persiguen;

f) en su caso, las transferencias de datos a un tercer país o a una organización internacional, incluido el nombre de dicho tercer país o de dicha organización internacional y, en el caso de las transferencias contempladas en el artículo 44, apartado 1, letra h), la documentación de garantías apropiadas;

g) una indicación general de los plazos establecidos para la supresión de las diferentes categorías de datos;

h) la descripción de los mecanismos contemplados en el artículo 22, apartado 3.

3. El responsable y el encargado del tratamiento, así como el representante del responsable, si lo hubiera, pondrán la documentación a disposición de la autoridad de control, a solicitud de esta."

No previsión específica para PYMES

Medidas de Seguridad

Art. 30

"1. El responsable y el encargado del tratamiento implementarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en relación con los riesgos que entrañe el tratamiento y la naturaleza de los datos personales que deban protegerse, habida cuenta de las técnicas existentes y de los costes asociados a su implementación.

2. A raíz de una evaluación de los riesgos, el responsable y el encargado del tratamiento adoptarán las medidas contempladas en el apartado 1 a fin de proteger los datos personales contra su destrucción accidental o ilícita, o su pérdida accidental, y de impedir cualquier forma de tratamiento ilícito, en particular la comunicación, la difusión o el acceso no autorizados o la alteración de los datos personales."

Medidas de Seguridad

Art. 30

"3. La Comisión estará facultada para adoptar actos delegados de conformidad con lo dispuesto en el artículo 86, a fin de especificar los criterios y condiciones aplicables a las medidas técnicas y organizativas contempladas en los apartados 1 y 2, incluida la determinación de cuáles son las técnicas existentes, para sectores específicos y en situaciones de tratamiento de datos específicas, habida cuenta en particular de la evolución de la tecnología y de las soluciones de privacidad desde el diseño y la protección de datos por defecto, salvo que sea de aplicación el apartado 4.

4. La Comisión podrá adoptar, en su caso, actos de ejecución para especificar los requisitos establecidos en los apartados 1 y 2 en distintas situaciones, en particular a fin de:

a) impedir cualquier acceso no autorizado a datos personales;

b) impedir cualquier forma no autorizada de comunicación, lectura, copia, modificación, supresión o cancelación de datos personales;

c) garantizar la verificación de la legalidad de las operaciones de tratamiento."

Quiebras de Seguridad

- Novedad (salvo antecedente de Directiva "e-Privacy")
  - Obligación de notificar las "violaciones de datos" (Art. 31-32)
- La violación de datos se define como

  "Una quiebra en la seguridad que conduce a la destrucción, pérdida, alteración, comunicación o acceso no autorizados, de forma accidental o ilegal, de datos transmitidos, almacenados o tratados de cualquier otra forma"
- Se prevé notificación a:
  - APD
  - Interesados
- La obligación incumbe siempre al Responsable, aunque el Encargado está obligado a cooperar para que se realice eficazmente (Cloud computing)

Notificación a APD

- Sin demora y a más tardar en 24 horas desde que se haya tenido constancia. Más tarde, justificación motivada
- Reglamento prevé contenido mínimo de notificación
  - a) naturaleza de la violación de datos personales, en particular las categorías y el número de interesados afectados, y las categorías y el número de registros de datos de que se trate;
  - b) comunicar la identidad y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
  - c) recomendar medidas tendentes a atenuar los posibles efectos negativos de la violación de datos personales;
  - d) describir las consecuencias de la violación de datos personales;
  - e) describir las medidas propuestas o adoptadas por el responsable del tratamiento para poner remedio a la violación de datos personales.
- Documentación de todas las violaciones
- Problema → No se establece umbral a partir del que notificar, lo que puede conducir al colapso del sistema, aunque se prevé que la COM pueda determinarlo

Notificación a interesados

- Quiebra afecta negativamente a la protección de datos o a la privacidad (definición cuestionable → Todas lo hacen)
- Sin demora injustificada, después de a APD
- También se prevé contenido mínimo, incluyendo posibles medidas paliativas
- Excepción: Implementación de medidas de protección tecnológica adecuada a los datos afectados, a satisfacción de la APD, que haga ininteligibles los datos a terceros no autorizados (p.ej.: datos encriptados)
- APD puede obligar a notificar a interesados

Protección de datos desde el diseño y por defecto

- **Privacidad desde el Diseño**
  - Implementación en el momento de determinación de los medios del tratamiento y en el tratamiento propiamente dicho medidas y procedimientos técnicos y organizativos apropiados para cumplir el Reglamento y proteger los derechos de los interesados
  - Condiciones: Técnicas existentes y costes de implementación
- **Protección de datos por Defecto**
  - Minimización de los datos para cada finalidad
  - Conservación mínima para finalidad
  - Garantía de que, por defecto, no sean accesibles a un número indeterminado de personas (caso típico de configuración de privacidad para redes sociales)

Evaluación de impacto

- Deberá realizarse cuando los tratamientos previstos presenten riesgos específicos para los derechos y libertades de los interesados, entre otros casos, cuando:
  - Persigan una evaluación sistemática y exhaustiva de datos personales o analizar o predecir características de una persona
  - Procesen a gran escala información sensible destinada a tomar medidas sobre personas concretas
  - Se efectúe video-vigilancia a gran escala
  - Procesen a gran escala datos de niños, datos genéticos o datos biométricos
  - Deban ser autorizados por APD según Art. 34
- La obligación incumbe tanto al Responsable como al Encargado
- El Reglamento prevé un contenido mínimo de la evaluación
- Como novedad, se prevé que habrá de recabarse la opinión de los interesados

Evaluación de impacto- Consultas

Art. 34

- **Determinadas autorizaciones para Transferencias Internacionales**
- ***"2. El responsable o el encargado del tratamiento que actúe por cuenta de aquel deberán consultar a la autoridad de control antes de proceder al tratamiento de datos personales (…) cuando:***

  a) una evaluación del impacto en la protección de los datos, tal como dispone el artículo 33, indique que es probable que las operaciones de tratamiento, por su naturaleza, alcance o fines, entrañen un elevado nivel de riesgos específicos; o

  b) la autoridad de control considere necesario proceder a una consulta previa en relación con las operaciones de tratamiento que probablemente entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance y/o fines, y hayan sido especificadas con arreglo al apartado 4.

- ***3. Cuando la autoridad de control considere que el tratamiento previsto no es conforme con lo dispuesto en el presente Reglamento, en particular cuando los riesgos no estén suficientemente identificados o atenuados, prohibirá el tratamiento previsto y presentará propuestas apropiadas para poner remedio a esta falta de conformidad."***

Evaluación de impacto- Consultas

Art. 34

- *"4. La autoridad de control establecerá y publicará una lista de las operaciones de tratamiento que deben ser objeto de una consulta previa de conformidad con lo dispuesto en el apartado 2, letra b). La autoridad de control comunicará estas listas al Consejo Europeo de Protección de Datos.*
- *"7. Los Estados miembros consultarán a la autoridad de control en el marco de la elaboración de una medida legislativa antes de su adopción por los parlamentos nacionales o de una medida basada en una medida legislativa que defina la naturaleza del tratamiento, con el fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de atenuar los riesgos para los interesados."*

Delegado de Protección de Datos

- Deberá existir en:
  - Administraciones Públicas
  - Empresas de 250 o más empleados
  - Actividades que por su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados
- En responsables o encargados
- Grupo de empresas → Posibilidad de un solo DPD
- Administraciones Públicas → Un solo DPD para varias entidades
- En otros casos, los responsables, encargados o las asociaciones u organismos que agrupen a categorías de responsables o encargados pueden designarlo

Características

- Ha de reunir cualidades profesionales, en particular, conocimiento de legislación de PD
- Su función ha de ser compatible y no suponer conflicto de intereses con otras actividades profesionales
- Puede mantener relación laboral o de contrato de servicios
- Mandato de 2 años prorrogables. Sólo removible si deja de reunir requisitos para la función
- Comunicación de su identidad a APD y al público
- Derecho de acceso por los interesados
- Independencia
- Información directa a la dirección
- Respaldo y recursos

Delegado de protección de datos

Funciones

- Informar y asesorar a responsable y encargado, documentando esa actividad
- Supervisar la puesta en práctica de las políticas de protección de datos, incluidas la formación y la auditoría
- Supervisar la aplicación del Reglamento en lo relativo a PbD, PbDef y derechos de los interesados
- Asegurar la existencia y mantenimiento de documentación obligatoria
- Supervisar gestión de quiebras de seguridad
- Supervisar la realización de Evaluaciones de Impacto y la solicitud de autorizaciones o consultas que se requieran
- Supervisar respuestas a requerimientos de APD
- Cooperar con la APD en el marco de sus tareas
- Actuar como punto de contacto para la APD

Certificaciones

- Los Estados miembros y la COM promoverán la creación de
  - mecanismos de certificación en materia de protección de datos
  - sellos y marcas de protección de datos
- Objetivo → Facilitar a los interesados evaluar rápidamente el nivel de protección de datos que ofrecen responsables y encargados
- Inclusión positiva, pero quedan cuestiones abiertas →
  - ¿Quién establece los mecanismos en EEMM?
  - ¿Quién certifica?
  - ¿Cómo se certifica el certificador?
  - ¿En qué medida participan Autoridades de Supervisión?
- Cuestiones que podrá resolver la COM, que queda habilitada para adoptar
  - Criterios y requisitos aplicables a los mecanismos de certificación
  - Normas técnicas para los mecanismos de certificación y los sellos y marcas
  - Mecanismos para promover y reconocer los mecanismos de certificación y los sellos y marcas

Responsabilidad activa

- **Apoyo generalizado en Consejo a aplicar el criterio de "risk based approach" en obligaciones de responsables→**

Considerando 60 "Debe quedar establecida la responsabilidad del responsable en relación con cualquier tratamiento de datos personales realizado por él mismo o en su nombre. En particular, el responsable del tratamiento debe (…) estar obligado a aplicar las medidas oportunas y poder demostrar la conformidad de (…) las actividades de tratamiento con lo dispuesto en el presente Reglamento (...). Estas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

Responsabilidad activa

- **Problema → ¿Cómo medir riesgo y cómo guiar a responsables?**

***Considerando 60bis** "Dichos riesgos, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños físicos o morales, en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, perjuicio para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, cambio no autorizado de la seudonimización o cualquier otro perjuicio económico o social significativo; o en los casos en los que se prive a los interesados de sus derechos y libertades o de ejercer el control sobre sus datos personales; cuando los datos personales tratados revelen el origen étnico o racial, (lista de datos sensibles); cuando se evalúen aspectos personales, (…), con el fin de crear o utilizar perfiles personales; cuando se traten datos personales de personas vulnerables, en particular niños; cuando el tratamiento implique una gran cantidad de datos personales y afecte a una gran cantidad de interesados."*

***Considerando 60ter** "La probabilidad y la gravedad del riesgo deberá evaluarse en función de la naturaleza, ámbito, contexto y fines del tratamiento de datos. El riesgo deberá estimarse por medio de una evaluación objetiva, mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo elevado. Un riesgo elevado es un riesgo particular de perjuicio a los derechos y libertades de las personas físicas"*

Responsabilidad activa

Documentación

- **En PE → Se reduce la lista de elementos que deben documentarse, sustituyéndose por referencia genérica a *"documentación, actualizada periódicamente, que sea necesaria para cumplir los requisitos que se establecen en el presente Reglamento*."**

- **En Consejo→**
  - **Se mantiene listado amplio de elementos**
  - **Obligación no aplicable a PYMES (<250 empleados) salvo que realicen tratamientos de alto riesgo**

Responsabilidad activa

- Notificación de quiebras de seguridad en Consejo→
  - Se igualan requisitos para notificación a APD e interesados
  - Se exime de obligación cuando *"el responsable del tratamiento ha tomado medidas ulteriores que garantizan que ha desaparecido la probabilidad de que se materialice el alto riesgo de que los derechos y libertades de las personas objeto de los datos a que hace referencia el apartado 1 se vean gravemente afectados"*
- Notificación en PE → No parece posible modular para APD y se amplían casos para interesados ("intereses")
- PIA vinculada a tratamientos de alto riesgo → Alto grado de coincidencia en todas instituciones
- Códigos de conducta y esquemas de certificación → Mejora y mayor desarrollo en Consejo

Responsabilidad activa

DPO

- COM → Obligatorio en
  - Administraciones Públicas
  - Empresas de >250 empleados
  - Actividades que (…) requieran un seguimiento periódico y sistemático de los interesados
- PE → Obligatorio en
  - Autoridad u organismo públicos
  - Persona jurídica con respecto a más de 5.000 interesados durante un periodo consecutivo de 12 meses;
  - Actividades que, (…), requieran un seguimiento periódico y sistemático de los interesados;
  - Actividades principales (…) tratamiento de categorías especiales de datos, datos de localización o datos relativos a niños o a empleados en ficheros a gran escala
- Consejo → Voluntario, salvo previsión en ley nacional o UE

MUCHAS GRACIAS