AT GROUP
We know what we do

NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS U.E.

Novedades, repercusiones y comentarios 2013

Madrid, 24 de julio del 2013.

AT GROUP
We know what we do

Hoy hablaremos de:

- El nuevo Reglamento General de protección de datos de la U.E.
- Cambios generales
- Plan de adaptación
- Conclusiones

El nuevo Reglamento General de protección de datos de la U.E.

INTRODUCCIÓN:

La futura reforma de la Directiva CEE 46/95 de la UE, generará un **nuevo paradigma de responsabilidad** en la gestión de los datos personales que se traduce en nuevas obligaciones para las empresas e instituciones en materia de protección de datos.

Se introducen criterios de evaluación previa al tratamiento, criterios de autocontrol, rendición de ctas. y diligencia exigible en la gestión.

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Marco legal actual:

- Directiva CEE46/95
  - LO. 15/99 LOPD
    - RD 1720/2007
      - OTRAS. Instrucciones, jurisprudencia, etc.

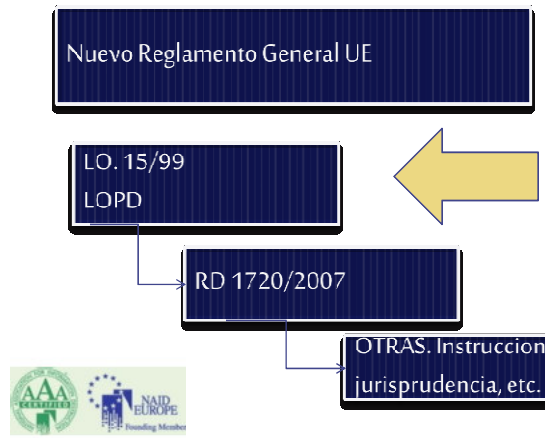
Necesaria transposición del Derecho comunitario al interno de cada estado.

Autoridad de control interna: Esp. AEPD y otras CCAA

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Marco legal futuro:



Aplicación Directa. Supremacía del Derecho Comunitario

Autoridad de control interna y Comisión y el Consejo Europeo de Protección de datos

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Motivación "oficial":

- Es un mandato especifico del artículo 16 del Tratado Funcionamiento de la Unión Europea.
- El Reglamento se elige entre la Directiva y la Recomendación, como medio más idóneo, ya que es de aplicación directa (art. 288 TFUE).
- Introduce un conjunto armonizado de normas básicas con el objeto de:
  - *Armonizar el mdo. Interior*
  - *Protección de un derecho fundamental reconocido a la PDP.*
  - *Otras no confesables: control o herramienta de presión sobre los grandes operadores americanos de Internet.*

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevos Principios en materia de PDP:

Definición: los principios son condiciones generales de obligado cumplimiento para el tratamiento de DP.

- De calidad de los datos (art.4)
- De consentimiento del afectado, (art. 5)
- De tratamiento de datos especialmente protegidos
- De seguridad de los datos, (art.9)
- Deber de secreto (art.10)
- De comunicación de los datos, (art.11)
- por cta. de terceros, (art.12)

Nuevos principios PDP

- Rendición de cuentas (Accountability)
- Principio de Transparencia

AT GROUP
We know what we do

El nuevo **Reglamento General** de protección de datos de la U.E.

Principio de rendición de cuentas (Accountability):

- Designa como responsables a las compañías en la implantación de medidas de seguridad eficiente.
- Exige un método de validación que garanticen su fiabilidad.
- Exigencia general para empresas pequeñas y grandes
- Sigue la doctrina general de *Compliance Managesment.*

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Principio de Transparencia:

- **Se centra en facilitar las relaciones entre el responsable de fichero y el interesado, así como entre el responsable de los datos y las autoridades de control.**
  - **Eliminación** de la obligación de notificar ficheros a la AC.
  - **Deber de conservación** de toda la documentación acreditativa, tanto del responsable de fichero, como del encargado de tratamiento.
  - Establecimiento de mecanismos sencillos para el **ejercicio de derechos**.

- ❑ *Posibilidad de ejercitar los derechos por vía electrónica*
- ❑ *Obligación de informar a los solicitantes sobre la posibilidad de reclamación ante la AEPD o judicial.*
- ❑ *La Comisión podrá establecer formularios y procedimientos normalizados para la comunicación a los interesados.*

  - **Cooperación con las autoridades de control**. No sólo se tendrá que colaborar con la AEPD , sino que se tendrá que rendir ctas. ante la Comisión y el Consejo Europeo de Protección de Datos.

Conclusión: estricto deber de cumplimiento.

ATGROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevo concepto consentimiento menores:

Situación del RD 1720/2007: se acepta el consentimiento de mayores de 14 años.

Nuevos concepto

- Se fija la edad de consentimiento a los 13 años en Servicios de la sociedad de la información.
- El tratamiento de los menores sólo será lícito si los padres o tutores legales ha prestado su consentimiento previo.

ATGROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevos Derechos para el ciudadano: Dº. al olvido.

Derecho al olvido. Supresión de datos por:

- No son necesarios para la finalidad para la que fueron captados
- Por que el interesado a revocado el consentimiento
- Porque ha expirado el tiempo legal para el tratamiento de los datos.
- Porque el interesado ha ejercitado su derecho de oposición.
- Porque el tratamiento no se ha hechos según lo estipulado en el Reglamento

Alcance

- Obliga a los responsables de difusión a terceros a comunicar la obligación de suprimir cualquier enlace a los datos publicados, así como a eliminar cualquier copia o replica de datos.

Consecuencia: Eliminación de Internet de los datos de la persona que quiera ser olvidada.

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevos Derechos para el ciudadano: oposición creación perfiles (similar ARCO)

- Prohibición de evaluación de forma automatizada, determinados aspectos personales propios de dicha persona física.
  - En particular análisis o predicciones::
  - Capacidad económica
  - Capacidades laborales
  - Estado de salud
  - Preferencias personales
  - Fiabilidad y/o comportamiento

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevos Derechos para el ciudadano: Portabilidad de los datos

Alcance

- Posibilidad de obtener del responsable de tratamiento una copia de datos objeto de tratamiento en un formato electrónico estructurado y en formato común.
- Pensado especialmente para las teleoperadoras, cambio del usuario de forma ágil y sencilla.

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevas obligaciones: Notificación de brechas de seguridad

El Reglamento no expone medidas de seguridad (legislación básica). Establece que se adoptaran las medidas según :

- Los riesgos que representan.
- La naturaleza de los datos.
- Los costes de implementación.

Alcance

- Obliga a los RF o ET, a notificar la incidencia de seguridad a la autoridad de control (24 h)
- Obliga a informar al interesado sobre la incidencia.
  - Aunque si se aplican medidas se puede evitar.

Se habilita a que la Comisión de UE, pueda realizar actos normativos de desarrollo.

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevas obligaciones: Delegado de Protección de Datos (DPO)

- Obligatorio para todas las organizaciones de mas de 250 empleados.
- Mandato de 2 años, interno o externo.
- Independiente.
- Puede ser uno para un Grupo

Perfil del DPO

- Supervisor de políticas internas PDP
- Responsable formación personal.
- Gestión de auditorias.
- Informador a interesados.
- Gestor D°s.ARCO
- Responsable documentación
- Surpervisor de la las PIA
- Coordinador con las Autoridades de control en materia PDP.

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevas obligaciones: Evaluación de Impacto

- ¿Cuándo?
- Por riesgos específicos, por razón de naturaleza, alcance o fines.
- En particular cuando:
  - *el tratamiento sirva para crear perfiles.*
  - *Se traten datos sensibles, genéticos, biométricos.*
  - *CCTV*
  - *Menores*

Evaluación de Impacto de Privacidad. PIA:

- **Descripción de tratamientos**
- **Evaluación riesgos derechos ARCO y otros**
- **Garantías y medidas de seguridad**
- **En su caso, recabar opinión interesados.**

AT GROUP
We know what we do

El nuevo Reglamento General de protección de datos de la U.E.

Nuevas obligaciones: Consultas a la autoridad de control

- ¿Cuándo?: Para la autorización de tratamientos de datos transnacionales.
- En el caso de ausencia de instrumento jurídico vinculante.
- En particular cuando:
  - *elevado nivel de riesgo (por su naturaleza, alcance o fines).*
  - *Por decisión de la Autoridad de Control.*
    - *Por riesgo elevado*
    - *Por estar en una lista de tratamiento de riesgo publicada por al Autoridad de Control.*

AT GROUP
We know what we do

CUADRO DE SANCIONES I:

A parte de la **pérdida reputacional** de la entidad, "***pena del Telediario"***, así como los problemas generados por la "*pena del banquillo"*, para el sancionado, el Reglamento contempla las siguientes sanciones:

- ***250.000€ Multa, si no es empresa (¿?), o el 0.5% de la facturación mundial por :***
  - *No proporcionar mecanismos de solicitud a los interesados, no responder en tiempo y forma.*
  - *Imponga el pago de una tasa por la respuesta.*

AT GROUP
We know what we do

CUADRO DE SANCIONES III:

- ***500.000€ Multa, si no es empresa (¿?), o el 1% de la facturación mundial por :***

- *No facilitar información, o facilitar información incompleta, o no de una forma suficientemente transparente.*
- *No facilitar acceso a datos , o no rectifique o no comunique al destinatario.*
- *No respete el derecho al olvido, o la supresión, no garantizar plazos de supresión de links.*
- *No facilitar copia datos en formato electrónico para portabilidad*
- *No determinar responsabilidades de los corresponsables*
- *No conservar documentación, o insuficiente.*
- *No cumplir libertad de expresión, laboral, salud , estadística, etc.*

AT GROUP
We know what we do

CUADRO DE SANCIONES III:

- ***1.000.000€ Multa, si no es empresa (¿?), o el 2% de la facturación mundial por :***

- *Tratar DP sin base jurídica o incumplir normas del consentimiento*
- *Tratar datos especiales con violación de lo establecido en el Reglamento*
- *No se allane a una oposición*
- *No cumpla las limitaciones para elaboración de perfiles*
- *No adopte políticas internas o no implemente medidas adecuadas de seguridad*
- *No designe representante.*
- *No hacer el PIA o no pedir el permiso previo para tratamientos que así lo requieran.*
- *No designe un "agente " de protección de datos.*
- *Haga uso indebido de los sellos y marcas contemplados en el art.39*
- *Trasferencias de datos si n autorización*
- *No cumplir requerimientos de bloqueo de ficheros de la AC*
- *No cumplir deber de colaboración con la AC*
- *No cumplir con las normas de salvaguarda de l secreto profesional*

AT GROUP
We know what we do

❖ ¿CÓMO EVITAR EL RIESGO?:

MEDIANTE UN PLAN INTEGRAL DE PROTECCIÓN DE DATOS (PIPD) o *Data Protection Compliance Program*

Dicho sistema, ha de contemplar obligatoriamente:

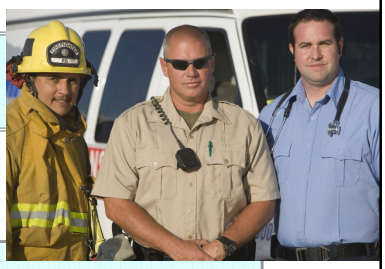
- **Plan preventivo** acreditativo de Diligencia Debida.
- **Plan formativo específico**.
- **Plan de control y auditoria de cumplimiento**.
- **Plan de asistencia jurídica** y la aportación de prueba **documental, testifical y pericial**.

AT GROUP
We know what we do

Visto lo anterior...TODA LA AYUDA ES POCA...

"...acreditar la DILIGENCIA DEBIDA es la única manera de evitar un proceso sancionador, la culpa de usuario o al fuerza mayor exoneran de responsabilidad."

"... la formación documentada es un elemento fundamental para acreditar la ACCIONES PREVENTIVAS ESPECÍFICAS."



¿QUÉ ES LA PLAN INTEGRAL DE PROTECCIÓN DE DATOS?

Es un sistema de protección integral a las empresas, que pueda permitirles **exonerar o limitar su responsabilidad administrativa o contenciosa administrativa** en caso de que alguno o algunos de sus empleados o colaboradores (ET, DPO, etc) realice un ilícito en materia de PDP que pueda ser susceptible de derivar en un proceso sancionador

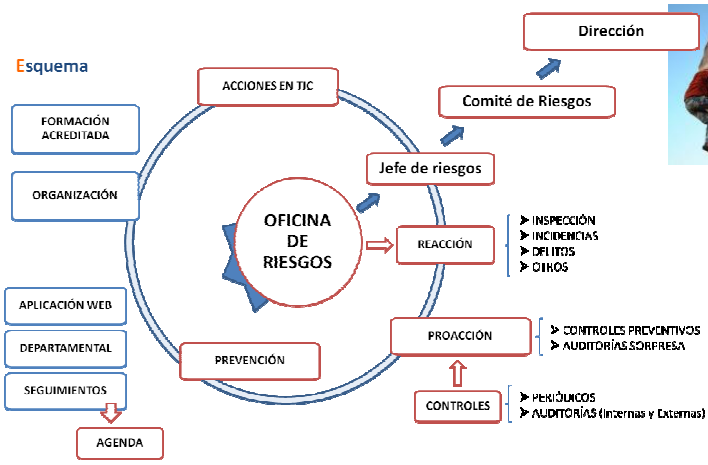
¿Cómo?

Establecimiento, dentro de un Plan Director, de medidas específicas:

- Preventivas
- Reactivas
- Proactivas.

AT GROUP
We know what we do

LA OFICINA PIPD



AT GROUP
We know what we do

¿Qué ha de contener el Plan de Acción? I:

- Programa de **adaptación de Ficheros y Tratamientos** a los nuevos requisitos.
- Programa de **adaptación de formularios de captación de datos** y resto de documentación o procesos de entrada de datos. (Captación del consentimiento según nuevos requisitos , no se acepta tácito).
- Programa de **adaptación de Derechos ARCO y Nuevos Derechos** (portabilidad y olvido)
- Programa de **formación en materia de PDP** al personal afectado.
- Programa de **gestión de notificación de incidencias a la Autoridad de Control** y a los usuarios.
- Programa de **colaboración con la Autoridad de Control** ante requerimientos e inspecciones.
- Programa de **auditorias y controles en 360º** acreditativos de la buena praxis en la PDP. (proveedores, colaboradores, personal propio, otros)

AT GROUP
We know what we do

¿Qué ha de contener el Plan de Acción? II:

- Programa de **Evaluaciones de Impacto de los Tratamientos** de DP actuales y futuros. Gestión de **consultas previas** a la autoridad de control.
- Programa de **Gestión inicial y configuración por defecto** de proyectos de tratamiento según PDP
- Programa de Gestión de **ventanilla única corporativa** (Grupo de empresas o Administraciones)
- Programa de **gestión y conservación de documentación acreditativa** obligatoria.
- Programa de creación , gestión y acreditación de garantías adecuadas, NORMAS CORPORATIVAS VINCULANTES o petición de autorización transferencia internacional de datos.
- Programa de **defensa jurídica** e información de mecanismos de cohesión en procedimientos de PDP

AT GROUP
We know what we do

¿Qué formatos-plantilla necesito en mi Plan de Acción? I:

- Documento de funciones y obligaciones del personal actualizado.
- Contrato de encargado de tratamiento , con plan de auditorios, monitoreo y controles art.26.
- Modelo de autorización al encargado de tratamiento para que subcontrate a un 2º encargado.
- Check list de evaluación de competencias de encargados de tratamiento cualificados . Art. 26
- Modelo de acta de designación de responsable ante la UE. Art. 25
- Contrato de corresponsables de tratamiento.
- Check list de cumplimiento desde el diseño (aplicaciones, servicios, etc).
- Check list de cumplimiento de limitación por defecto (aplicaciones, servicios, etc)
- Check list de obligaciones y cumplimiento del RF art. 22
- Respuesta acreditada a un ejercicio de derechos ARCO

AT GROUP
We know what we do

¿Qué formatos-plantilla necesito en mi Plan de Acción? II:

- Formulario de captación de datos que cumpla el dº info.
- Check list de cumplimiento del principio de medidas razonables de control en l a supresión de datos
- Acta de denegación de supresión de datos
- Acta de limitación del tratamiento
- Determinación del formato unificado de portabilidad de datos
- Recibo de conformidad en la entrega o respuesta de doc.
- Comunicación de la identidad y dirección del DPO a la autoridad de control
- Contrato de servicios con el DPO
- Acta de nombramiento del DPO
- Check lists de requisitos mínimos del DPO.

AT GROUP
We know what we do

¿Qué formatos-plantilla necesito en mi Plan de Acción? III:

- Modelo normalizado de información a la AC.
- Modelo de consulta o autorización previa a la AC
- PIA
- Notificación de violación de datos a la AC
- Notificación de violación de datos al interesado
- Notificación de violación de datos del ET al RF.

AT GROUP
We know what we do

EL PLAN UNA VEZ IMPLEMENTADO HA DE PERMITIR:

- ✓ **MONITOREAR** todos los riesgos inventariados
- ✓ **LOCALIZACIÓN** e **INVENTARIO** de documentos críticos
- ✓ Acreditación jurídica plantilla **DELEGACIÓN** de **FUNCIONES** (acreditable en juicio)
- ✓ Disponer de **FORMACIÓN** preventiva de prestigio (acreditable ante la AC y en juicio)
- ✓ **PERITACIÓN FORENSE** (acreditable ante la AC o en juicio)
- ✓ Seguimiento implementación **LOPD** + **LSSICE**
- ✓ Seguridad **FÍSICA**
- ✓ Control de **RIESGOS TECNOLÓGICOS**
- ✓ Seguimiento litigios PDP ya sean **ADMINISTRATIVOS** o **JUDICIALES**,.
- ✓ Coordinación con **SISTEMAS DE CALIDAD**

AT GROUP
We know what we do

CONCLUSIONES:

• Aumenta la presión a las empresas y profesionales.

• Existe una gran inseguridad jurídica motivada por:

- ○ Ausencia de precedentes en los conceptos jurídicos nuevos.
- ○ Abundancia de conceptos jurídicos indeterminados.
- ○ Imprecisión en la tipificación de las infracciones
- ○ Imprecisión en los sujetos activos de dichas infracciones

- Aumenta la carga de gestión.
- Departamento propio e independiente (DPO)
- Se necesita dotarlo de medios y presupuesto.
- Más cargas económicas de origen administrativo.
- Grandes retos para las autoridades de control
- Grandes retos para todos...

AT GROUP
We know what we do

Gracias por la atención

www.atgroup.es