Adecuación al Reglamento Europeo de Protección de Datos

PLAN DE ACCIÓN (MARZO 2017-MAYO 2018) CSAI (SGTIC)

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Situación de partida

- El RGPD se aplicará desde el 25 de mayo de 2018 (en vigor desde 25/05/2016).
- Sobre la situación actual regulada por la Ley Orgánica de Protección de Datos y su Reglamento, se plantean varias modificaciones:
  - Su eje cambia de "Fichero" a "Tratamiento" de datos personales.
  - Se elimina la necesidad de realizar Ordenes ministeriales con cada Fichero.
  - Se exige:
    - Una valoración de riesgos de los tratamientos y elegir las medidas derivadas.
    - Disponer de un Registro de los tratamientos con algunos datos nuevos.
    - Que los consentimientos sean explícitos y cumplan varias condiciones.
    - Proteger especialmente también los datos personales biométricos, genéticos y los que puedan generar perfiles descriptivos de las personas.
    - Regular las externalizaciones de los tratamientos.
    - Incorpora nuevos derechos (Olvido, portabilidad, …).
    - Nombrar un Delegado de Protección de Datos.

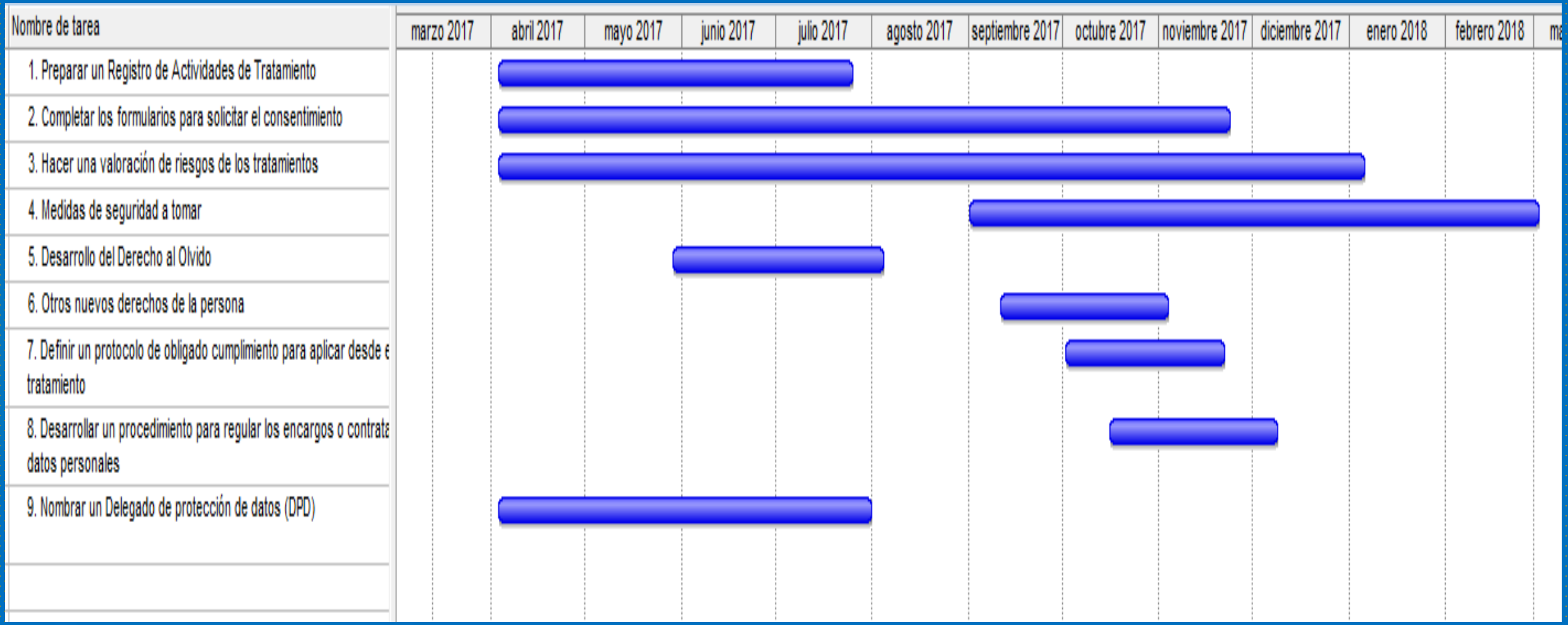
4 Terrenos Críticos

- El "**consentimiento expreso**" art. 28.2, ley 39/2015 (Procedimiento Advo. Común de las Administraciones Públicas): "…Se presumirá que la consulta u obtención es autorizada por los interesados salvo que conste en el procedimiento su oposición expresa o ley especial aplicable requiera consentimiento expreso"
- Las **medidas de protección y el ENS**
- La estructura de la Administración y el **DPD**
- La situación (Volatilidad/Incertidumbre/Complejidad/Ambigüedad) y **los "perfiles de aspectos personales "**

Líneas de acción

- 1. Preparar un Registro de Actividades de Tratamiento
- 2. Completar los formularios para solicitar el consentimiento
- 3. Hacer una valoración de riesgos de los tratamientos
- 4. Medidas de seguridad a tomar
- 5. Desarrollo del Derecho al Olvido
- 6. Otros nuevos derechos de la persona
- 7. Definir un protocolo de obligado cumplimiento para aplicar desde el diseño inicial de cualquier tratamiento
- 8. Desarrollar un procedimiento para regular los encargos o contrataciones de tratamiento de datos personales
- 9. Nombrar un Delegado de protección de datos (DPD)

Planificación inicial de líneas de acción (feb 2017-jun 2018)



1. Preparar un Registro de Actividades de Tratamiento

- Identificar todos los tratamientos de datos personales de la organización (hoy contamos con un registro de 2.437 ficheros con unos 240 responsables)
- Completar la información de cada fichero para transformarlos en Tratamientos, con:
  - Fundamento legal documentado
  - Si incluye datos especiales (biométricos, genéticos o susceptibles de producir perfiles)
  - Si requiere formulario para solicitar los consentimientos

2. Completar los formularios para solicitar el consentimiento

- Verificación de que el consentimiento es explícito y no tácito.
- Nuevos componentes a incluir:
  - Datos de contacto del Delegado de Protección de Datos o representante.
  - Fines y Base jurídica para el tratamiento.
  - Plazo o criterios de conservación de los datos.
  - Posible elaboración de perfiles.
  - Previsión de transferencias a terceros países.
  - Derecho de reclamación.
  - Si los datos no provienen del interesado (origen y categorías)
  - Consideración especial de los menores (Art. 8. 1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.)

3. Hacer una valoración de riesgos de los tratamientos

- General (todos los tratamientos)
- EIPD (Evaluación de Impacto) para los tratamientos que impliquen un alto riesgo para los derechos y libertades de los interesados.

4. Medidas de seguridad a tomar

- Según la valoración de riesgos y el tipo de datos:
  - Tratamientos con datos ordinarios / medidas ENS basico
  - Tratamientos con datos especiales / medidas ENS medio o …
  - Procedimiento de gestión y notificación de "quiebras de seguridad"

5. Desarrollo del Derecho al Olvido

- **Artículo 17 Derecho de supresión («el derecho al olvido»):**
- **1.** El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:…

6. Otros nuevos derechos de la persona: 6.1. a la portabilidad

- "Artículo 20 Derecho a la portabilidad de los datos:
  - 1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:...

6. Otros nuevos derechos de la persona: 6.2. a la limitación

- Artículo 18 Derecho a la limitación del tratamiento 1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: inexactitud de los datos, uso ilícito,…

6. Otros nuevos derechos de la persona: 6.3. a la transparencia de la información

- Art.12. 3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. …

7. Definir un protocolo de obligado cumplimiento para aplicar desde el diseño inicial de cualquier tratamiento

- 1. Identificar si el tratamiento de datos incluye datos personales
- 2. Explicitar si además de datos ordinarios se incluyen datos especiales.
- 3. Valorar los riesgos de l tratamiento previsto y establecer las medidas adecuadas para su protección.
- 4. Incluirlas en forma de cláusulas de obligado cumplimiento para el desarrollo a realizar .
- 5. Procesos posteriores de verificación.

8. Desarrollar un procedimiento para regular los encargos o contrataciones de tratamiento de datos personales

- 1. Instrucciones para el responsable
- 2. Deber de confidencialidad.
- 3. Medidas de seguridad.
- 4. Destino de los datos al finalizar la prestación.
- 5. Verificación del cumplimiento

9. Nombrar un Delegado de Protección de Datos (DPD)

- Requerimientos:
  - Total autonomía en el ejercicio de sus funciones.
  - Necesidad de que se relacione con el nivel superior de la Dirección (organigrama).
  - El responsable o el encargado deben facilitar todos los recursos necesarios al DPD para desarrollar su actividad.
  - Puede estar a tiempo completo o parcial pero debe evitar los conflictos de interés.
- Perfil sugerido:
  - Conocimiento de la legislación y práctica de la protección de datos (tecnología aplicable, conocimiento de las actividades afectadas)