IMPACTO DE LA NUEVA NORMATIVA DE PROTECCIÓN DE DATOS EN LAS EMPRESAS Y ORGANIZACIONES EMPRESARIALES

Jesús Rubí Navarrete
Adjunto a la Directora
Agencia Española de Protección de Datos
07/05/2018
CEOE

Armonización

El Reglamento 2016/679 sustituirá a la Directiva 95/46

- Publicado 4 de mayo 2016
- Entrada en vigor a los 20 días de publicación
- 2 años hasta inicio de aplicación: 25 de mayo de 2018

Principios

Principios se mantienen similares a Directiva, con refuerzo en algunos matices

- Licitud, lealtad y transparencia
- Limitación de finalidad
- Minimización de datos
- Exactitud (ALOPD no imputación al responsable)
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva

Legitimación

Art. 6.1

a) consentimiento para el tratamiento de sus datos personales para uno o más fines específicos

b) ejecución de un contrato en el que el interesado es parte o para la aplicación, a petición de éste, de medidas precontractuales

c) cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento

d) intereses vitales del interesado o de otra persona física

Legitimación

e) cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los interés o los derechos y libertades fundamentales del interesado que requieren la protección de los datos personales, en particular, cuando el interesado sea un niño. Ello no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones

Algunas aclaraciones (considerandos 47 a 49)

- Aplicación del principio de expectativa razonable derivada de la relación del afectado con el responsable
  - Existencia de una "relación pertinente o apropiada" (cliente, empleado, etc.)
  - Transmisiones de datos dentro de Grupos empresariales para fines administrativos internos
    - Por ejemplo, centralización de datos de clientes o empleados
  - Transmisiones para garantizar la seguridad de las redes, por ejemplo a los CERT

Control por los interesados

- **Consentimiento** →
  - Libre, específico, informado e "inequívoco" → A través de declaraciones o "claras acciones afirmativas"
  - Salvaguardas en articulado y considerandos
    - Situaciones de desequilibrio claro entre interesado y responsable
    - Consentimiento conjunto necesario para varias operaciones
    - Tratamientos vinculados a ejecución de contrato, incluida prestación de servicio, cuando tratamiento no es necesario para esa ejecución o prestación
    - Revocable
  - Consentimiento de menores con autorización → 16 años, pudiendo EEMM reducir hasta 13

Algunas aclaraciones

- Se considera que puede existir un acto afirmativo claro en supuestos como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal (Cdo. 32)
- También puede considerarse acto afirmativo marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta
  - El silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento (Cdo. 32)
  - Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos (Cdo. 32)
  - No debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno (Cdo 42)
  - No debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento"(Cdo. 43)

Algunas consecuencias

- El RGPD no implica necesariamente una obligación de recabar un nuevo consentimiento si el que se hubiera obtenido antes de su aplicación fuese conforme a los requisitos que establece
  - Siguen siendo válidos los consentimientos expresos y los consistentes en una manifestación o clara acción afirmativa
  - El Cdo. 32 clarifica supuestos que pueden considerarse consentimiento (declaración, marcación de una casilla, selección de parámetros)
  - En ningún caso hay aplicación retroactiva, dado que las normas del RGPD no se aplican a tratamientos anteriores al momento en que produce plenos efectos
- Cuando se preste el consentimiento para el tratamiento de datos con múltiples finalidades será preciso dar el consentimiento para todos ellos (Cdo. 32). En particular:
  - Consentimientos específicos en el marco de un contrato
  - Consentimientos específicos en el marco de declaraciones

Categorías especiales de datos

- Se incluyen datos genéticos y biométricos
- Se excluyen datos de infracciones y sanciones administrativas.

  Autorización por ley con garantías adicionales. (órganos competentes o terceros habilitados)

Regla general: queda prohibido su tratamiento (igual que en la Directiva)

Excepciones a la prohibición

- Consentimiento

Categorías especiales de datos

.../...

- **Habilitación en el ámbito del derecho laboral y de seguridad o protección social**
  - **Puede basarse en Convenio Colectivo**
- **Tratamiento para la protección de intereses vitales del afectado o un tercero**
- **Datos manifiestamente públicos**
- **Tratamiento necesario por razones de Interés público esencial según la Ley UE o Nacional siempre que sea proporcional a la finalidad perseguida**

Categorías especiales de datos

Excepciones a la prohibición

- Habilitaciones legales
  - Supuestos
    - Medicina preventiva o laboral y evaluación de la capacidad laboral
    - Diagnóstico médico o prestación sanitaria
    - Gestión de los sistemas o servicios sanitarios
  - Exigencia de tratamiento llevado a cabo por profesional sujeto a deber de secreto o bajo su responsabilidad

Categorías especiales de datos

- Razones de interés público en el ámbito de la salud pública, así como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios
- Archivo y fines de investigación histórica o científica o estadísticos en los términos del propio Reglamento (artículo 89)

Derechos

- Catálogo tradicional con tres novedades
  - Información
  - Acceso (copia de los documentos)
  - Rectificación
  - Derecho al borrado y al olvido
  - Limitación del tratamiento
  - Portabilidad
  - Oposición
- Previsiones sobre ejercicio de estos derechos
  - Lenguaje claro e inteligible
  - Obligación de "facilitar el ejercicio"
  - Plazos de respuesta → 1 mes
  - Formas de ejercicio → Posible vía electrónica
  - Gratuidad

El deber de informar/principio de transparencia en el Reglamento

Configuración de la información como derecho del interesado y no como obligación del responsable

Se incrementa la información que habrá de facilitarse cuando los datos se recaban del afectado

- **Datos de contacto del delegado de protección de datos**
- **Fines y base jurídica del tratamiento**
- **Intereses legítimos del responsable o de un tercero**
- **Destinatarios o las categorías de destinatarios de los datos personales**
- **Transferencias previstas**
- **Plazo de conservación**
- **Existencia de decisiones automatizadas, incluida la elaboración de perfiles la lógica aplicada y las consecuencias previstas**

Si los datos no se recaban del interesado deberá además informársele de:

- Categorías de datos que se van a tratar
- Fuente de la que proceden los datos personales y, en su caso, si proceden de "fuentes de acceso público"

Clarificación del plazo

Excepciones al deber de información

- Si los datos no proceden del interesado
  - Aclaración del esfuerzo desproporcionado en caso de tratamiento con fines de archivo, estadísticos o de investigación científica o histórica
  - Previsión legal expresa de tratamiento o revelación, con medidas oportunas de protección
  - Obligación de secreto legal o profesional

Exigencia de claridad, concisión y fácil acceso

El deber de informar/principio de transparencia en el proyecto de LOPD (art. 21)

Información por capas

- Información en la primera capa
  - En todo caso
    - Identidad del responsable del tratamiento o su representante
    - Finalidad del tratamiento
    - Modo de ejercicio de los derechos
    - Uso de los datos para la elaboración de perfiles, en su caso
    - Derecho de oposición a decisiones automáticas, en su caso
  - Si los datos no se han obtenido del afectado, además deberá informarse de:
    - Categorías de datos objeto de tratamiento
    - Fuentes u orígenes de los datos

El deber de informar/principio de transparencia en el Reglamento

Excepciones al deber de información

- **En general, cuando el interesado ya disponga de la información**
- **Si los datos no proceden del interesado**
  - **Aclaración del esfuerzo desproporcionado en caso de tratamiento con fines de archivo, estadísticos o de investigación científica o histórica**
  - **Previsión legal expresa de tratamiento o revelación, con medidas oportunas de protección**
  - **Obligación de secreto legal o profesional**
- **La prevalencia del derecho a la tutela judicial efectiva**

Exigencia de claridad, concisión y fácil acceso (criterios AEPD: información por capas y por tablas)

Cuestiones generales sobre los restantes derechos en el Reglamento

Condiciones generales

- Obligación de atender los derechos a menos que se acredite la imposibilidad de identificar al interesado
- Respuesta por medios electrónicos si el derecho se ejercitó por dichos medios salvo que el interesado manifieste lo contrario
- Gratuidad salvo en caso de solicitudes "manifiestamente infundadas o excesivas
  - Cobrar un canon
  - Negarse a actuar respecto de la solicitud.
- Posibilidad de solicitar información adicional para garantizar la identificación del solicitante

Limitación de tratamiento

- Casos en que existe derecho a solicitar la limitación
  - Mientras se verifica de la exactitud de los datos en casos de impugnación por el interesado
  - Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales
  - Cuando el interesado necesite que el responsable conserve los datos para la formulación, el ejercicio o la defensa de reclamaciones
  - Mientras se verifican circunstancias en derecho de oposición

Derecho a la portabilidad

Derecho del interesado a

- Recibir los datos personales que le incumban,
- Que haya facilitado a un responsable del tratamiento,
- En un formato estructurado y de uso habitual y de lectura mecánica
- Y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que se hubieran facilitado los datos

Requisitos para que pueda ejercitarse (acumulativos):

- El tratamiento esté basado en el consentimiento o en un contrato
- El tratamiento se efectúe por medios automatizados

Derecho a la portabilidad

Modo de ejercicio

- Podrá implicar la transmisión directa de responsable a responsable a instancia del interesado "cuando sea técnicamente posible"

Limitaciones

- Exceptuado cuando el tratamiento se funde en el cumplimiento de una misión de interés público o inherente al ejercicio del poder público

GT 29

- Aplicación a datos facilitados directamente o resultado del funcionamiento, pero no a los datos inducidos

Derecho de supresión ("olvido"). Especialidades y excepciones

Supresión de enlaces

- Cuando el responsable haya hecho públicos los datos y proceda la supresión
- Obligación de informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos
- Límites: tecnología disponible y coste de su aplicación

Excepciones

- Ejercicio de las libertades de expresión e información
- Cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento,
- Tratamiento para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable
- Razones de interés público en el ámbito de la salud pública
- Fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento
- Formulación, ejercicio o defensa de reclamaciones

Otros derechos

Derecho de rectificación

- Vinculación directa con el carácter inexacto o incompleto de los datos

Derecho de oposición

- General
  - Basado en motivos relacionados con la situación personal del afectado
  - Inversión de la prueba: será el responsable el que deberá justificar "motivos imperiosos para el tratamiento" que prevalezcan sobre los derechos de los afectados

Otros derechos

- **Opt-out en marketing directo**
  - **Incluye también la oposición a la elaboración de perfiles**
  - **Sin necesidad de especificar ningún motivo concreto**
  - **Obligación de especificación concreta y separada del derecho en la primera comunicación comercial que se le dirija**
  - **Posibilidad de ejercicio en todo caso a través de medios automatizados**
- **Opt out en caso de tratamiento con fines de investigación y estadísticos**
  - **Excepción: tratamiento por razones de interés público**

Otros derechos

Decisiones automatizadas

- Referencia expresa a la elaboración de perfiles
- Derecho a no ser objeto de una decisión que "produzca efectos" sobre el afectado o "le afecte significativamente de modo similar
- Excepciones
  - Vinculación a contrato
  - Autorización por el derecho Nacional o de la UE
  - Consentimiento explícito
- Salvo en caso de habilitación legal, el interesado tiene derecho a obtener intervención humana en la decisión y que el interesado pueda dar su opinión e impugnar la decisión
- Salvo que exista consentimiento o interés público, no podrá implicar datos sensibles

Obligación de comunicación de la rectificación, supresión o limitación del tratamiento a los cesionarios

Responsabilidad activa

- El Reglamento prevé que los responsables aplicarán las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el presente Reglamento. Tales medidas se revisarán y actualizarán cuando sea necesario

Responsabilidad activa

Tipos de medidas

- Mantener "registro de actividades de tratamiento"
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Aplicar medidas de seguridad adecuadas
- Llevar a cabo Evaluaciones de Impacto
- Autorización previa o consultas previas con APD
- Designación Delegado Protección de Datos (DPD)
- Notificación de Quiebras de Seguridad
- Códigos de conducta y esquemas de certificación

Enfoque de riesgo

- Medidas aplicables en función del riesgo para los derechos y libertades de los interesados
  - Alto riesgo vs. riesgo estándar
  - El riesgo como criterio de ponderación
- Problema de determinación del nivel de riesgo

Protección de Datos desde el diseño

- **Medidas técnicas y organizativas adecuadas** (p.ej. seudonimización, minimización) para aplicar principios de PD de forma eficaz y proteger los derechos
- **En el momento de determinar los medios para el tratamiento y en el momento del tratamiento** (integrar necesarias garantías)
- Teniendo en cuenta
  - Naturaleza, ámbito, contexto y fines del tratamiento
  - Riesgos de diversa probabilidad y gravedad (no sólo alto riesgo)
  - Estado de la técnica y coste

Protección de Datos por defecto

- Medidas técnicas y organizativas apropiadas
- Tratamiento **por defecto sólo de datos personales necesarios para cada fin específico**
  - Cantidad de datos recopilados
  - Extensión del tratamiento
  - Periodo de almacenamiento
  - Accesibilidad
  - En particular, evitar la accesibilidad a un número indeterminado sin intervención de alguien

Registro de tratamientos

- Obligación para responsable y encargado
- Los ficheros inscritos en el RGPD (ALOPD Art.32.1 "El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.")
- La desagregación de las actividades de tratamiento
- La incidencia en las medidas de cumplimiento normativo
- Contenido (responsable)
  - **Identificación** y datos contacto de responsable, corresponsable, representante y DPO
  - **Fines**

Registro de tratamientos

- Descripción de categorías de interesados y datos personales
- Categorías de destinatarios existentes o previstos (inclusive en terceros países u organizaciones internacionales)
- TID a terceros países u organizaciones internacionales y documentación de garantías para TID exceptuadas sobre base de intereses legítimos imperiosos
- Cuando sea posible, plazos previstos para supresión de datos
- Cuando sea posible, descripción general de medidas de seguridad

Medidas de seguridad

- Medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al **riesgo**, teniendo en cuenta
  - Estado de la **técnica y costes** de aplicación
  - **Naturaleza, alcance, contexto y fines** del tratamiento
  - **Riesgos** para los derechos y libertades de las personas

- La adhesión a un **código de conducta o a un mecanismo de certificación** podrá servir de elemento para demostrar el cumplimiento de los requisitos de seguridad

Notificación de violaciones de seguridad de los datos

Notificación a APD

- Sin demora y a más tardar en 72 horas desde que se haya tenido constancia. Más tarde, justificación motivada
- No obligación cuando "sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas"
- Reglamento prevé contenido mínimo de notificación
- Documentación de todas las violaciones de seguridad
- Obligación del encargado de notificar sin dilación indebida violaciones de seguridad al responsable

Notificación de violaciones de seguridad de los datos

Notificación a interesados

- Cuando es probable que la quiebra entrañe alto riesgo para los derechos y libertades de interesados
- Sin dilación indebida
- También se prevé contenido mínimo, que no incluye posibles medidas paliativas
- Excepciones
  - Implementación de medidas de protección tecnológica que haga ininteligibles los datos a terceros no autorizados (p.ej.: datos encriptados)
  - medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado
- APD puede obligar a notificar a interesados

Evaluación de impacto

- Deberá realizarse cuando sea probable que el tratamiento previstos presente un alto riesgo específicos para los derechos y libertades de los interesados, entre otros casos, cuando:
  - elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
  - tratamiento a gran escala de las categorías especiales de datos
  - observación sistemática a gran escala de una zona de acceso público
- Las APD deberán establecer listas adicionales de tratamientos de alto riesgo y podrán establecer listas que no requieren EIPD
- El RGPD prevé un contenido mínimo de la evaluación
- Como novedad, se prevé que habrá de recabarse "cuando proceda" la opinión de los interesados

Evaluación de impacto

- Lista de tratamiento de alto riesgo o no (AEPD)
- Actualización Guía Evaluación de Impacto (AEPD)
- GT 29 tratamientos de alto riesgo y evaluaciones de impacto
-
- El RGPD prevé un contenido mínimo de la evaluación
- Como novedad, se prevé que habrá de recabarse "cuando proceda" la opinión de los interesados

Consulta APD

- Consulta a APD cuando una EIPD muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo *"y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación"*
- APD podrá →
  - Asesorar por escrito al responsable, y en su caso al encargado
  - Utilizar cualquiera de sus poderes, incluido prohibir el tratamiento
- Obligación de consulta en elaboración de toda propuesta de medida legislativa o de una medida reglamentaria que la aplique
- El derecho nacional podrá establecer consulta y petición de autorización en tratamientos derivados del ejercicio de una misión realizada en interés público

¿Qué organizaciones están obligadas a designar un DPD?

El RGPD requiere la designación de un **DPD** en tres casos específicos:

- Cuando el tratamiento se realice por una autoridad u organismo público (independientemente de los datos que se estén procesando);
- Cuando las actividades principales del responsable del tratamiento o del procesador consisten en operaciones de tratamiento que exigen un control periódico y sistemático de los datos a gran escala;
- Cuando las actividades principales del responsable del tratamiento o del procesador consisten en procesar a gran escala categorías especiales de datos o datos personales relativos a condenas y delitos penales.

¿Es posible nombrar un DPD externo?

- El **DPD** puede ser un miembro del personal del responsable del tratamiento o del encargado del tratamiento (DPD interno) o «cumplir las tareas sobre la base de un contrato de servicios». Puede ejercerse sobre la base de un contrato de servicios celebrado con un individuo u organización
  - Equipo de personas bajo la responsabilidad del contrato designado
  - Cada miembro del equipo debe cumplir los requisitos del RGPD
- En las Administraciones Públicas puede nombrarse un solo **DPD** para varias entidades

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**

DPD

- **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 y los interesados**
- Comunicación **de su identidad al público**
- Derecho **de acceso por los interesados**
- Información **directa a la dirección**

¿Cuáles son las cualidades profesionales que debería tener el DPD?

El RGPD exige que el DPD «se designe sobre las base de cualidades profesionales y, en particular, conocimientos especializados sobre la legislación y las prácticas en materia de protección de datos y sobre la capacidad para cumplir las tareas a que se refiere el artículo 39»

Habilidades y experiencia :

- Experiencia en las leyes y prácticas nacionales y europeas en materia de protección de datos, incluida una comprensión en profundidad del RGPD
- Comprensión de las operaciones de tratamiento realizadas
- Comprensión de las tecnologías de la información y la seguridad de los datos
- Conocimiento del sector empresarial y de la organización
- Capacidad para promover una cultura de protección de datos
- No se prevé cómo acreditar cualidades profesionales
  - Titulación
  - Acreditación
- El mecanismo de certificación de ENAC

¿Cuáles son los recursos que se deben proporcionar al DPD para llevar a cabo sus tareas?

Dependiendo de la naturaleza de las operaciones de procesamiento y las actividades y tamaño de la organización, deben ser proporcionados al **DPD** los siguientes recursos:

- Apoyo activo de la función del **DPD** por parte de la alta dirección

DPD

- Tiempo suficiente para que los **DPD** cumplan sus obligaciones
- Apoyo adecuado en términos de recursos financieros, infraestructura (locales ,instalaciones, equipo) y personal, cuando corresponda
- Comunicación oficial de la designación del **DPD** a todo el personal
- Acceso a otros servicios dentro de la organización para que los **DPD** puedan recibir apoyo esencial, aportaciones o información de esos otros servicios
- Entrenamiento continuo

¿Cuáles son las salvaguardias que permiten al DPD realizar sus tareas de manera independiente?

- Ninguna instrucción de los controladores o procesadores sobre el ejercicio de las tareas del **DPD**
- Ningún despido o sanción por parte del controlador para el desempeño de las tareas del **DPD**
- No hay conflicto de intereses con otras posibles tareas y deberes

¿Cuáles son las «otras tareas y obligaciones» de un DPD que pueden dar lugar a un conflicto de intereses?

- El DPD no puede ocupar un puesto dentro de la organización que lo conduzca a determinar los propósitos y los medios del tratamiento de los datos personales. Debido a la estructura organizativa específica en cada organización, esto debe ser considerado caso por caso.

DPD

- Como regla general, las posiciones conflictivas pueden incluir posiciones de alta dirección, jefe de Recursos Humanos o jefe de departamentos de TI, pero también otros roles más bajos en la estructura organizativa si tales posiciones o roles conducen a la determinación de propósitos y medios de procesamiento

¿El DPD es personalmente responsable del incumplimiento del RGPD?

No, los **DPD** no son personalmente responsables por el incumplimiento del RGPD. El RGPD deja claro que es el responsable del tratamiento o del procesador quien debe garantizar y demostrar que el tratamiento se realiza de conformidad con el presente Reglamento. El cumplimiento de la protección de datos es responsabilidad del controlador o del procesador.

Responsable y encargado del tratamiento

- Obligación general de diligencia en selección de encargado
- Regulación más detallada que en Directiva → Contrato que fije
  - Objeto, duración, naturaleza y finalidad del tratamiento, tipo de datos personales, categorías de interesados afectados, obligaciones y derechos del responsable del tratamiento
  - Obligación de tratar los datos únicamente siguiendo instrucciones documentadas del responsable

Responsable y encargado del tratamiento

- Confidencialidad de personas que manejen datos
- Medidas de seguridad
- Contratación de subencargados con autorización previa, general o específica, del responsable, y posibilidad de rechazar subencargados
- Asistencia al responsable en ejercicio de derechos y en cumplimiento de obligaciones de arts. 32 a 36 (seguridad, notificación de violaciones de seguridad, evaluaciones de impacto, consulta previa a la AEPD)

Responsable y encargado del tratamiento

- Algunas peculiaridades

- Previsión de que el responsable "realice **auditorías** y contribuya a ellas, incluidas las inspecciones dirigidas por el responsable o por otro auditor autorizado por dicho responsable"
- Fin de la prestación implica **borrado o devolución** de datos, sin incluir transferencia a otro encargado
- Obligación de **informar** al responsable "si, en su opinión, una **instrucción infringe el presente Reglamento** o las disposiciones nacionales o de la Unión en materia de protección de datos"
- Posibilidad de **"contratos modelo"**

Adaptación al RGPD – Sector Privado

Para aquellas empresas y organizaciones a las que no resulte útil Facilita_RGPD, la Agencia ha elaborado una HOJA DE RUTA sobre cómo adaptarse al Reglamento General de Protección de Datos (RGPD), normativa aplicable el 25 de mayo de 2018.

1. Designación del DELEGADO DE PROTECCIÓN DE DATOS (DPD) si es obligatorio para la empresa o si lo asume voluntariamente. En caso de no ser necesario designar un DPD, identificar a la/s persona/s responsables de COORDINAR LA ADAPTACIÓN.
2. Elaborar el REGISTRO ACTIVIDADES DE TRATAMIENTO (servicio de solicitud de copia de la inscripción como ayuda), teniendo en cuenta su finalidad y la base jurídica.
3. Realizar un ANÁLISIS DE RIESGOS (guía práctica).
4. Revisar MEDIDAS DE SEGURIDAD a la luz de los resultados del análisis de riesgos.

Adaptación al RGPD – Sector Privado

5. Establecer mecanismos y procedimiento de NOTIFICACIÓN DE QUIEBRAS DE SEGURIDAD
6. A partir de los resultados del análisis de riesgos, realizar, en su caso, una EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS (guía práctica)

Actuaciones simultáneas a los pasos anteriores:

- Adecuar los FORMULARIOS derecho de información.
- Adaptar los MECANISMOS Y PROCEDIMIENTOS para el ejercicio de derechos
- Valorar si los ENCARGADOS ofrecen garantías y adaptación de contratos
- Elaborar / Adaptar POLÍTICA DE PRIVACIDAD

En todo caso, es imprescindible documentar todas las actuaciones realizadas para poder acreditar la diligencia en el cumplimiento del RGPD.

Códigos de Conducta

- Obligación general de promoción para EEMM, APD, CEPD y COM
- Promovidos por asociaciones y otros organismos representativos de categorías de responsables o encargados
- Objetivo → Especificar aplicación del RGPD
- RGPD recoge contenido indicativo →
  - Intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos
  - Recogida de datos personales
  - Seudonimización de datos personales
  - Información proporcionada al público y a los interesados
  - Ejercicio de los derechos de los interesados…

Códigos de Conducta

- Posibilidad de que haya un organismo específico de supervisión, sin perjuicio de competencias de APD
- Si ese órgano existe → necesidad de incluir mecanismos que permitan el ejercicio de sus funciones de supervisión
- Procedimientos de mediación y resolución extrajudicial de conflictos

Códigos de Conducta

- **Organismo de supervisión**
- **Debe ser acreditado por APD, siguiendo criterios que han de ser aprobados por CEPD**
- **Criterios deben incluir →**
  - **Independencia y pericia**
  - **Procedimientos de evaluación y supervisión**
  - **Procedimientos para atender reclamaciones de interesados**
  - **Ausencia de conflicto de intereses**

Certificaciones

- **Objeto → *"Demostrar el cumplimiento de lo dispuesto en el presente Reglamento" y "permitir a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes"***
- ***Certificación DPD***

Transferencias internacionales

- El Reglamento parte del criterio clásico de que los datos de los europeos sólo pueden enviarse a países que ofrezcan un **nivel adecuado de protección**
- Se amplían y flexibilizan instrumentos de garantía
  - Responsables y encargados pueden ser exportadores
  - **Instrumentos jurídicamente vinculantes** y ejecutables entre autoridades u organismos públicos
  - **BCR** (de responsables y de encargados)
  - **Cláusulas contractuales** estándar aprobadas por la **Comisión**
  - **Cláusulas contractuales** estándar aprobadas por una **APD nacional y aceptadas por la Comisión**
  - **Códigos de Conducta y Esquemas de Certificación**, junto con compromisos vinculantes y ejecutables del responsable o encargado en el tercer país para aplicar las salvaguardas apropiadas, incluidos los derechos del interesado
- Ampliación de excepciones para casos basados **en interés legítimo imperioso del responsable**

Modelo de supervisión

- Acciones correctivas →
  - Sancionar con una advertencia cuando las operaciones de tratamiento previstas puedan infringir RGPD
  - Sancionar con apercibimiento cuando las operaciones de tratamiento hayan infringido RGPD
  - Ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos
  - Ordenar que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, de una determinada manera y dentro de un plazo especificado
  - Ordenar al responsable que comunique al interesado las violaciones de la seguridad de los datos personales
  - Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición

Modelo de supervisión

- Multas deberán ser efectivas, proporcionadas y disuasorias
- Cantidad deberá modularse atendiendo a circunstancias del caso
- Aplicables a responsables y encargados
- Clasificación de infracciones y sanciones
    - Multa hasta 10 M € o para empresas, optándose por la de mayor cuantía, hasta el 2 % de volumen de negocio anual a nivel mundial
        - Obligaciones de responsable o encargado
        - Obligación de organismos de certificación
        - Obligaciones de APD en relación con organismos de supervisión de códigos de conducta

Modelo de supervisión

- Multa hasta 20 M € o hasta el 4%
  - Principios básicos
  - Derechos
  - Transferencias internacionales..
- Multa hasta 20 M € o hasta el 4%
  - Incumplimiento de resoluciones de APD

¡MUCHAS GRACIAS!

Twitter: @AEPD_es