LEGISLACIÓN Y REGULACIÓN

Curso Febrero 2019 – Junio 2019

Prueba de Evaluación Continua 2

PROTECCIÓN DE DATOS DE CARACTER PERSONAL

SUPUESTO PRÁCTICO I (5 puntos)

NOTA: El supuesto tiene muchos elementos, por lo que en esta propuesta de solución se ha partido de la base que el Ayuntamiento ha sido muy cuidadoso en todo el proceso. Dado que al haber varios elementos pueden haber interpretaciones distintas, si estas están bien fundamentadas y llegan a una conclusión distinta a la propuesta no necesariamente significa que esté sea incorrecto.

En esta propuesta de solución me extiendo más de lo estrictamente necesario dado que aprovecho para introducir cortas aclaraciones que no tienen por qué estar en la pec que habéis presentado.

CUESTIONES

Después de haber estudiado el RGPD y los demás documentos contesta razonadamente a las siguientes cuestiones:

1. Analiza la problemática que plantea el caso.

   Para ello, en este apartado ponemos de relieve los elementos que intervienen en el suceso, con una explicación.

   Tipología de datos tratados: De acuerdo con el enunciado se tratan datos relativos a menores. También nos dice el enunciado que no se utilizan datos identificativos, sino un identificativo consistente en el número de expediente, ello como veremos después nos remite al concepto de seudonimización.

   Así pues, se cumple perfectamente el art. 4. 1) del RGPD son datos personales. Además se tratan categorías especiales de datos. El art. 9.1 del RGPD establece la prohibición general del tratamiento de los datos de categorías especiales, entre los cuales se cuentan los datos de salud. Sin embargo, el art. 9.2 RGPD establece algunas excepciones a la prohibición general de tratamiento entre la que se cuenta (apartado h)) cuando el tratamiento sea necesario por razones de interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros (...). Añadir que los considerandos 52 y 53 del RGPD destacan que la excepción es aplicable, entre otros, en el ámbito de la legislación sobre protección social, con fines relacionados con la salud cuando sea necesario para lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, incluido en el contexto

de la protección social.

NOTA: podéis haber considerado o no que está amparado bajo razones de interés público. Cualquiera de los presupuestos tiene sus argumentos.

Anonimización: El art. 4.5 del RGPD establece el concepto de seudonimización como el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a mediadas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. Contrariamente a lo que pasa con los datos anonimizados, los datos seudonimizados deben considerarse información personal (Considerandos 26 y 28 RGPD), ya que las personas pueden identificarse. Los profesionales que integran el área de Servicios Sociales pueden identificar, de hecho es lo que hacen, a los menores.

Tratamiento: El RGPD adopta un concepto amplio de tratamiento de datos (art.4.2) hasta el punto que cualquier actividad sobre los datos personales es considerada tratamiento de datos. El tipo de tratamiento que se efectúa es la elaboración de perfiles.

Encargado del Tratamiento: Nos podríamos preguntar si la empresa encargada de realizar el algoritmo y de su posterior mantenimiento puede ser considerado un encargado de tratamiento. Si bien se podría alegar que para la creación del algoritmo no necesita trabajar con datos reales, lo cierto es que si se encarga del mantenimiento del mismo, a la práctica, podría tener acceso a datos reales, máximo teniendo en cuenta que en muchos ayuntamientos no tienen personal especializado para solucionar los problemas que se pueden presentar. Por ese motivo puede considerarse que se trata de un encargado de tratamiento.

Responsable del Tratamiento: El Ayuntamiento es el responsable, y como tal deberá garantizar la seguridad adecuada y establecerá las medidas técnicas y organizativas apropiadas que impidan el tratamiento no autorizado, la pérdida, destrucción o daño accidental de los datos. Es, por tanto, quien determina los fines y medios del tratamiento, en este caso los fines vienen determinados en la Ley por tratarse de una AAPP (art.4.7 RGPD).

Delegado de protección de datos (DPD): Al tratarse de una administración pública deberá haber designado un DPD, de acuerdo con el art. 37 1.a).

Elaboración de perfiles: El art. 4.4 del RGPD define la elaboración de perfiles como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos a la personalidad, la salud, preferencias, etc. Por tanto, el objetivo es evaluar determinados aspectos personales. El WP251 sobre decisiones individuales y elaboración de perfiles del GT29 (en adelante WP251) remarca que la simple clasificación de individuos basada en características de edad, sexo o altura no necesariamente se encuadra en el concepto de elaboración de perfiles, ello dependerá de la finalidad de la misma. El

GP29 aclara que únicamente cuando la finalidad sea la evaluación de las características de una persona se entenderá como elaboración de perfiles. Para una mejor comprensión del concepto de lo que debemos entender por elaboración de perfiles de acuerdo con el RGPD, conviene tener en cuenta la Recomendación CM/Rec (2010) del Consejo de Europa.

Toma de decisiones individuales automatizadas (art.22 RGPD): La creación de perfiles no siempre implica la toma de decisiones individuales automatizadas. Si bien podrían utilizarse conjuntamente, no es requisito necesario. La toma de decisiones individuales automatizadas es la habilidad de tomar decisiones únicamente por medios tecnológicos, sin que intervenga el factor humano. Podemos decir que se crean perfiles de menores, ya que se tratan datos de menores y de sus familias, se analizan automáticamente los mismos para establecer correlaciones y los resultados de éstas se aplican a los menores. Sin embargo, en ningún caso se toman decisiones automatizadas sobre los menores, porque siempre interviene el factor humano para la toma de decisiones sobre los menores. El resultado del algoritmo es evaluado por el Equipo de Valoración de los menores que teniendo en cuenta todas las circunstancias de la Unidad familiar adoptará una determinada decisión sobre las acciones de prevención. Por lo tanto, es el Equipo de Valoración quien toma la decisión en base al algoritmo y al resto de circunstancias que conforman cada caso particular.

NOTA: podéis haber considerado o no que hay una decisión individual automatizada. Está claro que no, pero dado que es un punto conflictivo he dado como correcto cualquiera de las dos posibilidades.

Consentimiento: Es otro de los puntos problemáticos. Si se considera que no hacía falta entonces hay que considerar que hay un uso distinto al inicial pero compatible con el fin inicial. Si se considera que si era necesario, entonces está claro que el ayuntamiento debe haber recogido el consentimiento de todas las familias con las que ha hecho el tratamiento.

Uso de datos para otros fines distintos al inicial (considerando 50 y art.89.1 RGPD): El ayuntamiento puede haber "cogido" los datos de sus bases de datos para este tratamiento y por lo tanto estaría haciendo un uso distinto al inicial por el que el interesado dio su consentimiento. Es otro de los 'problemas', dado que inicialmente se podría haber supuesto que está todo bajo el paraguas de *razones de interés público* o no.

NOTA: Cualquiera de los dos presupuestos tiene sus argumentos, de modo que es posible haber considerado uno u otro. Tened presente que partiendo en función de la posibilidad elegida, los artículos en que sustentar el argumento varian.

2. Explica qué medidas generales habría de cumplir el tratamiento que se pretende realizar.

   De hecho es una pregunta general sobre el tratamiento, no sobre las obligaciones del RT. Más concretamente sobre los principios generales aplicables a los tratamientos de datos personales. Teniendo en cuenta que el tratamiento se encuentra dentro de la creación de perfiles, el considerando 72 del RGPD aclara que la elaboración de perfiles está sujeta a las normas establecidas en el mismo que rigen el tratamiento de datos personales. Así pues, no hay medidas excepcionales para este tipo de tratamiento y por lo tanto nos remitimos a los principios generales aplicables a los tratamientos de datos en el RGPD.

   Art. 5.1 (a) Licitud, lealtad y transparencia.

   Art. 5.1 (b) Limitación de la finalidad y tratamiento ulterior de datos.

   Art. 5.1 (c) Minimización de datos Art.

   Art. 5.1 (d) Exactitud

   Art. 5.1 (e) Limitación del plazo de conservación.

   Art. 5.1 (f) Integridad y confidencialidad.

   Finalmente, hay que verificar que el tratamiento es lícito (Art. 6 RGPD)

3. Antes de empezar a tratar datos, el Ayuntamiento deberá adoptar una serie de medidas de cumplimiento normativo aplicables a este tipo de tratamientos. Enuméralas y explica en qué consisten.

   A parte de las obligaciones generales que deberá cumplir el Ayuntamiento como responsable del tratamiento en relación a los tratamientos que realiza, en este caso concreto, por la tipología de tratamiento de que se trata, antes comenzar el tratamiento deberá realizar una evaluación de impacto de protección de datos (EIPD). Será necesario realizar una EIPD cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos fundamentales y las libertades de las personas. El art. 35.3 a) se refiere a la obligación de llevar a cabo una EIPD cuando se elaboren perfiles, sobre los cuales se tomen decisiones sobre las personas que produzcan efectos jurídicos sobre las mismas o que les afecten significativamente de manera similar.

   De acuerdo con la interpretación que realiza el WP251 del art. 35.3 (a) el RT deberá llevar a cabo una EIPD cuando pretenda hacer un tratamiento que consista en la elaboración de perfiles para la toma de decisiones que produzcan efectos legales o similares significativos efectos jurídicos sobre las personas, incluso cuando el tratamiento no se realice de manera totalmente automatizada, es decir, incluso en los casos en los que exista intervención humana. Por descontado que también se deberá llevar a cabo en los casos de decisiones individuales totalmente automatizadas (art.22.1).

   El Ayuntamiento, como RT deberá velar por el cumplimiento del Art 32

(seguridad del tratamiento) por parte del ET (encargado del tratamiento).

El ayuntamiento deberá diseñar el tratamiento, adoptar políticas internas y aplicar medidas que cumplan los principios de protección de datos desde el diseño y por defecto (art 25).

Finalmente, tened presente que una EIPD resultará útil para determinar las medidas técnicas y organizativas que el RT deberá aplicar al tratamiento.

> Artículos como la seguridad del tratamiento (art 32), la revisión de las bases jurídicas del tratamiento (art 6), la elaboración del registro de actividades del tratamiento (art 30) o la designación de un DPD (art 37) entre otras no dependen de este caso concreto y por tanto son las 'normales' en cualquier situación)

4. ¿Cuál sería la base legal del tratamiento en este caso? Razona la respuesta.

   Las situaciones en que es lícito el tratamiento de datos están recogidas en el artículo 6. El RGPD ofrece seis bases legales para la recopilación y el procesamiento de datos en Europa. Por lo tanto, para recopilar datos personales de cualquier tipo, debe haber una base legal:

   - Interés vital del individuo
   - Interés público
   - Necesidad contractual
   - Cumplimiento de obligaciones legales
   - Consentimiento inequívoco del individuo
   - Interés legítimo del responsable del tratamiento de datos

   A señalar que estas seis bases legales tienen el mismo valor legal, lo que significa que son autosuficientes y exclusivas entre sí. Así pues, el tratamiento resultará ilegal cuando no podamos demostrar que tratamos los datos de acuerdo con alguna de las bases legales recogidas en el Reglamento.

5. ¿Qué medidas tendría que adoptar el Ayuntamiento respecto a la empresa que desarrollará el algoritmo?

   El Ayuntamiento (como responsable del tratamiento) está obligado a ejercer el control y la supervisión del encargado de tratamiento. Para ello deberá establecer medidas precontractuales (due diligence), contractuales (establecidas como obligatorias en el RGPD y postcontractuales (auditorias, inspecciones, etc). Todo ello para dar cumplimiento a las obligaciones que el RGPD le exige.

   El art. 28.1 obliga al RT a elegir únicamente a un ET que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, para que el tratamiento cumpla los requistos exigidos en el

RGPD y para garantizar la protección de los datos. Tal como se ha comentado, una EIPD guiará al RT para poder exigir las medidas adecuadas. Otra de las obligaciones que impone el RGPD es la necesidad de subscribir un contrato de tratamiento, cuyo contenido mínimo se especifica en el art. 28.3. RGPD. El contrato deberá constar por escrito, inclusive en formato electrónico (Art. 28.9)

6. ¿Qué garantías deberá ofrecer el algoritmo?

   Cumplimiento de las medidas técnicas y organizativas. Se deberán aplicar las medidas técnicas y organizativas que garanticen un nivel adecuado de seguridad para los datos personales, de acuerdo con el resultado de la EIPD y lo prescrito en el art.32 del RGPD.

   Auditoria. Una de las recomendaciones del WP251 es que el algoritmo sea auditado por terceros. Por eso el Ayuntamiento debería exigir a la empresa desarrolladora que aporte garantías de que el algoritmo ha sido testado y auditado por una empresa externa y que cumple los estándares de seguridad, que podrá acreditarse mediante certificaciones.

   Privacidad por diseño y por defecto. Otro aspecto a tener en cuenta es la privacidad desde el diseño y por defecto (art. 25 RGPD). El RT deberá aplicar a los medios de tratamiento (en este caso al tratamiento de los datos por medio de un algoritmo predictivo), medidas como la seudonimización, la minimización de datos e integrar las garantías adecuadas para proteger los derechos de las personas (art. 25.1). Además, por defecto únicamente tratará los datos necesarios para alcanzar los fines específicos del tratamiento, su accesibilidad limitada únicamente a las personas con autorización de acuerdo al establecimiento de roles preestablecida, la encriptación de los datos, entre otras (art.25.2).

   El problema que plantea este tipo de tratamiento es la posibilidad de que los resultados produzcan errores o resultados injustificables. De, todo ello sin las debidas garantías podría comportar incluso situaciones discriminatorias

7. Supongamos que los padres de algunos de los menores se oponen al tratamiento:

   a) ¿Cómo debería actuar el ayuntamiento?

   De acuerdo con el art 12.2, "El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22.". El RT deberá facilitar los derechos en el plazo de un mes desde la recepción de la solicitud (art 12.3). Por otro lado, cuando el RT considere que no es procedente el ejercicio del derecho que se solicita deberá igualmente contestar en el plazo del mes desde la solicitud, alegando los motivos de la no actuación e informando a la persona de que puede presentar una reclamación ante la autoridad de control y de ejercitar acciones judiciales (art.12.5 RGPD).

   Por lo tanto tienen derecho a saber los fines, categorías….y en el caso de decisiones automatizada, "información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado". (art 15).

El art. 21 del RGPD recoge el derecho de oposición al tratamiento. De acuerdo con el mismo, la persona podrá oponerse en cualquier momento, por motivos relacionados con su situación particular, a que sus datos sean tratados en algunos supuestos, entre los cuales se encuentra cuando el tratamiento se realice para el cumplimiento de una misión en interés público (art. 6.1 e)).

Así pues, el Ayuntamiento debería dejar de tratar los datos, salvo que se dé alguna de las dos circunstancias contempladas en el art 21.1.

b) ¿Estaría obligado el ayuntamiento a hacer efectivo el derecho de oposición en todas las circunstancias? Razona la respuesta.

Hay dos supuestos en que no estaría obligado (art 21.1).

- Cuando el RT acredite motivos legítimos imperiosos para el tratamiento y demuestre que estos prevalecen sobre los intereses, derechos o libertades del interesado.

- Para la formulación, ejercicio o la defensa de reclamaciones.

8. El algoritmo ha clasificado a un menor concreto en situación de riesgo de abuso infantil. Los progenitores del menor no están conformes con el resultado de la clasificación y han pedido al ayuntamiento una explicación y una evaluación en profundidad de su caso. Sin embargo, el ayuntamiento se niega a dar una explicación alegando que el algoritmo únicamente predice la mayor probabilidad de padecer abusos por parte del menor y no que realmente vaya a padecerlos.

a) ¿Podría el ayuntamiento tener problemas por no acceder a la petición de los padres si éstos reclamaran ante la Agencia Española de Protección de Datos?

Dado que los padres no están de acuerdo con el resultado les asiste el derecho de acceso (art. 15 RGPD) y el derecho de rectificación si procede (art. 16 RGPD). Así pues, el Ayuntamiento está obligado a proporcionar pues no piden acceder a los datos, sino una explicación porqué los padres no están conformes. El perfil únicamente refleja la mayor posibilidad de que la situación analizada sea real. Por todo ello, la persona tendría derecho a que se revisara su caso

Los padres están ejerciendo el derecho de rectificación del art. 16 RGPD.

La creación de perfiles supone un componente de predicción, el cual incrementa el riesgo de inexactitud. El art. 16 RGPD se aplica cuando un individuo es colocado incorrectamente en una categoría que lo clasifica como en este caso potencial víctima de abusos. Podría darse el caso que la clasificación estuviera basada en información incorrecta. Es por ello que las personas tienen derecho a cuestionar la exactitud de los datos utilizados o la categoría que se les ha aplicado. Tal como se señala en el WP251, este derecho no solo se aplica a los datos utilizados para la creación del perfil, sino también al perfil creado.

b) ¿Crees que la AEPD podría considerar que se ha vulnerado algún derecho? Razona la respuesta.

Si el Ayuntamiento no accede a revisar el caso estaría vulnerando el derecho de rectificación del art.16 y podría ser

sancionado de acuerdo con el régimen sancionador establecido en los arts. 83 y 84 del RGPD. Al tratarse de una AAPP no se establecería una sanción económica.

SUPUESTO PRÁCTICO II (5 puntos)

El 17 de septiembre de 2018 se publicó que la escuela de negocios IESE había sido víctima de una ciberataque perpetrado por "La Nueve" grupo vinculado a "Anonymous".

En este ejercicio se pretende realizar un estudio del caso circunscrito únicamente a la legislación relativa a la protección de los datos personales (RGPD). Por tanto obviaremos otros aspectos del caso.

Para determinar los hechos nos basaremos en las informaciones aparecidas en los medios de comunicación y en algunos de los tuits publicados que encontraréis en el aula.

CUESTIONES

1. Analiza los hechos del caso y el incidente de seguridad en base a las informaciones aportadas y otras que consideres relevantes.

   Elementos que intervienen incluyen varios tuits, capturas de pantalla,

   Hechos:

   El acceso no autorizado al sistema informático de IESE.

   El acceso a información personal (e incluso copia) de datos personales y correos electrónicos.

   Suplantación de identidad de usuarios.

   Ataques repetidos al servidor web.

   Infracción: Con las informaciones publicadas, la escuela de negocios podría haber infringido el art. 32 del RGPD, pues no estaría aplicando las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado para el riesgo del tratamiento.

   Consideraciones técnicas:

   Existencia de un servidor en el que es posible acceder al sistema de directorios. Está corriendo en Windows XP i ASP.Net, y el fabricante ya no da soporte desde abril de 2014.

   Consideraciones jurídicas del incidente:

   a). Se deberá determinar si estamos ante un incidente de seguridad que afecta a datos personales. El RGPD define "violación de seguridad de los datos personales" toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados (art. 4.12). Es evidente que en este caso, como mínimo, hay un acceso no autorizado a datos personales.

   b). Se deberá determinar el perjuicio que la brecha de seguridad ha causado o puede causar a los derechos y libertades de los afectados,

determinando el grado de severidad del incidente y las posibles consecuencias para las personas. Entre otros se analizará: perfil de usuarios afectados, número de sistemas, impacto el incidente en la organización, etc. También será útil recurrir al análisis de riesgos o a la EIPD si se ha realizado para este tratamiento, lo cual nos ayudará a determinar la peligrosidad potencial del incidente y la magnitud del daño para los derechos y libertades de las personas.

c) Clasificación del incidente teniendo en cuenta si se trata de una brecha de confidencialidad, integridad o disponibilidad. En este caso todo apunta que estamos ante una brecha que afecta a la confidencialidad de los datos puesto que los datos se han hecho públicos.

2. Explica cómo debería proceder IESE ante este incidente de seguridad y describe los pasos que debería de tomar para cumplir con el RGPD.

   Dejando de lado el proceso interno que deberá seguir IESE para gestionar la brecha de seguridad de los datos personales y que deberéis establecer en el Plan de Gestión o de Respuesta a incidentes de seguridad que afecten a datos personales, aquí nos centraremos en las obligaciones del RT establecidas en el RGPD.

   Una vez se tenga conocimiento de la violación de seguridad que afecta a los datos personales, IESE deberá notificarlo a la Autoridad de Control correspondiente, en este caso a la AEPD. La notificación se deberá realizar dentro del plazo de las 72 horas desde que se tiene conocimiento de la violación de seguridad (art.33.1). El contenido mínimo que deberá tener se establece en el art. 33.3 del RGPD. La AEPD tiene establecido en su sede electrónica un trámite para la notificación de las violaciones de seguridad.

   Además de la notificación, el RGPD obliga a comunicar la violación a las personas afectadas cuando de la valoración del incidente se desprenda que exista la probabilidad que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, lo cual deberá hacerlo sin dilación indebida (art.34.1 RGPD).

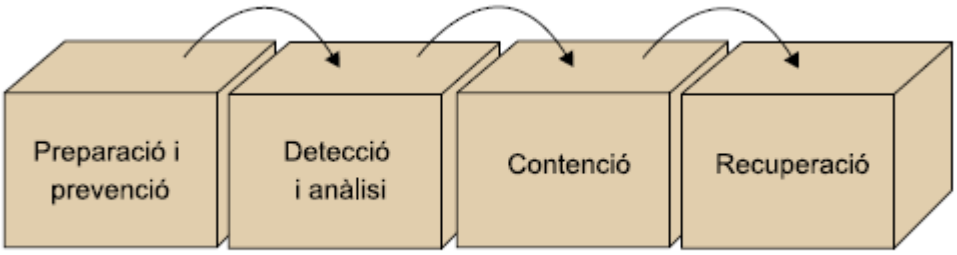
3. Como consecuencia del incidente de seguridad la escuela de negocios se arriesga a una sanción económica y al menoscabo de su reputación. Para que no vuelva a pasar, IESE quiere establecer un Plan de Respuesta a Incidentes de Seguridad que resulte efectivo. Imagínate que te ha contratado para que elabores dicho plan.

   En esta pregunta se requiere que elabores un documento que contenga el procedimiento de gestión de incidentes de seguridad cuando afecten a los datos personales.

   La información para realizarla, ejemplos y el esquema los podéis encontrar en la Guía de Brechas de Seguridad de la AEPD

   https://www.aepd.es/media/guias/guia-brechas-seguridad.pdf

   En general la gestión de incidentes de seguretat tiene 4 grandes bloques, prevención, detección, contención y recuperación.



Esquema bàsic de la gestió d'incidents

No es objeto de esta asignatura entrar en detalle de cada bloque. Si hay que mencionar de forma muy especial, que la Guia de la AEPD añade un paso, que en este caso estaría dentro de la recuperación, que es la notificación de brechas de seguridad a la autoridad competente.