CNS 34/2014

Dictamen en relación con la consulta planteada por una entidad de derecho público sobre el modelo de gestión y de servicios para dar valor a la información del sistema sanitario catalán en el marco de las políticas públicas (en adelante VISC+)

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de una entidad de derecho pública (en adelante, la entidad), en el cual solicita que la Autoridad valore la adecuación de las medidas de seguridad que se aplicarán sobre los datos incluidos en el ámbito del contrato VISC+, a la legislación en materia de protección de datos, que se describen en los documentos que se adjuntan a la consulta.

En concreto, se adjunta copia del Documento Administrativo de solución final VISC+ (en adelante, DA), del Documento Técnico de solución final VISC+ (en adelante, DT), y del Documento de procedimiento para la cesión de datos personales anonimizados de salud al Adjudicatario de VISC+ para investigación médica y evaluación, que incluye, como anexos, los Estatutos de la entidad (anexo 1), el documento de encargo de gestión (anexo 2), y el documento sobre el procedimiento de anonimización (anexo 3).

Analizada la consulta y la documentación que la acompaña, vistos los informes del Coordinador de Auditoría y Seguridad de la Información de la Autoridad, y de la Asesoría Jurídica, emito el siguiente dictamen.

I

(...)

II

Objeto de la consulta

A través de la consulta formulada, la entidad expone que está licitando un contrato de colaboración publico privada para la implantación y la operación de un modelo de gestión de servicios para dar valor a la información del sistema sanitario catalán en el marco de las políticas públicas (VISC+). Se añade que en este marco contractual se regulan los mecanismos y procesos de seguridad que serán aplicables sobre los datos incluidos en el alcance del contrato, y que tienen que asegurar el cumplimiento de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD).

En relación con el proyecto VISC+, la entidad solicita informe sobre la adecuación de las medidas de seguridad que se aplicarán sobre los datos incluidos en el objeto del contrato VISC+, a la legislación en materia de protección de datos.

En lo que se refiere al alcance de este informe, tal como se plantea en la consulta, se centrará en aspectos relativos a las medidas de seguridad, pero las consideraciones sobre estos aspectos no se pueden desvincular de los principios y obligaciones derivados de la normativa de protección de datos. Por ello, y a partir de la documentación aportada, también se analizarán, con carácter previo algunas

cuestiones generales sobre el alcance, las características del proyecto y las garantías necesarias para el cumplimiento de la normativa de protección de datos.

Por otra parte, este dictamen tiene por objeto el análisis del modelo de seguridad y anonimización de los datos que se describe básicamente en el Anexo 1 del DT, relativo al *"modelo de seguridad, disponibilidad y uso de los datos*", para comprobar si se adecua a la normativa de protección de datos y hacer aquellas consideraciones que, desde la perspectiva de la protección de datos, se consideren pertinentes para mejorarlo. Pero hay que dejar claro que el objeto de este dictamen no consiste en validar un determinado modelo de seguridad, cuestión que por otra parte no sería posible debido a la falta de concreción de diferentes aspectos relacionados con la seguridad. La validación del sistema de seguridad es algo que sólo se puede llevar a cabo después de un acurado procedimiento de auditoría que se tendrá que poner en práctica una vez esté implementado. Por ello, en el punto 3.1 del DT, debería hacerse referencia a que el modelo del Anexo 1 del DT ha sido objeto de Dictamen de la Autoridad, y no de validación. En cualquier caso, se valora positivamente la previsión que las futuras modificaciones del Modelo de seguridad, disponibilidad y uso de los datos, de dicho Anexo 1, también se someterán a la opinión de la Autoridad.

III

Descripción del proyecto

La consulta planteada por la entidad, trae causa del contrato de colaboración publico privada para el diseño, implantación y operación de un modelo de gestión y servicios para dar valor a la información del sistema sanitario catalán.

La entidad que formula la consulta es una entidad de derecho público de la Generalitat sometida al ordenamiento jurídico privado, adscrita al departamento competente en materia de salud de la Generalitat de Catalunya, con personalidad jurídica propia, autonomía administrativa y financiera y plena capacidad de obrar para el cumplimiento de sus objetivos y sus funciones, y actúa, en el marco de las funciones que le atribuyen sus Estatutos, bajo las directrices de dicho departamento, el cual ejerce el control de eficacia y eficiencia sobre su actividad. Son objetivos de la entidad generar el conocimiento relevante para contribuir a la mejora de la calidad, seguridad y sostenibilidad del sistema de salud de Cataluña que faciliten la toma de decisiones a la ciudadanía, a los profesionales y a los gestores del ámbito de la salud, y a los órganos responsables de la planificación en salud, así como facilitar la implicación de los profesionales sanitarios en el sistema y su corresponsabilidad en la consecución de las finalidades comunes y la calidad de la atención (artículo 2 del Decreto 97/2013). Entre otras funciones, corresponde a la entidad definir, impulsar y desplegar la estrategia del sistema de información y las tecnologías de la información y comunicación del sistema de salud de responsabilidad pública, así como llevar a cabo la gestión y el mantenimiento de los elementos comunes y/o unificados del sistema de información del sistema sanitario integral de utilización pública de Cataluña (SISCAT) y su explotación y rendibilización garantizando, de acuerdo con las directrices del departamento competente en materia de salud, la disponibilidad de la información del sistema sanitario de Cataluña, haciéndola accesible e interoperable al servicio de una asistencia sanitaria de calidad, de acuerdo con la política corporativa de la Generalitat de Catalunya en materia de telecomunicaciones y tecnologías de la información, según los Estatutos de la entidad.

El Plan de Gobierno 2013-2016, incluyó el "proyecto VISC+ (Valorización de Información del Sistema Sanitario Catalán), entre los proyectos de interés para el Eje de Cohesión Social y servicios de interés público, incluido en dicho Plan de Gobierno.

Hay que decir que al elaborar este dictamen no se ha dispuesto de una memoria global que describa de una manera detallada las necesidades, las alternativas disponibles y las características (flujos de información, características del sistema de anonimización de datos, colectivos concretos afectados, etc.) y los beneficios de la opción escogida. Sólo se dispone de diversos documentos -descritos en el apartado de antecedentes de este informe- que, desde perspectivas diferentes, describen diferentes aspectos del proyecto. Así, algunos de los documentos aportados parece que forman parte de la documentación contractual de la relación entre la entidad y el Adjudicatario (DA y DT), otros se refieren a la relación entre los responsables del fichero y la entidad (Encargo de servicios) y otros no resulta clara qué naturaleza tienen (Documento sobre procedimiento para la cesión).

Hay que decir también que, vistas las fuertes implicaciones para la privacidad de las personas y para los otros derechos que se podrían ver afectados en caso de un tratamiento inadecuado de una información tan sensible como la que se incluye en el proyecto, **sería recomendable disponer de una evaluación del impacto sobre la privacidad** que puede tener esta iniciativa. La elaboración de este estudio, que actualmente no es preceptivo de acuerdo con la normativa vigente en materia de protección de datos, se alinearía con las previsiones del proyecto de Reglamento europeo de protección de datos que actualmente se está tramitando, el cual prevé, entre otros, la elaboración, por parte del responsable del tratamiento, de una evaluación del impacto sobre la privacidad cuando se lleven a cabo tratamientos a gran escala de datos de salud.

Esta evaluación tendría que incluir una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas previstas para hacer frente a los riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la conformidad con la normativa de protección de datos. En este sentido, la Agencia Española de Protección de Datos ha publicado recientemente una *"guía para una evaluación de impacto en la protección de datos*", disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php .

En síntesis, por lo que se desprende de los diferentes documentos aportados, el esquema del Proyecto VISC+ es el siguiente:

La constitución de un encargo del tratamiento (artículo 12 LOPD) entre el Departamento de Salud, el Servicio Catalán de la Salud (CATSALUT) y el Instituto Catalán de la Salud (ICS), como responsables de los ficheros de datos implicados en el Proyecto, y la entidad, como prestador de servicios y encargado del tratamiento, tiene que permitir que la entidad proceda a anonimizar la información a fin de que el Adjudicatario, a quien se le comunicaría la información, la facilite a terceros (clientes o usuarios finales).

También se prevé que la entidad pueda ceder directamente a terceros datos personales no anonimizados, previa comprobación, por parte de la entidad, que el cesionario dispone de los consentimientos correspondientes de los afectados y de una auditoría de cumplimiento de la LOPD.

El Adjudicatario se encargará de definir, construir y poner en marcha un catálogo de servicios útil, eficiente, competitivo e innovador, y contrastar las necesidades del mercado y de los clientes finales del proyecto, así como definir un plan de difusión y de comercialización, canalizando de manera adecuada la demanda del mercado nacional e internacional. También tendrá que ejecutar otros proyectos o iniciativas relacionadas con VISC+, y crear un centro de competencia en analítica en datos de salud, las funciones y composición del cual se describen en el apartado 3.4.1 del DT.

El Proyecto articula un doble procedimiento de cesión de datos personales:

a) Procedimiento para la cesión de datos anonimizados de salud al Adjudicatario para investigación médica y evaluación (punto 1 del Documento *Procedimiento para la cesión de datos(...),* que al mismo tiempo facilitaría los datos a los clientes finales.

b) Procedimiento para la cesión de datos de salud no anonimizados para investigación médica y evaluación al usuario final (punto 2 del mismo Documento*).* Este segundo procedimiento tiene la particularidad que los datos serían cedidos directamente al usuario final por parte de la entidad.

Si bien no todos (pues también se prevé tratar ficheros como el Registro sanitario de empresas e industrias, o el Registro de personal docente, a modo de ejemplo), la mayoría de los ficheros afectados por el Proyecto VISC+ contienen datos de salud. Si tenemos en cuenta el alcance de los datos que la entidad prevé poner a disposición del Adjudicatario tanto inicialmente como en incorporaciones futuras (punto 2.2.2 del DT) claro está que los datos de salud conforman la principal fuente de información del Proyecto analizado.

La LOPD establece un régimen de protección reforzado en relación con determinadas tipologías de datos personales, entre otros, los datos de salud, entendiendo como tales las informaciones que conciernen la salud pasada, presente y futura, física o mental, de un individuo, así como las referidas a su porcentaje de discapacidad y a su información genética (artículo 5.1.g) RLOPD), que se traduce en una serie de garantías (artículos 7 y 8 de la LOPD) y la exigencia de la aplicación de medidas de seguridad de nivel alto (art. 81 RLOPD).

Dado que el Proyecto VISC+ tiene por objetivo desarrollar un modelo de gestión que permita dar valor a la información que genera el sistema sanitario catalán, en la medida en que ello implique, principalmente, el tratamiento de datos de salud, tendrá que atender a este régimen de protección previsto en la LOPD para los datos sensibles, y a las previsiones de la normativa sectorial aplicable. Los datos que conforman la historia clínica (HC) se recogen para realizar el tratamiento médico que requiere el paciente, principalmente y, si procede, para otros usos o finalidades, previstos en la normativa específica, en concreto, la Ley 41/2002, de 14 de noviembre, estatales, reguladoras de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que regula con carácter básico determinadas cuestiones relativas a la HC y los derechos de los pacientes, así como, en el ámbito de Cataluña, la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y a la documentación clínica. De acuerdo con esta normativa para tratar los datos que constan en la HC, será necesario el consentimiento de su titular, salvo que concurra alguna de las excepciones previstas en la ley o que se anonimice la información (artículos 16.3 de la Ley 41/2002 y 11.3 de la Ley 21/2000).

IV

Sobre la información que se tratará en el proyecto Visc+

Desde la perspectiva de la protección de datos hay que partir de la base que la recogida y el posterior tratamiento de datos personales tiene que dar cumplimiento a lo que dispone la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica (LOPD y RLOPD).

El artículo 4.1 del LOPD recoge el principio de calidad de los datos, que en su vertiente de proporcionalidad, establece lo siguiente:

> *"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*

Este principio de proporcionalidad en un proyecto como el que nos ocupa desplegará sus efectos tanto desde el punto de vista de los ficheros que tienen que formar parte del proyecto, como de la información que se podrá comunicar a los clientes finales.

Con respecto a los ficheros afectados por el Proyecto VISC+, según lo que se describe en el documento relativo al encargo de servicios, son ficheros responsabilidad del Departamento de Salud (19 ficheros), del CATSALUT (10 ficheros) y del ICS (3 ficheros), que la entidad podrá tratar en base a un contrato de encargo del tratamiento al que nos referiremos más adelante. También se explicita, en el Documento relativo al encargo del tratamiento - *"encargo de servicios de anonimización (...)"-,* determinados ficheros que quedan fuera del alcance del proyecto.

Ahora bien, hay que señalar que según el apartado 2.2.2 del DT, la entidad pondrá al alcance del Adjudicatario *"toda la información anonimizada"* que se genere en el SISCAT. Hay pues una discordancia que tendría que llevar a rectificar el apartado 2.2.2.

En cualquier caso, con respecto a los ficheros afectados, hay que valorar positivamente que, a pesar del gran número de ficheros mencionados en el Documento de encargo de servicios de anonimización, el DT prevea un "*alcance inicial*" limitado de los datos que estarán disponibles en un primer momento del Proyecto (apartado 2.2.2.1 del DT). En esta línea el apartado 5.2.1 del DT prevé que "*En la Fase 1 del proyecto se consensuarán qué fuentes de datos, de entre las incluidas en el alcance inicial, se pondrán a disposición del Adjudicatario una vez se haya construido y validado el proceso de anonimización de acuerdo con el modelo de seguridad* (...)". De ello parece poder inferirse que, en atención a los resultados que se puedan obtener inicialmente, la incorporación de nuevos ficheros y de nuevos datos tendrá en cuenta la experiencia alcanzada a la hora de valorar la viabilidad y la proporcionalidad.

Pero este principio, aparte de regir en el momento de la puesta a disposición de la entidad de los ficheros afectados, se deberá tener presente también en el momento de la comunicación de los datos concretos necesarios para las finalidades que pretendan llevar a cabo los clientes finales. Especialmente si se trata de datos personales, pero también si se trata de datos anonimizados.

La información entregada a los clientes finales sería, en buena parte, datos de salud de los afectados, contenidos en la HC - o datos anonimizados obtenidos a partir de éstos. Desde la perspectiva del principio de calidad, hay que tener en cuenta que el contenido de la HC, definido en la normativa (fundamentalmente artículo 15.2 Ley 41/2002, y artículo 10 Ley 21/2000) es amplio, de manera que se contienen datos sensibles, informes relativos al paciente, y otros que pueden dar información de terceras personas, como los antecedentes familiares. Teniendo esto en cuenta, cuando se lleve a cabo la cesión y cuando se articule el correspondiente consentimiento informado, hay que limitar la cesión de datos sólo a aquellos que sean relevantes a los efectos del estudio o investigación que se quiera llevar a cabo por parte del cliente final.

Ello, que es esencial en el caso de los datos personales no anonimizados, es relevante también para al caso de los datos anonimizados, porque no hay que perder de vista que en el entorno del *big data* el cruce de información obtenida de orígenes diversos, incluso si ha sido anonimizada, puede acabar haciendo identificable una persona. Por ello, para intentar reducir en estos casos los riesgos de reidentificación también sería necesario limitar los datos comunicados a los mínimos indispensables para alcanzar la finalidad pretendida por el cliente final. Y dentro de los datos anonimizados, es todavía más relevante en aquéllos que se ofrecen en abierto. Por ello, vistos los riesgos inherentes, hay que ser muy restrictivo con la información de salud que se ofrezca en abierto, a menos que se ofrezca con niveles de agregación sobradamente amplios.

Cuando en el apartado 3.2.1 del DT se refiere a los datos abiertos no se concreta cuáles serán estos datos ni los criterios y el procedimiento que se seguirán para decidir qué datos tendrán que estar accesibles en abierto. Sería conveniente que ya desde esta fase de diseño del proyecto se aclararan estos extremos.

En cualquier caso, éste es el único supuesto (servicios de datos abiertos) en que el DT examinado explicita que se trabajará con "datos anonimizados", mientras que en el resto de servicios identificados no se explicita si los clientes finales podrían recibir y tratar información anonimizada o datos personales no anonimizados.

El principio de minimización en el tratamiento de los datos personales, del cual se deriva que si una finalidad se puede alcanzar sin necesidad de tratar datos personales, se tiene que optar por esta posibilidad, se tendría que incorporar de una forma más visible en el proyecto, de modo que -con independencia que se pueda conseguir el consentimiento de las personas afectadas- un determinado tratamiento, sólo se base en información de personas identificadas en aquellos casos que resulte imprescindible.

Hay que acotar en qué casos puede ser, no ya necesario, sino imprescindible, trabajar con datos no anonimizados. Como se ha visto, el proyecto se refiere a la comercialización de informes de diversa naturaleza, en relación con algunos de los cuales sólo se menciona que responden "a necesidades específicas" del solicitante, sin más concreción, respecto de qué tipo y volumen de información agregada o no agregada pueden requerir.

V

Sobre la finalidad del tratamiento

Tal como hemos visto, el artículo 4.1 prevé que la información sólo puede tratarse "en r*elación con el ámbito y las finalidades determinadas, explícitas y legítimas para las cuales se han obtenido."*

Y además, el apartado 2 del mismo artículo 4 añade:

> *2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.*
> *(...)".*

Estas previsiones conforman lo que se nombra principio de finalidad en la normativa de protección de datos de carácter personal.

En la documentación aportada se menciona que el objetivo del Proyecto es dar valor a la información generada por el sistema sanitario catalán. Más en concreto, se hace referencia a la finalidad de "investigación médica y evaluación" (Documento de encargo de servicios, Documento de Procedimiento de cesión de datos, y DT).

Ahora bien, con respecto a las finalidades concretas para las cuales los clientes finales pueden solicitar los datos, hay alguna discordancia:

En el Anexo 1 del DT, referido al *"modelo de seguridad, disponibilidad y uso de los datos", se* expone lo siguiente : *"El Adjudicatario sólo podrá utilizar los datos, tanto si son personales como anonimizados, para alguna de las finalidades siguientes: estudios de investigación médica, estudios de epidemiología, docencia, asistencia sanitaria, administración y gestión de centros sanitarios, inspección por parte de la administración sanitaria, gestión sanitaria para la administración sanitaria o estadística oficial declarada en el Plan Estadístico.".* Y ello parece que abarcaría tanto los supuestos de datos abiertos como otros en que se solicite la información por el usuario final, según las diferentes modalidades previstas.

También en el Documento *"Procedimiento para la cesión de datos personales (...)"*, en el apartado 1.3.1 *"Supervisión de las solicitudes de los usuarios al Adjudicatario",* y en el apartado 2 relativo a la cesión de datos no anonimizados, se hace una referencia general a todas las finalidades de uso de la HC análoga al Anexo 1 del DT.

En cambio, en los encabezamientos de los apartados relativos a los procedimientos 1 y 2 se hace referencia sólo a "*investigación médica y evaluación*". Y en el Documento de encargo de servicios de anonimización, que se adjunta, y al que después nos referiremos con más detalle, se prevé que la finalidad del servicio es la *"gestión sanitaria para la administración sanitaria; Estudios de epidemiología; Investigación".*

Es decir, se constata que **las referencias a las finalidades del proyecto no siempre coinciden en los diferentes apartados de la documentación aportada**. Así, se hace una referencia, en algunos documentos, acotada a la investigación médica y evaluación, y en otros, a la práctica totalidad de las finalidades descritas en la normativa sectorial para los datos de la HC.

Aparte de esto, hay que señalar dos precisiones:

El Anexo 1 del DT se refiere a que "*el Adjudicatario sólo podrá utilizar los datos*..." con alguna de estas finalidades. En realidad sin embargo, el uso principal que haga el adjudicatario no parece que tenga que ser éste, sino ponerlos a disposición de terceros según las diferentes modalidades previstas, para que sean éstos quienes lleven a cabo estas finalidades.

Por otra parte, en caso de que el cliente final solicite los datos, se puede comprobar en este trámite la finalidad prevista, a fin de que encaje en alguna de estas finalidades. Pero en cambio, cuando se trate de datos abiertos, el análisis de la finalidad hay que hacerlo en el momento de la previa puesta a disposición y, en consecuencia, limitar la publicación de datos en abierto a aquéllos que desde el punto de vista de las finalidades mencionadas resulten imprescindibles.

En segundo lugar, según la documentación aportada, las finalidades del tratamiento de datos en el contexto del Proyecto VISC+ abarcan desde la asistencia sanitaria (artículo 11.1 Ley 21/2000), a funciones de inspección (artículo 11.5 Ley 21/2000), a tareas de administración de centros sanitarios (artículo 11.4 Ley 21/2000), y a finalidades epidemiológicas y de investigación o docencia (artículo 11.3 Ley 21/2000). Si nos atenemos a las previsiones de la normativa sectorial (Leyes 41/2002 y 21/2000), algunas de estas finalidades pueden no requerir el consentimiento de los titulares, mientras que otros (principalmente, a los efectos que nos ocupan, la finalidad de investigación o investigación médica), requieren ineludiblemente del consentimiento de los afectados a menos que se proceda a la anonimización, en unos términos que aseguren la protección de la privacidad de los afectados.

Por ello hace falta recordar que resultan confusas algunas de las previsiones de la documentación aportada, en el sentido que no queda claro si el tratamiento de datos personales del Proyecto VISC+ debe tener como objetivo, principalmente o, incluso, únicamente, la investigación o "investigación médica" (como parecería deducirse de algunos de los Documentos citados), o si se puede producir un tratamiento y cesión a los "clientes finales" para, en definitiva, la práctica totalidad de las finalidades o usos de la HC descritos en el artículo 11 de la Ley 21/2000 (y artículo 16 de la Ley 21/2000). Tampoco queda clara cuál es la finalidad de "evaluación" a que hacen referencia algunos de los Documentos aportados, como ha quedado dicho. En relación con esta finalidad de evaluación, se recomienda que se concrete la referencia, en atención a los usos de la HC previstos en la Ley 21/2000.

Habría que explicitar, en la medida de lo posible, que los "clientes finales" sólo podrán tratar la información personal (singularmente, información no anonimizada) necesaria, en atención a la finalidad para la cual lo hayan solicitado, y teniendo en cuenta las limitaciones que se puedan derivar de la normativa aplicable.

En este sentido, debemos recordar **que se echa de menos, en el conjunto de documentación aportada, una conexión clara entre "cliente final", la finalidad a cumplir, la concreción de la información a que podría tener acceso, y si esta información tiene que ser anonimizada o puede comportar una cesión de datos personales.**

Al respecto, hay que señalar que en el DT se identifican una serie de servicios o productos, que, a propuesta de La entidad, el Adjudicatario tendrá que configurar. En concreto:

- *Servicios de datos abiertos: publicación sin coste de subset (subconjuntos) de datos anonimizados.*

- *Servicios de datos no abiertos: comercialización de subset de datos para una finalidad de investigación concreta. Se destinan a usuarios que dispongan de subvenciones, fondos competitivos o que hayan pasado a un Comité ético de investigación.*
- *Servicios de licenciamiento, por explotación y análisis de los datos incluidos en el objeto del contrato.*
- *Servicios de informes estándar: comercialización de informes de análisis y evaluación, basados en los datos incluidos en el alcance del presente contrato.*
- *Servicios de informes ad hoc, adaptados a necesidades específicas del solicitante.*
- *Servicios de optimización de la gestión de servicios sanitarios o de práctica clínica.*
- *Otros servicios ad hoc.*

De entrada, se prevén servicios de datos abiertos ("*open data*"), es decir, subconjuntos de datos que se ponen libremente a disposición de todo el mundo para su reutilización tanto para finalidades comerciales como no comerciales (según definición de la Comunicación de la Comisión Europea COM(2014)442 final, *"Hacia una economía de los datos próspera").* En este contexto, y con la evolución que se está produciendo en el ámbito del big data, en función del volumen de datos que sean puestos a disposición de cualquier persona (el apartado 3.2.2 del DT se refiere tanto a ciudadanos como a industria o instituciones privadas en el ámbito de las ciencias de la vida, pero en realidad puede ser cualquier persona o empresa) y según la forma como se ofrezcan, la posibilidad de que la combinación de esta información con informaciones obtenidas de otras fuentes pueda acabar haciendo identificables personas, no se puede descartar. Por ello hay que tener especialmente en cuenta que no se produzca un riesgo para la privacidad de los afectados, como se ha puesto de manifiesto, entre otros, en la Comunicación de la Comisión sobre *"Datos abiertos. Un motor para la innovación, el crecimiento y la gobernanza transparente"* (COM(2011)882 final).

A ello hay que añadir la amplia tipología de clientes identificados en el Proyecto (apartado 3.2.2 *"Gestión de clientes",* del DT), que incluyen agentes del sistema sanitario integral de utilización pública de Cataluña (SISCAT); investigadores; industria o instituciones privadas en el ámbito de las ciencias de la vida; ciudadanía (personas físicas, asociaciones de ciudadanos, de pacientes, empresas especializadas o con interés en el uso y reuso de los datos, y "otros destinatarios".

Como ha recordado esta Autoridad en anteriores ocasiones, entre otros, en el Informe 3/2014, relativo al Proyecto de decreto de modificación del Decreto 67/2010 -que se puede consultar en el web www.apd.cat-, **la exigencia de legitimidad**, presente en relación con cualquier tratamiento de datos, tiene que ser más estricta en casos en que se prevé el tratamiento de datos sensibles, como es el caso que nos ocupa.

A modo de ejemplo, teniendo en cuenta la normativa aplicable, los usos y finalidades de la HC, y vista la tipología de clientes finales de la información a tratar, que puede ser, insistimos, según el Proyecto, información personal no anonimizada, desde la perspectiva de la protección de datos y de los usos admitidos para la HC, puede ser difícilmente asumible que una asociación de ciudadanos o determinadas empresas, tengan que poder acceder, a través del Proyecto, a información personal sensible no anonimizada, independientemente de que se vehicule a través del consentimiento. Por contra, si los clientes finales son investigadores y requieren los datos para finalidades de investigación (artículo 11.3 Ley 21/2000), en algunos casos sí podría ser necesario acceder y tratar información no anonimizada, si se dispone de los necesarios

consentimientos, si bien, en otros casos, se podrá llevar a cabo la investigación con información agregada.

Contrariamente, la normativa prevé determinadas finalidades que tienen que permitir el acceso a información contenida en la HC, sin consentimiento. A modo de ejemplo, según el artículo 11.5 de la Ley 21/2000, se prevé el acceso a las HC para funciones de inspección, limitado al personal al servicio de la Administración sanitaria.

Por todo ello, vista la casuística amplia y diversa que se puede dar en relación con los clientes potenciales, las finalidades previstas, los servicios identificados, y los ficheros que serían fuente de información en el contexto del Proyecto VISC+, y sin perjuicio que en la Documentación aportada se haga referencia a la necesidad de consentimiento de los afectados en determinados supuestos, desde la perspectiva de la protección de datos, **sería conveniente una mayor claridad y concreción en el Proyecto VISC+**, **respecto de qué servicios y tipologías de clientes pueden llegar a requerir la utilización de información personal sensible no anonimizada, y cuáles no, y para qué finalidad concreta.**

VI

Régimen de comunicación de datos personales

Con respecto al régimen de comunicación de datos personales, el artículo 11 de la LOPD dispone lo siguiente:

> *"**1.** Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.*
> ***2.** El consentimiento exigido en el apartado anterior no será preciso:*
> ***a)** Cuando la cesión está autorizada en una ley.*
> *(...)".*

El artículo 11.6 LOPD, por su parte, establece que si la comunicación se produce previo procedimiento de disociación, no es aplicable lo que se establece en los apartados anteriores.

Como se ha apuntado, el Proyecto VISC+ se enmarcaría principalmente en la finalidad de investigación, si bien la documentación aportada hace referencia, también, a otras finalidades. Dado que la información objeto de tratamiento (incluida en los diferentes ficheros descritos) es información sensible, y puede provenir en buena parte de la HC, a los efectos de la previsión del artículo 11.2.a) LOPD hay que tener en cuenta las previsiones de la normativa sectorial.

Según disponen los artículos 16.3 de la Ley 41/2002, y 11.3 de la Ley 21/2000, el acceso a la HC con finalidades de investigación, entre otros, requiere el consentimiento expreso de los titulares a menos que los datos se traten de forma anonimizada en los términos previstos en la normativa citada (Ley 41/2002 y Ley 21/2000).

El Proyecto VISC+ comporta, en parte, el acceso de los clientes finales a datos anonimizados -Apartado 1. del Documento *"Procedimiento para la cesión de datos (...)"*-. Ahora bien, también se prevé la cesión al usuario final de datos personales de salud que no han sido anonimizados para investigación médica y evaluación. En este

último supuesto habrá que disponer del consentimiento informado de los titulares de los datos, por aplicación de la normativa sectorial citada.

El artículo 5.1.d) del RLOPD define el consentimiento como *"cualquier manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de datos personales que lo conciernen."*

En relación, concretamente, con la cesión de datos personales, el artículo 12.2 del RLOPD dispone que:

> ***"2.** Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.*

Según dispone el artículo 11.3 de la LOPD:

> ***3.** Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.*

En lo que se refiere, en cambio, a la cesión de datos sin ningún dato que permita la identificación del afectado, se trataría de una cesión de datos anonimizados, que ya no requeriría del consentimiento de los afectados, vista la previsión de los artículos 11.6 LOPD, 16.3 de la Ley 41/2002 y 11.3 de la Ley 21/2000, citadas. Por aplicación de las leyes citadas de autonomía del paciente, la anonimización de los datos de la HC habilita la comunicación de la información para finalidades de investigación, de manera que, estrictamente, el consentimiento del paciente ya no sería necesario.

En este punto, recordamos que el Considerando 26 de la Directiva 95/46/CE, de protección de datos personales, dispone que los principios de la protección de datos personales se tendrán que aplicar a cualquier información relativa a una persona identificada o identificable, y añade que, para determinar si una persona es identificable hay que considerar el conjunto de los medios que pueda utilizar razonablemente el responsable del tratamiento o cualquier otra persona, para identificar a esta persona; que los principios de la protección de datos no se aplicarán a aquellos datos hechos anónimos de manera que ya no sea posible identificar al interesado.

Según el artículo 2.a) de la Directiva citada, son "datos personales" toda información sobre una persona física identificada o identificable; y se considera identificable a toda persona la identidad de la cual se pueda determinar, directamente o indirectamente, en particular mediante un número de identificación o uno o diversos elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Ya avanzamos que el procedimiento de disociación de la información de salud que se pueda contener en los ficheros afectados por el Proyecto VISC+, entendido como *"cualquier tratamiento de datos personales de manera que la información que se obtenga no se pueda asociar a una persona identificada o identificable"* (art. 3.f) LOPD) tendrá que ser adecuado, con el fin de asegurar que se ceden *"datos disociados"* (art. 5.1.e) RLOPD), es decir, datos que no permiten la identificación del afectado.

Por eso no parece que pueda ser admisible una previsión como la contenida en el apartado 3.2.3 del DT. En la página 15 de este documento se afirma lo siguiente:

"En c*aso de que la petición del cliente se corresponda con el acceso a un volumen de datos anonimizados que implique un riesgo de desanonimización /personalización de estos datos, será necesario que la entidad, a través del comité de dirección, evalúe y autorice esta solicitud con el fin de dar cumplimiento a la LOPD*."

En caso de que exista el riesgo que se menciona en este párrafo no parece que el comité de dirección pueda autorizar la petición. **Si existe un riesgo de reidentificación, se tendrá que denegar la solicitud o introducir las garantías suficientes para hacer desaparecer este riesgo**. Observación ésta que se puede trasladar también al apartado 1.3.2 del Documento relativo al procedimiento, donde se recoge esta previsión (pág .7)

Estas mismas consideraciones son extensibles a la posibilidad prevista en el apartado "Disponibilidad de los datos" del Anexo 1, en qué se requeriría autorización de la entidad así como justificación para el adjudicatario que la petición se corresponde con una necesidad concreta.

Sin perjuicio de las consideraciones que se puedan hacer más adelante, en relación con los procedimientos de disociación o anonimización que se tengan que llevar a cabo en el contexto del Proyecto VISC+, resultan de especial interés el Dictamen del Grupo de Trabajo del Artículo 29 (GTA29), 6/2013, sobre datos abiertos y reutilización de la información del sector público (ISP), de 5 de junio de 2013, así como el Dictamen 5/2014, del GTA29, sobre técnicas de anonimización, de 10 de abril de 2014.

Hechas estas consideraciones generales, a continuación se hará referencia específica a diversas previsiones de la Documentación aportada, relativa al Proyecto VISC+.

VII

Responsabilidad y propiedad de la información

En relación con el alcance del contrato (apartado 5 del DA), se prevé que el Adjudicatario ostentará sobre la información tratada, un derecho de uso, tratamiento, agregación y explotación vinculado a la comercialización de los productos y servicios VISC+, y que el Adjudicatario *"no ostenta la propiedad ni ningún derecho ilimitado sobre los datos, siendo responsable delante de ésta, las autoridades competentes y terceros, del cumplimiento de la normativa aplicable al tratamiento de datos de carácter personal."*

A efectos de claridad, y con el fin de dejar constancia que las posibles responsabilidades del adjudicatario en relación con el tratamiento de datos personales no desvirtúan las que correspondan a La entidad o a los diferentes responsables (artículo 3.d) LOPD) de los ficheros de datos (artículo 3. b) LOPD) que son fuente de origen de la información tratada, sería conveniente añadir una referencia a que la responsabilidad del Adjudicatario es sin perjuicio de la que pueda corresponder a la entidad o a los responsables de dichos ficheros.

En cualquier caso, vistas las menciones hechas a la propiedad sobre los datos (en este apartado 5 del DA, entre otros), conviene recordar que la titularidad de un dato

personal (que no la propiedad), corresponde siempre a la persona física (artículo 3.e) LOPD).

Por otra parte, la cláusula 39 del DA se refiere, al acceso a "*datos de la entidad*". Sería más claro referirse a los *"datos que la entidad cede al Adjudicatario",* pues los datos personales que, anonimizados o no, puedan ser objeto de cesión a los efectos del cumplimiento del contrato, no son, desde la perspectiva de la LOPD, de la entidad, sino que su titularidad pertenece siempre a la persona física afectada. Hacemos extensiva esta consideración al resto de menciones, de la cláusula 39, a datos de la entidad y del Departamento de Salud, en el sentido que sería más ajustado a la LOPD referirse a los datos de los ficheros responsabilidad de l'entitat o del Departamento de Salud o, si procede, de ficheros de otros responsables.

Similares consideraciones pueden hacerse con respecto a las referencias contenidas en la cláusula 21.1 del DA a la titularidad de las bases de datos, los conjuntos o subconjuntos de datos o a la 21.2 con respecto a la titularidad de los datos relativos a los contactos y a los clientes del Adjudicatario.

Por otra parte, dicha cláusula 21 también prevé que, con respecto a los datos de los contactos y clientes del Adjudicatario, éste garantiza que dispone de las correspondientes autorizaciones para llevar a cabo la cesión, que se realizará de conformidad con la normativa de protección de datos personales. Aunque se valora positivamente la mención que ésta se produciría de acuerdo con la LOPD, no parece claro de qué cesión se trataría.

VIII

Deber de confidencialidad

Según la documentación aportada, el objeto del contrato de colaboración publico privada para desarrollar el Proyecto VISC+ tiene que consistir en poner en valor los datos generados por el sistema público catalán, "mediante el tratamiento, el análisis y la explotación de estos datos, previamente anonimizados, garantizando en todo momento el cumplimiento de la normativa en materia de protección y tratamiento de datos (...)" (apartado 4 del DA). Se añade que "*la puesta a disposición del Adjudicatario de esta información y datos se producirá de forma anonimizada, en los términos y condiciones descritos en el DT de solución final*" (apartado 5. DA).

En este sentido, la cláusula 39 del DA hace referencia al "Deber de confidencialidad y protección de datos", y obliga al Adjudicatario a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato incluyendo una remisión a la LOPD. Sin perjuicio que esta remisión a la LOPD resulte adecuada, convendría hacer referencia en concreto al artículo 10 de la LOPD, que prevé el deber de secreto en el tratamiento de datos personales.

Dicho esto, la cláusula 39 continúa exponiendo que *"la puesta a disposición del Adjudicatario de los datos se producirá de forma anonimizada, por lo cual los datos tendrán la condición de disociados al no permitir la identificación de los afectados o interesados. En este sentido, la prestación de los servicios no supone en ningún caso el acceso a datos personales de la entidad y del Departamento de Salud, por parte del personal puesto a disposición por parte del Adjudicatario, comprometiéndose éste a no acceder en ningún momento en virtud de la ejecución del contrato a datos de carácter personal titularidad de la entidad ni del Departamento de Salud, ni tratar ningún tipo de dato de carácter personal a la hora de ejercer sus funciones."*

Sin perjuicio de las consideraciones que se harán a continuación respecto del proceso de anonimización y del flujo informativo entre La entidad y el Adjudicatario, conviene señalar que difícilmente el Adjudicatario podrá ejercer sus funciones sin *"tratar ningún tipo de dato de carácter personal*". Por ello, habría que ceñir esta afirmación a los datos facilitados por la entidad. Pero es que además, en otros apartados (p. ej. en el apartado "servicios a prestar" del Anexo 1) no parece que se pueda descartar que en algunos casos el Adjudicatario tenga acceso a datos personales, dado que por ejemplo en este Anexo 1 se prevé que en la ejecución del proceso de anonimización el Adjudicatario participe en la verificación del anonimización o que la entidad pueda requerir el apoyo del Adjudicatario.

Por otra parte, en esta misma cláusula, en el subapartado intitulado "Respecto de la información confidencial" se hace referencia a que tendrá el carácter de confidencial la información revelada por la entidad "por escrito o cualquier otro soporte que garantice su recepción". Recordar que, de acuerdo con el artículo 10 de la LOPD el carácter de confidencial se tiene que predicar de cualquier dato de carácter personal, con independencia de la forma o el soporte en que se haya enviado.

IX

Niveles de aprobación y gestión de la demanda

El DT, en el apartado 3.2.3 *"Gestión de la demanda",* prevé **tres niveles** de aprobación de las peticiones de los clientes finales, atendiendo, entre otros, al cliente que solicita el servicio, los objetivos para las cuales se solicita, si la petición requiere incorporar nuevas fuentes de información, o en atención a la cuantía económica del servicio, entre otros.

El Nivel 1 de aprobación se refiere a clientes calificados como de bajo riesgo (los tres responsables de los ficheros implicados en el Proyecto, citados, agentes del SISCAT, la propia entidad, investigadores y centros de investigación, e industria o instituciones privadas en el ámbito de las ciencias de la vida y la salud). La solicitud, en estos casos, queda pre-aprobada, sin perjuicio que se pueda denegar y pasar a un nivel 2 o 3 de gestión. Uno de los elementos a tener en cuenta en este nivel, para acceder a la solicitud del cliente, es que la petición de información esté alineada y sea proporcional al objetivo perseguido.

Esta proporcionalidad predicada en el texto respecto del objetivo perseguido, habría que ponerla en relación no sólo con el objetivo que se persiga, sino también con los eventuales riesgos o perjuicios que se puedan causar en los derechos de las personas afectadas, y en concreto en el derecho a la protección de datos de carácter personal.

Con respecto a la consideración de clientes de bajo riesgo, el amplio número y categorías de éstos no permite inferir que todos ellos deban tener acceso a toda la información solicitada. Cómo se ha recordado anteriormente, ello sólo se puede decidir valorando la información solicitada (cuantitativa y cualitativamente), la habilitación legal para hacerlo, si procede, y la finalidad pretendida.

En la misma línea, con respecto al Nivel 2 de aprobación, también habría que explicitar que al evaluar la solicitud se tendrá en cuenta las exigencias de la normativa de protección de datos. En este nivel se evalúan las solicitudes de los mismos clientes que en el Nivel 1, pero se trata de peticiones *"que para ser entregadas se requiere incorporar nuevas fuentes de datos (no disponibles en el momento de hacer la*

petición) o realizar un tratamiento específico de los datos ya disponibles." A los efectos que nos ocupan, una petición de nuevos datos obligará a examinar su pertenencia atendiendo a los principios de calidad y de finalidad. Aparte de ello, no resulta claro cuál puede ser este tratamiento específico, ni las implicaciones que ello puede tener para la protección de datos. Convendría, pues, aclarar estos extremos.

Con respecto al Nivel 3 de aprobación, se reserva para las solicitudes relacionadas con la realización de un ensayo clínico, con proyectos de investigación que comportan algún riesgo físico o psicológico para un ser humano, o para los que tienen **consentimiento informado asociado a la petición.**

Según el DT, en estos casos, y en los que se prevean según la normativa, el Adjudicatario tendrá que comprobar que el solicitante acompaña la petición con los consentimientos necesarios y la aprobación correspondiente para realizar el estudio por parte de un CEIC, que haya tenido en cuenta que se obtendrán datos o información provenientes de VISC+.

Con respecto a la descripción de este Nivel 3, el hecho de que se mencione la concurrencia de consentimiento informado asociado a la petición, permitiría deducir que se está refiriendo a aquellos casos en qué la cesión de datos se producirá sin anonimización previa de la información. A *sensu contrario*, también se podría inferir de ello que los Niveles 1 y 2, en los que no hay ninguna mención al consentimiento informado, se reservan para las cesiones de datos anonimizados.

Ahora bien, desde la perspectiva de la protección de datos, **hay que recordar que se debería especificar, en términos lo bastante claros, la vinculación entre cada nivel y la posibilidad de ceder datos anonimizados o datos personales.** Ya se ha puesto de manifiesto que en el contexto del Proyecto VISC+ la comunicación de datos anonimizados en origen presenta un menor riesgo potencial para la protección de datos, y se tendría que priorizar ante cesiones de datos de salud no anonimizadas, que debería ser excepcional.

Esta excepcionalidad, justificada en los principios de calidad -en la vertiente de proporcionalidad y minimización-, y de finalidad, debería quedar explicitada en la información que se refiere a los 3 Niveles de autorización referidos. Es decir, habría que explicitar que todos aquellos casos en que se prevea que el cliente final tiene que acceder y tratar datos sin anonimizar, tendrán que ser validados según los principios y obligaciones de la normativa de protección de datos, y quedarán sometidos al Nivel 3 de aprobación.

Nuevamente hay que reiterar que, sin descartar que en algunos casos determinados clientes finales pueden requerir una cesión de datos de salud junto con datos de identificación del paciente, esta posibilidad no tendría que ser la norma general, sino sólo fruto de una evaluación que tenga especialmente en cuenta los riesgos potenciales desde la perspectiva de la protección de datos.

X

Procedimiento técnico de anonimización

El Anexo 1 del DT y el anexo 3 del documento relativo al procedimiento, describen el proceso de anonimización que se tiene que llevar a cabo. En concreto, se prevé en primer lugar eliminar la información identificativa de personas físicas (datos identificativos y "información genética"), y también eliminar o reducir al mínimo

imprescindible el detalle de la información u otras variables que puedan dar lugar a identificaciones indirectas.

Parecería en un principio que la actuación del adjudicatario no tiene que comportar el acceso a datos de carácter personal, dado que la información que se le enviaría, sería información anonimizada previamente. Así se desprende de la página 1 del documento relativo al procedimiento de cesión, y también de la cláusula 39 del DA. No obstante, hay diferentes previsiones en el Anexo 1 del DT que parecen apuntar lo contrario. Así encontramos diferentes referencias que podrían comportar el tratamiento de datos personales por parte del adjudicatario:

- En el apartado "Proceso de anonimización: se afirma que el adjudicatario participa en el proceso de verificación de la anonimización.
- En el apartado "Servicios a prestar" se afirma que la entidad podrá requerir la colaboración del adjudicatario en el proceso de anonimización.
- En el apartado "Ubicación de los datos" se afirma que puede haber datos que permitan la identificación indirecta.

Igualmente en el apartado 2.2.2.1 del DT se manifiesta que se entregará al adjudicatario una muestra representativa de estas fuentes de datos, a fin de que el adjudicatario diseñe el catálogo de servicios, el proceso de comercialización y el proceso de anonimización.

Siendo así, en la relación jurídica que se establezca entre la entidad y el Adjudicatario, se debería recoger de forma expresa las cláusulas previstas al artículo 12.2 LOPD, al configurarse el adjudicatario como un encargado del tratamiento. En cambio, en el apartado 1.3 del documento relativo al procedimiento no se encuentra ninguna referencia a esta cuestión.

Respecto de las variables a eliminar, en atención a la finalidad, se podría valorar eliminar también la información sobre el centro sanitario, en línea con la previsión de anonimizar, si procede, el dato sobre los profesionales sanitarios que atienden a un paciente.

El Anexo 3 citado prevé que se establezca un *"código anónimo de la persona".* Se prevé que la entidad facilitará los datos estructurados ya anonimizados al Adjudicatario utilizando, para una misma persona, un mismo código anónimo de persona con el fin de permitir relacionar los diferentes conjuntos de datos. A ello se añade que *"El Adjudicatario tendrá que utilizar un sistema de anonimización diferente para cada entidad jurídica usuario final. El Adjudicatario tendrá que aplicar un segundo proceso sobre el código de caso anónimo que facilite la entidad para que cada entidad jurídica usuario diferente tenga un código de caso anónimo calculado de forma diferente."*

El Anexo 3 del Documento *de "Procedimiento para la cesión de datos (...)",* en línea con el Anexo 1 del DT, añade información relativa al algoritmo de cálculo que aplicaría La entidad para calcular el código anónimo de persona, a la que nos remitimos. En línea con lo que se ha apuntado, se prevé la eliminación de identificaciones directas (eliminar los datos identificativos de personas físicas -pacientes, profesionales sanitarios, etc-) y también las identificaciones indirectas, como, a modo de ejemplo, sustituir la fecha de nacimiento por el año, o la altura y el peso por rangos de la altura y peso. Por último, se prevé en este documento informar sobre riesgos de identificaciones directas o indirectas, y sobre riesgos derivados de la excesiva información sobre un mismo afectado, sobre códigos anónimos mal calculados, o sobre la revelación de la clave de cifrado. En este punto hacemos extensiva la

consideración anterior sobre la eliminación, si procede, de información sobre el centro sanitario, si no es relevante para la finalidad pretendida.

Se valora positivamente que en el Documento *"Procedimiento para la cesión de datos (...)"* En el apartado 1.3.3 *"Supervisión de la formalización del contrato",* se prevé que la entidad podrá supervisar en todo momento los contratos que se formalicen con los usuarios finales, y que comprobará "*que en los contratos se indique que se aplicará una transformación del código anónimo de persona para obtener un código de caso específico y diferenciado para cada usuario final*".

Desde la perspectiva de la protección de datos, y de las exigencias referidas al proceso de anonimización de datos que se tiene que llevar a cabo en el contexto del Proyecto VISC+, las previsiones del Anexo 3, citado, se deben valorar positivamente, ya que tienen que suponer no sólo anonimizar la información personal sobre un individuo, sino que se explicita que cada cliente final recibirá la información en unos términos que no tendrían que permitir, en principio, la vinculación con la información que habrá recibido otro cliente final, debido a que el código de caso anónimo no coincidirá en uno y otro caso.

De todos modos, con el fin de reducir los riesgos de reidentificación de información anonimizada (cuestión que concretaremos a continuación), se recomienda prever que, cuando se trate de peticiones que, a pesar de ser formuladas por un mismo cliente final, no estén vinculadas a un mismo proyecto, convendría atribuir un código de caso diferente.

No obstante, en virtud del principio de minimización al cual ya hemos hecho referencia, no parece que la atribución de un código tenga que ser necesario en todos los casos. Por ello habría que plantearse que, en aquellos casos en que la finalidad no lo requiera, se anonimice sin atribuir ningún tipo de código.

También es relevante y debe ser valorado positivamente, que se tengan en cuenta medidas concretas de análisis de riesgos. Sobre estas cuestiones, nos remitimos nuevamente al Dictamen del GTA29 5/2014, sobre técnicas de anonimización.

Por otra parte, en la cláusula 5 del DA se prevé que el Adjudicatario *"no podrá hacer ninguna acción para reidentificar datos que la entidad haya facilitado de forma anonimizada y tendrá que comunicar a la entidad cualquier dato que se le haya facilitado en principio anonimizado pero que se detecte que puede ser posible asociarlo a una persona concreta."*

Se valora positivamente esta mención, en el sentido que, desde la perspectiva de la protección de datos, incluso en el caso de anonimización previa de la información personal (en el caso que nos ocupa, en buena parte datos sensibles), hace falta tener en cuenta las posibilidades que esta información pueda permitir la identificación de su titular. Así lo ha puesto de manifiesto el GTA 29 en su Dictamen 5/2014, sobre técnicas de anonimización, cuando expone lo siguiente:

"(...) los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizado puede entrañar todavía riesgos residuales para los interesados. Efectivamente, por una parte, la anonimización y la reidentificación son campos de investigación activos en los que se publican con regularidad nuevos descubrimientos y, por otra, incluso los datos anonimizados, como las estadísticas, pueden usarse para enriquecer los perfiles existentes de personas, con la consiguiente creación de nuevos problemas de protección de datos. En suma, la anonimización no debe contemplarse

como un procedimiento esporádico, y los responsables del tratamiento de datos han de evaluar regularmente los riesgos existentes."

Así, según el GTA29, el riesgo de reidentificación es inherente a cualquier técnica de anonimización, por lo cual la intimidad y el derecho a la protección de datos del titular, podrían verse comprometidos.

En este sentido, resulta positivo que en el contexto del Proyecto VISC+ se prevea que la detección, por parte del Adjudicatario, de la posibilidad de reidentificaciones del titular de los datos, tenga que ser puesto en conocimiento de la entidad. Volveremos sobre esta cuestión en el apartado de este informe relativo a las medidas de seguridad.

En cualquier caso, se recomienda que se tengan en cuenta, en el contexto del Proyecto VISC+, las consideraciones del Dictamen 5/2014 del GTA29, citado, respecto de la necesidad de hacer un análisis de riesgos en función de las técnicas de anonimización utilizadas y las posibilidades de reidentificación inherentes a estas técnicas.

Con respecto a la re-identificación, hacer notar también que en el apartado "Re-identificación de los datos" del Anexo 1 del DT se hace referencia como supuesto en que se podrá desanonimizar, los casos en que se haga "*con trazabilidad de los accesos*". No parece que esta sola circunstancia tenga que habilitar la reidentificación. En cualquier caso tampoco queda claro en este apartado quién podría llevar a cabo esta desanonimización.

También se hace referencia a la reidentificación en el pacto noveno del Acuerdo de encargo del tratamiento, al que nos referiremos más adelante, recogido en el Documento *"Encargo de servicios de anonimización de datos (...)",* aportado con la consulta, y que se tiene que firmar entre el Departamento de Salud, CATSALUT y el ICS como responsables de los ficheros, y la entidad, como prestador de servicios (encargado del tratamiento). En este pacto noveno se prevé que *"en caso de que el Prestador de Servicios sea conocedor de posibles peligros para la salud presente o futura de los afectados como resultado del análisis de una combinación de datos, concreta, éste se compromete a informar a los Responsables de ficheros para que tomen las medidas pertinentes y reidentifiquen al afectado, en caso de que fuera necesario. En ningún caso se autoriza el Prestador de Servicios a hacer la reidentificación de los casos en situación de riesgo."* Esta previsión se valora positivamente, ya que hace recaer en el responsable del fichero la decisión de una posible reidentificación. De esta manera, claro está que es este responsable quien tendrá que llevar a cabo la reidentificación en los casos en que pueda ser justificado.

Finalmente, hay que señalar que en el apartado 3.2.3 *"Gestión de la demanda",* del DT, en que se hace referencia a los 3 Niveles de autorización de solicitudes de datos, también se tiene en cuenta aquellos casos en que la petición del cliente se refiera a un volumen de datos anonimizados que implique un riesgo de desanonimización/personalización de los datos, respecto de los cuales se prevé que la entidad tendrá que evaluar y autorizar esta solicitud con el fin de dar cumplimiento a la LOPD. Se considera positiva esta previsión general de detección de casos en que, por el volumen de la información solicitada, se pueda detectar un riesgo de reidentificación, que exigirá un análisis más cuidadoso desde la perspectiva de la protección de datos.

Dicho esto, en la línea de la observación formulada en el Fundamento jurídico VI, se recomienda que se incorpore una referencia a las medidas compensatorias que en

estos casos puedan minimizar tanto el riesgo potencial de reidentificación, como los efectos negativos en las personas afectadas, a fin de que se pueda autorizar.

XI

Procedimiento establecido para la cesión de datos

En este apartado se analizan las particularidades del procedimiento de cesión de datos previsto en el contexto del Proyecto VISC+, incluidas en el Documento *"Procedimiento para la cesión de datos personales anonimizados de salud al Adjudicatario de VISC+ para investigación médica y evaluación".*

De entrada, hay que señalar que el título del Documento es confuso, ya que las cesiones de datos previstas no se limitan a datos anonimizados, como se podría deducir del título citado, sino que el propio Documento que analizamos establece el procedimiento para ceder, también, datos personales que no han sufrido un proceso de anonimización. Convendría, a efectos de claridad, referirse en el título a la cesión de datos anonimizados y de datos personales. Con respecto a las menciones de este documento a la finalidad de *"evaluación",* nos remitimos a lo que ya se ha apuntado sobre la falta de concreción del tipo de evaluación a que se está refiriendo.

Este documento define dos procesos diferentes sobre la cesión de información en el contexto del Proyecto VISC+:

1) Procedimiento para la cesión de datos personales anonimizados de salud al Adjudicatario de VISC+ para investigación médica y evaluación.

De entrada, como se ha recordado en este informe, desde la perspectiva de la protección de datos, éste es el procedimiento de cesión que convendría priorizar en el contexto del Proyecto VISC+, teniendo en cuenta que la anonimización ofrece un tratamiento menos invasivo y de menor riesgo para los afectados.

Partiendo de esta premisa, se hacen las siguientes consideraciones.

Se prevé la creación inicial de los conjuntos de datos anonimizados que se pondrán a disposición del Adjudicatario, por lo cual éste tiene que elaborar un informe en el cual se detalle, entre otros, la propuesta de procedimientos y herramientas para anonimizar y generar un conjunto de datos no estructurados (imágenes médicas, PDFs, etc.), y la valoración del riesgo de identificaciones indirectas, que será imprescindible cuando se trate de obtener datos para un destinatario y finalidad concreta.

Se valora positivamente la previsión de que se podrá incorporar una propuesta de marcaje de datos o de "sembrado de la información" (introducción de datos ocultos o enmascarados entre los reales que, sin afectar a la calidad de la información, permiten la detección de usos no autorizados), técnica que permitiría identificar posibles fugas -o accesos indebidos- que se pudieran producir, y también que este marcaje deberá ser diferenciado para cada usuario final que solicite los datos. Más allá de la posibilidad de aplicar estas técnicas de marcaje en un procedimiento concreto de cesión de datos anonimizados, se sugiere que se incluya esta cuestión en el contrato y a la vez que se valore introducirla no ya como una posibilidad en manos del Adjudicatario sino como una obligación de éste.

También se hace remisión a los criterios de anonimización aprobados por la entidad (Anexo 3), y se explicita que *"cualquier excepción a la no aplicación de alguno de los*

criterios de anonimización tendrá que acompañarse de una justificación de los motivos de excepcionalidad."

Teniendo en cuenta que la cesión de datos no anonimizados ya está prevista en el Procedimiento 2, no está claro qué motivo podría justificar la no aplicación de la anonimización prevista en el Anexo 3, ni como -o por parte de quien- se tendría que evaluar esta excepción. Caso que no exista consentimiento expreso de las personas afectadas o una ley que habilite la comunicación, la información tendrá que ser inevitablemente anonimizada, sin que puedan existir motivos de excepcionalidad.

En la valoración que la entidad tiene que hacer de las solicitudes del Adjudicatario (con el fin de obtener datos anonimizados), se explicita que se deberá hacer una valoración del cumplimiento de la LOPD, y se prevé que, en esta evaluación, se invitará a asistir al responsable de los datos que han sido objeto de solicitud, *"especialmente en caso que se considere que existe algún riesgo significativo que ponga en peligro el cumplimiento de la LOPD".*

Esta previsión, que se entiende referida al responsable del fichero o ficheros afectados, se considera pertinente, pues el responsable podrá participar, en estos casos, de la evaluación en cuestión. Ahora bien, de la redacción de este apartado *(" ... se podrá invitar a asistir..."*) no queda claro si invitar al responsable es una opción, o bien un compromiso. En cualquier caso, la opción más garantista aconsejaría la implicación en todos estos casos del responsable.

2) Procedimiento para la cesión de datos personales de salud para investigación médica y evaluación al usuario final.

Nos referimos, en este caso, al proceso que recoge todas las actividades necesarias para la creación inicial de los **conjuntos de datos personales** por solicitud del Adjudicatario con motivo de un encargo de un usuario final.

En principio, en este procedimiento, aunque el Adjudicatario intervendría en la presentación de la solicitud del usuario final ante la entidad (apartados 2.1 y 2.2 del documento relativo al procedimiento), por lo que se describe en este apartado parecería que el Adjudicatario no tiene que intervenir en la entrega de los datos. Así se desprende también del apartado 2.2.2 del DT.

No obstante, del apartado "Usos del los datos" del Anexo 1 del DT parece desprenderse lo contrario, dado que se manifiesta que el Adjudicatario tendrá que preservar el modelo de seguridad, disponibilidad y uso de datos que esté vigente en cada momento y no podrá utilizarlos para ninguna otra finalidad que las enumeradas anteriormente ni facilitarlos a terceros, sin consentimiento expreso por parte de la entidad. También parece desprenderse esto de las menciones al adjudicatario contenidas en los apartados 2.3.1, 2.3.3.1 y 2.3.3.2 del documento relativo al procedimiento.

También parece desprenderse de la referencia a la elaboración de un informe del apartado 2.3.2 del documento relativo al procedimiento, porque, aunque en este caso no se menciona directamente el adjudicatario, parece que se está refiriendo a él.

Las referencias hechas en estos apartados al adjudicatario, sólo tendrían sentido si el adjudicatario interviniera en el tratamiento de datos no anonimizados (qué son los datos a que se refieren estos apartados). Por eso habría que corregir esta falta de congruencia.

Este procedimiento implica no ya un flujo informativo de información anonimizada, sino de datos personales de salud. Por ello, hace falta insistir en qué, aparte de la necesidad del consentimiento de las personas afectadas, cualquier cesión se tendrá que fundamentar en una finalidad legítima, habrá que comprobar que el usuario final está habilitado para tratar datos para esta finalidad, y valorar que los datos no son excesivos para dicha finalidad, cuestión que se prevé en el documento (punto 2.1.1). Asimismo, también en el apartado 2.1.1, que comentamos, se hace mención que el informe del Adjudicatario debe tener en cuenta, entre otros, *"el grado de detalle de los valores de las variables, cuando son tan detalladas que podrían dar lugar a identificaciones indirectas".* Teniendo en cuenta que en este segundo procedimiento se tratarán datos personales, hay que señalar que la posibilidad de identificación de los afectados será más que probable, y no sólo de manera "indirecta". Teniendo en cuenta esto, como ha sido abastamente expuesto en este informe, hay que extremar las precauciones, en atención a la normativa de protección de datos, a la hora de dar viabilidad a cualquier petición de usuarios finales en el marco de este procedimiento.

En relación con el consentimiento de los afectados, en el apartado 2.1.1 *"Solicitud del adjudicatario",* se prevé que el informe del Adjudicatario debe tener, entre otros, el siguiente contenido:

"Los consentimientos informados de las personas incluidas en el conjunto de datos solicitado. Estos consentimientos tendrán que cumplir con los requerimientos de la LOPD y cubrir explícitamente la cesión de datos solicitados."

El Anexo 1 del DT hace referencia a que si se facilitan datos de personas identificables, porque el cliente final necesita enriquecer datos personales que ya tiene con datos del Departamento de Salud (o, se supone, de los otros responsables de los ficheros implicados en el proyecto), hará falta que aquél facilite una auditoría que demuestre que cumplirá con las obligaciones de la LOPD, en referencia, entre otros, al *"consentimiento válido de todos los afectados".*

De entrada, aparte de prever los requerimientos de la LOPD, se debería incluir una referencia explícita a los requerimientos que se puedan prever en la normativa aplicable en cada supuesto. Como se ha dicho, en materia de investigación médica, las leyes de autonomía del paciente, u otras leyes aplicables a los ensayos clínicos, a la investigación biomédica, etc, prevén particularidades respecto del consentimiento informado de los afectados, que se deberá tener en cuenta en cada caso.

En conexión con ello, en el apartado 2.1.3 *"Generación y entrega del conjunto de datos* personales", se dispone que la entidad ejecutará el proceso para obtener efectivamente estos datos, y que *"cuando se hayan obtenido estos datos se realizará una prueba de la aplicación y una verificación de la selección de pacientes con consentimiento."* A continuación, la entidad elaborará el informe de verificación y prueba sobre la correcta selección de los casos, y sobre *"la comprobación que los casos de los conjuntos de datos se corresponden con los casos en que el usuario final aporta consentimientos de los afectados."*

Hay que recordar que no es lo bastante claro el mecanismo descrito para la obtención del consentimiento de los afectados. Parece claro que es el usuario final el que aporta los consentimientos (se tiene que entender, las hojas de consentimiento informado debidamente rellenadas en base a lo que pueda prever la normativa aplicable en cada caso), pero estos consentimientos se refieren a personas incluidas en los conjuntos de datos solicitados, en definitiva, en ficheros de datos a los cuales el usuario final no

tiene acceso, ni es el responsable de los mismos, ni el encargado del tratamiento (artículo 12 LOPD).

Hay que tener presente que, en el marco de las previsiones relativas al consentimiento de los titulares de los datos (artículos 6 y 11 LOPD), el artículo 12 del RLOPD concreta lo siguiente:

> ***1.*** *El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.*
> *La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.*
> ***2.*** *Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.*
> ***3.*** *Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.*

En principio, es pues al responsable (artículo 3.d) LOPD), en el caso que nos ocupa, el Departamento de Salud, el CATSALUT y el ICS, responsables de los ficheros implicados en el Proyecto, VISC+, a quien corresponde solicitar el consentimiento para poder ceder datos personales.

En estos términos, no está claro como uno tercero ajeno a los responsables, y a priori indeterminado (pues los usuarios finales pueden ser entidades de muy diversa naturaleza), podrá identificar, contactar y obtener el consentimiento de los afectados, cuyos datos se tratan en estos ficheros. Sin prejuzgar que en algunos casos este esquema pueda ser realizable (p. ej. cuándo las mismas personas ya hayan dado su consentimiento para participar en otras fases de un estudio) y pueda facilitar llevar a cabo este tipo de estudios, debería quedar abierta la posibilidad de que pueda ser el mismo responsable del fichero, o si procede la entidad, quién obtenga dicho consentimiento. En cualquier caso conviene recordar que la responsabilidad sobre el adecuado tratamiento de los datos seguirá correspondiendo al responsable del fichero.

Aún en relación con el consentimiento, el punto 2.2 del procedimiento que describimos (cesión de datos personales) prevé que a la hora de actualizar la información ("actualizaciones temporales acordadas"), la entidad revisará *"si hay altas o bajas en los consentimientos informados que se facilitaron inicialmente."*

Si, como parece, los consentimientos informados los tiene que obtener el usuario final, parece lógico inferir que será éste el que, habiendo informado adecuadamente a los afectados sobre la posibilidad de revocación de dicho consentimiento (artículos 6.3 11.4 LOPD), dispondrá de la información relativa a posibles revocaciones, o posibles nuevos consentimientos. Siguiendo este esquema, se prevé que la entidad tendrá que contrastar esta nueva información (nuevos consentimientos o revocación de los anteriores) antes de dar nueva información. Esta medida supone una garantía, pues condiciona la cesión de datos a las oportunas comprobaciones.

A ello añadimos que el punto 2.2, que comentamos, prevé que la actualización de la información tendrá que tener en cuenta posibles modificaciones a consecuencia del ejercicio de Derechos ARCO (Título III LOPD y Títol III RLOPD), por parte de los

pacientes de centros sanitarios, que son los que habrán modificado información a consecuencia del ejercicio de estos derechos. Si bien esta previsión supone una garantía respecto de la actualización de la información que llegaría a los usuarios finales, sería recomendable sustituir la expresión "*centro sanitario*" por "*responsable del fichero*".

También cabe señalar que en el apartado 2.1.3, aparte de las cuestiones relativas al consentimiento que hemos apuntado, se prevé que *"finalmente se realizará una validación de seguridad",* pero no se concretan los aspectos a verificar.

Finalmente, hacemos un apunte formal, dado que en la página 7 del Documento para la cesión de datos, se hace una referencia al Anexo 3 (condiciones de seguridad, uso y disponibilidad de datos), en lugar de referirse al Anexo 1.

XII

Medidas de seguridad

Si bien con carácter general el Proyecto VISC+ supone el tratamiento de información que a priori habrá sido anonimizada por la entidad, de manera tal que la actividad principal del Adjudicatario no implica, con carácter ordinario, el tratamiento de datos de carácter personal, también se prevé el tratamiento y cesión de datos personales. En consecuencia, sin perjuicio de las consideraciones ya hechas, conviene plantear un **modelo integral de seguridad de la información para el conjunto del contrato VISC+, aplicable tanto al tratamiento de datos anonimizados como al de datos personales.**

El Proyecto VISC+ implica el tratamiento de datos de carácter personal que requieren la aplicación del **nivel alto de medidas de seguridad** (artículo 9 LOPD y título VIII del RLOPD).

El Pacto Cuarto del Acuerdo de encargo del tratamiento, incluido en el documento *"Encargo de servicios de anonimización de datos y de cesión de datos anonimizados y personal para finalidades de evaluación y investigación médicas",* aportado con la consulta, explicita que, de acuerdo con el artículo 9 del LOPD, la entidad se compromete a adoptar las medidas de seguridad del nivel que se indica en el encabezamiento. Dado que el encabezamiento del documento no se refiere expresamente al nivel de seguridad (la referencia al nivel de seguridad aplicable no se encuentra hasta la página 7 del "encargo de servicios..."), sería recomendable hacer una referencia directa al nivel alto en el Pacto Cuarto.

En cualquier caso, queda claro que el nivel alto de medidas de seguridad resulta de necesaria aplicación, cómo se ha apuntado, teniendo en cuenta la información que se trata en los ficheros del Departamento de Salud, de CATSALUT y del ICS, que son la fuente de donde se extraerán los datos para el tratamiento objeto del Proyecto VISC+.

Ahora bien, las especiales características de los tratamientos y las actividades que derivan del contrato VISC+ aconsejan plantearse un **modelo de seguridad que vaya más allá de** las previsiones de seguridad que prevé el título VIII del RLOPD.

El conjunto de la documentación aportada evidencia una clara voluntad de ofrecer las máximas garantías de seguridad para los datos, estableciendo medidas técnicas y organizativas que den como resultado un "modelo de seguridad, disponibilidad y uso de los datos" orientado a la protección del conjunto del sistema VISC+.

Con carácter general convendría que, como punto de partida, la seguridad de la información exigible al Adjudicatario estuviera alineada con alguno de los **conjuntos de buenas prácticas** existentes (Tipo ISO27001). Si bien no sería necesario que el contrato determine un conjunto concreto de buenas prácticas, si haría falta determinar que las que finalmente implante el Adjudicatario tendrán que basarse en la gestión de riesgos, ser susceptibles de ser certificados por uno tercero independiente y poder ser revisables mediante procedimientos estándares de auditoría de seguridad o de sistemas de información. A partir de esta base, se podría verificar cómo se implantan los requisitos en relación con la protección de datos de carácter personal.

Dicho esto, a continuación se hacen las siguientes consideraciones.

En los criterios de valoración del contrato, previstos en el apartado 8.2 del DA, aparentemente no se incluyen los aspectos de gestión de la seguridad que pueda aportar el Adjudicatario. Este extremo tendría que ser relevante a la hora de valorar las propuestas. Respecto de la valoración de la "*gestión y operación de los servicios de análisis, tratamiento y explotación de datos*" (hasta 17 puntos), donde a priori se incluirían las cuestiones de gestión de la seguridad, sólo se hace referencia a que se valorará cómo se da respuesta a los requerimientos especificados en el apartado 3.2 del DT, sin hacer mención del apartado 3.1 del mismo documento, que detalla la "seguridad y anonimización de los datos".

Según el apartado 2.2.2 del DT, se prevé poner a disposición del Adjudicatario una muestra de datos, con el fin de diseñar las infraestructuras y procedimientos relacionados con el contrato. En consecuencia, se deberá tener en cuenta, también en esta fase, las medidas de seguridad previstas en los artículos 87 del RLOPD (ficheros temporales o copias de trabajo de documentos) y 94.4 RLOPD (pruebas anteriores a la implantación o modificación de los sistemas de información). Esta consideración se hace extensible al apartado 2.1.3 del Documento *"Procedimiento para la cesión de datos",* en el que se prevé la generación y entrega del conjunto de datos personales.

En cualquier caso, sería oportuno que en el apartado 4.1 del DT ("Fase de preparación y construcción"), se explicitara que el tratamiento de datos en esta fase inicial queda sujeto a la normativa de protección de datos, específicamente, en relación con las medidas de seguridad aplicables.

En relación con las previsiones sobre la realización de auditorías (artículo 96 RLOPD), el apartado 5.3 del DT *"Auditorías y gobernanza de la seguridad",* prevé que la entidad "*podrá realizar auditorías* (...)". Sobre esta previsión, convendría hacer una definición más abierta del papel de la entidad, en el sentido que pueda "realizar" o bien "encargar a terceros" la auditoría del modelo de seguridad.

En el apartado 1.4.1 "Auditorías" del Documento *"Procedimiento para la cesión..."* , se prevé, entre otros, una auditoría anual, cuyo alcance sería del 50%. Ello podría generar ciertos riesgos, pues puede resultar complejo determinar qué 50% daría suficiente evidencia de que las medidas de seguridad dan el resultado esperado y se adecuan a las previsiones del contrato y la normativa aplicable.

Con el fin de simplificar el modelo de auditoría, esta Autoridad propone un modelo más sencillo de implementar y potencialmente más eficaz, esto es, **un modelo de auditoría continuada,** en base a la verificación de la aplicación de los procedimientos y resultados de los procesos de seguridad, realizada internamente por el Adjudicatario, y con emisión de informes periódicos (quizás trimestrales, o incluso semestrales) para ser analizados por la entidad, y una auditoría formal cada 2 años, realizada por una

entidad externa e independiente, que finalice con un informe de auditoría con los contenidos mínimos exigidos por la normativa de protección de datos (artículo 96.2 RLOPD).

También hacemos mención que en el Anexo 3 del Documento de *"Procedimiento para la cesión de datos personales (...)",* comentado, se prevé que *"El envío de los datos que realice la entidad, tanto al Adjudicatario en caso de datos anonimizados como al usuario final en caso de datos personales, lo realizará mediante un sistema de transmisión de ficheros (FTP) cifrado*." De hecho, se hace mención de esta cuestión (sistema de transmisión cifrado) en diversos puntos de este Documento. Estas previsiones se ajustarían al artículo 104 del RLOPD, según el cual, cuando se requiere la implantación de medidas de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes sin hilo de comunicaciones electrónicas se tiene que hacer cifrando los datos, o bien utilizando otros mecanismos que garanticen que la información no es inteligible ni manipulada por terceros. Ahora bien, por la trascendencia y los riesgos inherentes a esta operación, pues presumiblemente el intercambio de información se hará mediante redes públicas de telecomunicaciones, sería muy recomendable concretar más algunos aspectos técnicos, como la red de comunicaciones que se utilizará; los requisitos del software utilizado para la transmisión de los datos; las restricciones a nivel de red con respecto al filtrado de direcciones IP (origen y destinación); los requisitos mínimos de los algoritmos de cifrado a utilizar, etc. También se recomienda prever el cifrado del canal de transporte, así como cifrar en origen los datos objeto de transmisión.

También hay que hacer mención de la previsión relativa a la tecnología utilizada por el "centro de competencia", citado, que centraliza la tarea llevada a cabo por el Adjudicatario en el Proyecto VISC+ con el objetivo que los servicios de análisis y explotación de datos que tiene que ofrecer el Adjudicatario se presten desde un mismo espacio (apartado 3.4 del DT). Así, se prevé que el Adjudicatario tendrá que dotar al centro de competencia de los componentes y herramientas tecnológicas adecuadas para prestar los productos y servicios VISC+ (apartado 3.4.3 del DT). Se prevé que la tecnología utilizada tiene que ser, entre otros, interoperable, para integrarse con otros sistemas corporativos y relacionarse con sistemas externos en torno a la Generalitat, y segura a nivel de datos y a nivel lógico, para garantizar el acceso seguro a la información y al sistema, para custodiar los datos y evitar fugas o accesos no deseados a los servicios y a la información, de acuerdo con el modelo de seguridad, disponibilidad y uso de los datos (Anexo 1 del DT). Por lo tanto, hay que entender que el centro de competencia queda vinculado por las medidas previstas en dicho Anexo 1. Con respecto al centro de competencia, desde la perspectiva de las medidas de seguridad aplicables, a nivel organizativo se sugiere identificar e incorporar las funciones básicas del delegado de protección de datos, especialmente por parte del Adjudicatario, con el fin de empezar a alinear las previsiones del contrato VISC+ con lo que prevé el Proyecto de Reglamento Europeo de Protección de Datos, actualmente en tramitación.

Con respecto a la gestión de las incidencias, se hace referencia en los apartados 1.4.3 y 2.3.3 del Documento del Procedimiento para la cesión de datos, analizado. En síntesis, se prevé que el Adjudicatario y la entidad pueden detectar casos mal anonimizados o cualquier incidencia que afecte a la seguridad de los datos, y que en estos casos, se hará un análisis y una propuesta de plan de acción (que debe tener un contenido mínimo que se detalla), el cual tendrá que ser aprobado por la entidad. En conexión con ello, como se ha mencionado, en la cláusula 5 del DA se prevé que el Adjudicatario no puede hacer ninguna acción para reidentificar datos, y que deberá comunicar a la entidad cualquier dato que se le haya facilitado, en principio

anonimizado, pero que se detecte que puede ser posible asociarlo a una persona concreta.

Desde la perspectiva de las medidas de seguridad previstas en el RLOPD, se debería considerar esta casuística como un incidente de seguridad. En caso de producirse un acceso no autorizado a datos de carácter personal, este supuesto tendría que ser registrado formalmente como un incidente de seguridad. Por la relevancia de la cuestión, se debería establecer en el contrato la obligación del Adjudicatario de mantener un registro de incidencias en los términos del RLOPD (artículos 90 y 100 del RLOPD).

Finalmente, dado que se prevé la comunicación a la entidad, por la importancia de este tipo de incidente sería recomendable concretar en el contrato algunos aspectos de esta comunicación: plazo para comunicarlo; quien comunica a quien; canal de comunicación preferente; y contenido mínimo de la comunicación, que en todo caso tendría que incluir, aparte de los hechos ocurridos, el número de afectados y su ubicación en el tiempo, las medidas tomadas y las potenciales consecuencias de este incidente. Como sugerencia, y para alinear el Proyecto VISC+ con algunas obligaciones que se podrían derivar de la aprobación de Reglamento Europeo de Protección de Datos, citado, sería conveniente, con la intención de generar confianza en dicho proyecto, que la comunicación también se hiciera efectiva a la Autoridad Catalana de Protección de Datos.

Estos comentarios se hacen extensivos a los puntos 1.4.3 y 2.3.3 del Documento de "Procedimiento para la cesión de datos".

XIII

Ubicación de la información

También desde el punto de vista de la seguridad, hay que hacer algunas consideraciones sobre la ubicación de la información.

El Anexo 1 del DT, citado, también hace referencia a la *"ubicación de los datos".* Desde un punto de vista formal, convendría mencionar en este apartado el RLOPD, que es la norma en que se concretan las medidas de seguridad aplicables, y no sólo la LOPD.

Dicho esto, en este apartado se hace referencia a la necesidad de garantizar, entre otros, "*la trazabilidad de todos los accesos*". Al respecto, hay que señalar que el RLOPD exige, para los ficheros que requieren medidas de nivel alto, articular un registro de accesos, de manera que de cada intento de acceso se tienen que guardar, como mínimo, la identificación del usuario, la fecha y la hora en que se realizó, el fichero a que se ha accedido, el tipo de acceso y si ha sido autorizado o denegado (artículo 103 RLOPD). Se valoran, pues, en términos positivos, las diversas menciones que se hacen en la documentación aportada a la trazabilidad de los accesos.

En este apartado también se hace referencia a la necesidad de autorización previa de esta Autoridad para una transferencia internacional de datos, excepto dentro del Espacio Económico Europeo, entidades *Safe Harbour* de Estados Unidos y otros países homologados.

Dado que el propio DT, en el apartado 2.2.1 *"Alcance del modelo de gestión y operación",* explicita que el Adjudicatario tiene que canalizar la demanda del mercado

nacional e internacional, no se descarta que alguno de los clientes potenciales de la información objeto de tratamiento en el contexto del Proyecto VISC+ pueda comportar una transferencia internacional de datos. Si es así, ésta se encuentra sometida al régimen establecido en los artículos 33 y 34 de la LOPD.

En caso de no poder garantizar, por lo tanto, la adhesión a los principios del acuerdo Safe Harbor, en un caso determinado, o de no darse ninguna otra de las excepciones previstas en la LOPD hará falta, aparte de cumplir con el resto de principios y obligaciones de la LOPD, contar con la autorización del Director de la Agencia Española de Protección de Datos (artículo 37.1.l) LOPD). Por lo tanto, la referencia que se hace a la APDCAT en esta apartado se tendría que hacer a la Agencia Española de Protección de Datos.

Finalmente, según este mismo punto del Anexo 1 del DT, se impide utilizar tecnologías *"cloud computing"* sin restricción de país o que se puedan utilizar CPDs que previamente no hayan superado con éxito una auditoría del cumplimiento de la LOPD, la cual, conviene puntualizar, tendrá que haberse realizado dentro del plazo de 2 años anteriores al uso del centro de proceso de datos (CPD). Es decir, éste tendrá que estar al día con respecto a la realización de auditorías de seguridad, en los términos del RLOPD (artículo 96).

En cualquier caso, con estas referencias a la computación en nube, se deduce que el Proyecto tiene en cuenta que un tratamiento de datos derivado de una transferencia internacional, en estos términos, podría no asegurar el correcto cumplimiento del régimen citado (artículos 33 y 34 LOPD), de manera que hay que valorar positivamente esta previsión.

XIV

Encargo del tratamiento y posibilidad de subcontratación de las prestaciones del contrato

La documentación aportada incluye el documento *"Encargo de servicios de anonimización de datos y de cesión de datos anonimizados y personales para finalidades de evaluación y investigación médicas",* ya mencionado.

Este documento se refiere al Acuerdo que tienen que suscribir, por una parte, los responsables de los ficheros relacionados con el Proyecto VISC+ (Departamento de Salud, CATSALUT y ICS), y por la otra, la entidad, como prestador de servicios, y que tiene que constituir un encargo del tratamiento regulado en el artículo 12 del LOPD, tal como se explicita en el punto 4 de dicho Acuerdo.

Con respecto a la *"descripción de los servicios encargados",* incluida en el Acuerdo de encargo del tratamiento, conviene hacer las siguientes consideraciones:

a) Nuevamente se hacen referencias a la anonimización "*de la información de los responsables de los ficheros*...". Como se ha apuntado, convendría referirse a la información contenida en los ficheros de datos personales.

b) Se prevé que la entidad deberá comprobar que el cesionario dispone del consentimiento válido de cada una de las personas afectadas para ceder la información, y que dispone de una auditoría que demuestra el cumplimiento de las medidas de seguridad de la LOPD. Sin perjuicio de otras consideraciones hechas en este informe respecto de estas cuestiones (consentimiento informado y auditoría), y de

las responsabilidades que, en atención a la normativa de protección de datos, correspondan a los responsables de los ficheros, la previsión que será la entidad la que comprobará estos extremos (consentimientos y auditoría) se ajusta a la previsión hecha en el Anexo 1 del DT, según la cual es la entidad la que efectivamente tiene que revisar que el "cliente final" (receptor de la información personal) dispone de dichos consentimientos y auditoría.

El Acuerdo de encargo del tratamiento examinado contiene un apartado en que se relacionan los *"ficheros administrativos de carácter personal a los cuales pertenecen los datos que se someterán a tratamiento dentro de los servicios encargados".* Desde un punto de vista formal, y atendiendo a la terminología de la LOPD, habría que referirse a "ficheros de datos de carácter personal", y no a "ficheros administrativos de carácter personal".

En concreto, se relacionan ficheros titularidad del Departamento de Salud, del Servicio Catalán de la Salud y del Instituto Catalán de la Salud. En los tres casos también se excluyen del encargo determinados ficheros, y se prevé, también en relación con los ficheros de los tres responsables, la siguiente fórmula:

"Y en el futuro cualquier otro fichero del (responsable) con datos de salud o centros asistenciales de interés por la investigación y evaluación médicas".

Desde la perspectiva de la protección de datos, en concreto, de los principios de calidad y de finalidad (artículo 4 LOPD), hay que cuestionar que se utilice esta fórmula, pues abre la puerta a que ficheros que todavía no han sido creados y de los cuales, por lo tanto, se desconoce la finalidad y la información tratada, puedan quedar automáticamente afectados por el encargo del tratamiento y, por lo tanto, ser incluidos en el objeto del contrato que nos ocupa, referido al Proyecto VISC+. Esta inclusión automática de futuros ficheros es desaconsejable, ya que parece obviar la previa valoración del responsable (sea el Departamento de Salud, el CATSALUT o el ICS), de la conveniencia de incluir un determinado fichero en el Proyecto VISC+. Por lo tanto, el Acuerdo de encargo del tratamiento se tendría que circunscribir a los ficheros existentes determinados en el momento de su firma, o de otros que se pueda establecer de acuerdo con un previo proceso que permita evaluar su adecuación.

En cualquier caso, conviene recordar y sería bueno recoger de forma expresa que, al finalizar el encargo, resultará de aplicación lo que prevé el artículo 12.3 de la LOPD, es decir, habrá que proceder al retorno de los datos al responsable o bien, si procede, a su destrucción.

Todavía en relación con el encargo del tratamiento, nos referimos a la cláusula 27 del DA, según la cual en los términos previstos en los artículos 227 y 228 del Real decreto legislativo 3/2011, de 14 de noviembre, que aprueba el texto refundido de la Ley de contratos del sector público (TRLCSP), las prestaciones del contrato que nos ocupa podrán ser objeto de subcontratación, y se especifican una serie de requisitos (página 35 del DA).

Dado que entre estos requisitos no se hace mención de cuestiones relativas a la protección de datos, conviene recordar que en caso de que la subcontratación mencionada en la cláusula 27, citada, pueda afectar a datos personales, hay que tener en cuenta que, según el apartado 3 de la disposición adicional 26ª del TRLCSP:

> *"3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:*

a) Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.
b) Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.
c) Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
En estos casos, el tercero tendrá también la consideración de encargado del tratamiento."

Por lo tanto, en la cláusula 27, citada, del DA, convendría hacer constar que en caso de que la empresa que resulte adjudicataria subcontrate alguna prestación del contrato, se deberá cumplir con las obligaciones de la LOPD en relación con el encargo del tratamiento, en los términos de la disposición adicional 26ª, apartado 3, del TRLCSP.

De acuerdo con las consideraciones hechas en estos fundamentos jurídicos en relación con la consulta planteada, se hacen las siguientes,

Conclusiones

Vista la casuística amplia y diversa que se puede dar en relación con los clientes potenciales, las finalidades previstas, los servicios ofrecidos y los ficheros que serían fuente de información en el contexto del Proyecto VISC+, sería conveniente una mayor claridad y concreción respecto de qué finalidades pueden justificar el acceso a la información, por parte de qué clientes y en qué condiciones. A estos efectos sería de utilidad disponer de una memoria general que describa el proyecto de manera global, que recoja de forma armonizada las previsiones de los diferentes documentos aportados y clarifique los diferentes aspectos puestos de manifiesto a lo largo de este informe, como también una evaluación de impacto sobre la privacidad.

Desde la perspectiva de los principios de calidad y de finalidad, y por el volumen de información sensible generada a través de VISC+, se recomienda priorizar los supuestos de cesión de datos previamente anonimizados, asociados a un código no identificable o, si es posible, no asociados a ningún código, por delante de los supuestos de cesión de datos personales de personas identificables que hayan prestado su consentimiento.

El conjunto de la documentación aportada evidencia una clara voluntad de ofrecer las máximas garantías de seguridad para los datos, estableciendo medidas técnicas y organizativas que dan como resultado un *"modelo de seguridad, disponibilidad y uso de los datos*" orientado a la protección del conjunto del sistema VISC+.

De acuerdo con el RLOPD hay que aplicar un nivel alto de medidas de seguridad. No obstante, se recomienda la adopción de un modelo integral de seguridad de la información para el conjunto del contrato VISC+, aplicable tanto al tratamiento de datos anonimizados como de datos personales, que vaya más allá de las previsiones de seguridad que prevé el título VIII del RLOPD y que esté alineado con alguno de los conjuntos de buenas prácticas existentes.

Con respecto a las medidas de seguridad previstas en el RLOPD, convendría especificar diversas cuestiones relativas a las auditorías de seguridad, los registros de

incidencias, o los requisitos de seguridad relacionados con la transmisión de datos, entre otros, en los términos expuestos en el Fundamento Jurídico XII de este informe.

Con respecto al encargo del tratamiento entre los responsables de los ficheros implicados en el Proyecto y la entidad, conviene tener en cuenta las previsiones del artículo 12 LOPD, en los términos apuntados en el Fundamento Jurídico XIV de este informe.

Barcelona, 23 de julio de 2014