**ANEXO 5**

Al pliego de cláusulas administrativas particulares aplicable a la contratación del servicio de vigilancia de la salud y de diferentes prestaciones vinculadas con la salud de las personas empleadas públicas adscritas a la Diputación de Barcelona y a otras entidades integradas en su sector público adheridas a este contrato.

**Expediente n.º: 2023/38632**

**PROTECCIÓN DE DATOS PERSONALES**

1. **Objeto del encargo del tratamiento**

Mediante estas cláusulas se habilita al contratista, Encargado del Tratamiento, para tratar por cuenta de cada una de las entidades contratantes relacionadas en la Cláusula 1.1 de este PCAP, Responsables de Tratamiento, los datos personales necesarios para prestar el servicio de vigilancia de la salud y de diferentes prestaciones vinculadas con la salud de los trabajadores de cada una de ellas respectivamente.

Cuando el tratamiento de los datos personales tenga por finalidad la prestación del servicio de vigilancia de la salud individual y servicio médico de empresa, en el marco de ejecución de este concreto servicio de prevención, el contratista tendrá la consideración de Responsable del Tratamiento en relación con todos los datos personales necesarios que el trabajador le proporcione en desarrollo de su actividad. Las entidades contratantes serán informadas de las conclusiones que se deriven de los reconocimientos médicos efectuados a sus trabajadores, pero solo y únicamente de la aptitud del trabajador para el desempeño de su puesto de trabajo, en conformidad con lo establecido, en el artículo 22 de la Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales.

El contratista garantiza que el acceso a la información médica y sanitaria en el marco de la prestación de este servicio de vigilancia de la salud individual y servicio médico de empresa se limitará al personal médico y a las propias autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores en los términos exigidos por el RGPD.

**El tratamiento consistirá en:**

Concreción de los tratamientos a realizar:

 Cotejo  Interconexión

X Conservación  Limitación

X Consulta X Modificación

X Comunicación X Organización

X Comunicación por transmisión X Recogida

 Destrucción X Registro

 Difusión X Supresión

X Extracción X Utilización

**2. Identificación de la información afectada**

Para ejecutar las prestaciones derivadas del cumplimiento del objeto de este encargo, cada una de las entidades contratantes relacionadas en la Cláusula 1.1 de este PCAP, Responsables del Tratamiento, ponen a disposición y permiten la recogida por la contratista, entidad encargada del tratamiento, la información que se describe a continuación:

* Datos identificativos y laborales de los trabajadores usuarios de los servicios necesarios para la prestación de los servicio contratados (nombre y apellidos, categoría, puesto de trabajo, funciones, ...).
* Datos relativos a los resultados de los estudios de evaluaciones de riesgos, en el marco de los servicios de vigilancia de la salud colectiva prevista en el apartado II.1.1.1.a) del Pliego de Prescripciones Técnicas, con el siguiente contenido mínimo:
  + 1. Descripción detallada del puesto de trabajo.
    2. Riesgos detectados.
    3. Medidas preventivas adoptadas.

La información sobre el estado de salud de las personas trabajadoras, como por ejemplo pruebas diagnósticas, cirugías, enfermedades, discapacidades, medicamentos, antecedentes familiares etc., que constituye la llamada “Historia Clínica-laboral”, comprende el conjunto de documentos relativos a los procesos asistenciales de cada persona y tiene como finalidad principal facilitar la asistencia sanitaria, dejando constancia de todos los datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud. Esta información sobre el estado de salud de las personas trabajadoras podrá ser recogida por el adjudicatario por la prestación del servicio de vigilancia de la salud individual y servicio médico de empresa, en calidad de Responsable del Tratamiento, de acuerdo con las resoluciones de las Autoridades de Control.

**3. Duración**

Este anexo tiene la duración prevista en su punto 1.5 del presente pliego cláusulas administrativas particulares, sin perjuicio del que se prevé en el apartado r) de la cláusula 4 siguiente.

**4. Obligaciones de la entidad encargada del tratamiento**

La entidad encargada del tratamiento y todo su personal se obliga a:

1. Utilizar los datos personales objeto de tratamiento, o las que recoja para su inclusión, solo para la finalidad objeto de este encargo. En ningún caso puede utilizar los datos para finalidades propias o diferentes de la referida al objeto de este encargo.
2. Tratar los datos de acuerdo con las instrucciones de los responsables del tratamiento.

Si la entidad encargada del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los estados miembros, la entidad encargada tiene que informar inmediatamente a los responsables.

1. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de los responsables, que contenga:
2. El nombre y los datos de contacto de la entidad encargada (o encargadas) y de cada responsable por cuenta del cual actúa la entidad encargada y, si procede, del representante del responsable o de la entidad encargada y del delegado de protección de datos.
3. Las categorías de datos personales de tratamientos efectuados por cuenta de cada responsable.
4. Si procede, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de este país o esta organización internacional, y en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.
5. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

* La pseudonimización y el cifrado de datos personales.
* La capacidad de garantizar la confidencialidad, la integridad, la disponibilidad y la resiliencia permanentes de los sistemas y servicios de tratamiento.
* La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
* El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas que garantizan la eficacia del tratamiento.

1. No comunicar los datos a terceras personas, salvo que tenga la autorización expresa de los responsables del tratamiento, en los supuestos legalmente admisibles.

La entidad encargada puede comunicar los datos a otras entidades encargadas del tratamiento del mismo responsable, de acuerdo con las instrucciones de éste. En este caso, los responsables tienen que identificar, previamente y por escrito, la entidad a la cual se tienen que comunicar los datos, los datos a comunicar y las medidas de seguridad que hay que aplicar para proceder a la comunicación.

Si la entidad encargada tiene que transferir datos personales a un tercer país o a una organización internacional, en virtud del derecho de la Unión o de los estados miembros que le sea aplicable, tiene que informar a los responsables de esta exigencia legal de manera previa, salvo que este derecho lo prohíba por razones importantes de interés público.

1. **Subcontratación**

Se autoriza la entidad encargada a subcontratar, con las limitaciones establecidas en su punto. 2.11 del presente pliego de cláusulas administrativas particulares.

Para subcontratar con otras empresas, la entidad encargada tiene que comunicar este hecho por escrito a los responsables e identificar de forma clara e inequívoca los tratamientos que se pretende subcontratar, la entidad subencargada y sus datos de contacto. La subcontratación se puede llevar a cabo si los responsables no manifiestan oposición en el plazo establecido.

La subcontratista/subentidad encargada, que también tiene la condición de entidad encargada del tratamiento, está obligada igualmente a cumplir las obligaciones que este documento establece para la entidad encargada del tratamiento y las instrucciones que dicten los responsables. Corresponde a la entidad encargada inicial regular la nueva relación, de forma que la nueva entidad encargada quede sujeta a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que ella, en cuanto al tratamiento adecuado de los datos personales y a la garantía de los derechos de las personas afectadas. Si la subencargada lo incumple, la entidad encargada inicial continúa siendo plenamente responsable ante los responsables en cuanto al cumplimiento de las obligaciones.

1. Mantener el deber de secreto respecto de los datos personales a los cuales haya tenido acceso en virtud de este encargo, incluso después de que finalice el objeto.
2. Garantizar que las personas autorizadas para tratar datos personales se comprometen, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las cuales hay que informarles convenientemente.
3. Mantener a disposición de los responsables la documentación que acredita que se cumple la obligación que establece el apartado anterior.
4. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
5. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos siguientes:
6. Acceso, rectificación, supresión y oposición
7. Limitación del tratamiento
8. Portabilidad de datos

La entidad encargada del tratamiento tiene que resolver, por cuenta de los responsables y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento y portabilidad de datos, en relación con los datos objeto del encargo.

La entidad encargada del tratamiento tendrá que comunicarlo a los responsables del contrato que se han indicado en su punto 2.18 del presente pliego de cláusulas administrativas particulares, según corresponda, las solicitudes recibidas y las resoluciones efectuadas para su conocimiento.

1. Derecho de información y consentimiento

La entidad encargada del tratamiento tiene que facilitar, en el momento de recoger los datos, la información relativa a los tratamientos de datos que se llevarán a cabo y, cuando se proceda, recoger el consentimiento. La redacción y el formato en que se facilitará la información y se prestará el consentimiento se tiene que consensuar con los responsables, antes de iniciar la recogida de los datos.

1. **Notificación de violaciones de la seguridad de los datos.**
2. **La entidad encargada del tratamiento tiene que informar y comunicar al responsable del tratamiento** que corresponda, sin más dilación indebida y en cualquier caso antes del plazo máximo de 24 horas, de las violaciones de la seguridad de los datos personales a su cargo que constituyan un riesgo para los derechos y libertades de las personas físicas (en los términos previstos en el bloque normativo de protección de datos personales de aplicación en cada momento) de las cuales tenga conocimiento, junto con toda la información relevante para documentar y comunicar la incidencia.

Si se dispone, hay que facilitar, como mínimo, la información siguiente:

1. Descripción de la naturaleza de la violación de la seguridad de los datos personales, incluidas, cuando sea posible, las categorías de datos y el número aproximado de interesados afectados y las categorías y el número aproximado de registros de datos personales afectados.
2. Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el cual se pueda obtener más información.
3. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
4. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluidas, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se tiene que facilitar de manera gradual sin más dilación indebida.

1. **Si la violación de seguridad se produce en el tratamiento de los datos personales de la prestación del servicio de vigilancia de la salud individual y servicio médico de empresa**, en el que la empresa contratista tiene la consideración de Responsable del Tratamiento, **corresponde a ésta comunicar las violaciones de la seguridad de los datos personales a la Autoridad de Control que corresponda** por los canales previstos por la propia Autoridad y en los términos previstos en el bloque normativo de protección de datos personales de aplicación en cada momento. Así mismo, tendrá que informar al Delegado de Protección de Datos de la entidad contratante relacionada en la Cláusula 1.1 de este PCAP que se vea afectada en el momento de conocer la mencionada violación. En este ámbito, corresponde también a la contratista comunicar en el menor tiempo posible a los interesados las violaciones de la seguridad de los datos personales, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas. De lo contrario, tendrá que informar y librar copia de la comunicación a los interesados al Delegado de Protección de Datos de la entidad contratante relacionada en la Cláusula 1.1 de este PCAP que se vea afectada.
2. Apoyar a los responsables del tratamiento a la hora de hacer las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
3. Apoyar a los responsables del tratamiento a la hora de hacer las consultas previas a la autoridad de control, cuando proceda.
4. Poner a disposición de los responsables toda la información necesaria para demostrar que cumple sus obligaciones, así como para realizar las auditorías o las inspecciones que efectúen la responsable u otro auditor autorizado por ella.
5. **Seguridad de la información.**

La seguridad de la información tiene que haberse pensado desde el diseño del servicio de información y por lo tanto se trata de un requerimiento funcional que el contratista se encuentra obligado a considerar, especialmente si se hace uso de portales de acceso web o soluciones cloud.

En todo caso, la contratista está obligada:

* al cumplimiento normativo del “Reglamento europeo 2016/679, de 27 de abril de 2016 relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)” y la normativa sectorial que sea de aplicación.
* a implementar las medidas de seguridad necesarias para dar cumplimiento a lo que establecen la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos Personales y garantía de los derechos digitales, sobre Medidas de seguridad al ámbito del sector público, y el Real Decreto 311/2022, de 3 mayo, por el que se regula el Esquema Nacional de Seguridad (ENTE).

Del mismo modo la empresa contratista velará por el desempeño de las obligaciones de confidencialidad y deber de secreto de su personal en cuanto a los datos personales a los sistemas de información y a cualquier otra información o recurso corporativo que puedan tener acceso en el decurso del presente contrato.

Si procede, todos los dispositivos que intervengan en la ejecución de este contrato tendrán que estar configurados para la eliminación de archivos de datos temporales, permitiendo eliminar los residuos del material confidencial que se originan a la hora de digitalizar, imprimir, copiar y enviar correo-e diariamente.

A petición de cualquier entidad contratante relacionada en la Cláusula 1.1 de este PCAP, de forma puntual o periódica, la empresa contratista (entidad encargada) tendrá que efectuar una autoevaluación de cumplimiento del ENTE, que tendrá que estar firmada por el responsable de seguridad de la entidad encargada o, caso de no tener, por el DPD.

Así mismo, tendrá que adoptar todas aquellas medidas y mecanismos para:

1. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
2. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
3. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
4. Pseudonimizar y cifrar los datos personales, si procede.

La adhesión a códigos de conducta o la posesión de una certificación son elementos que sirven para demostrar el cumplimiento de los requisitos indicados anteriormente. Hay que facilitar la información sobre estas certificaciones.

1. Tener designado un delegado de protección de datos y comunicar la identidad y los datos de contacto a los responsables del tratamiento.
2. Destino de los datos

Librar a la entidad encargada que los responsables del tratamiento designen por escrito, los datos personales necesarios por la prestación del servicio y, si procede, los apoyos donde consten, una vez cumplida la prestación.

La entidad encargada una vez cumplida la prestación contractual, garantizará la portabilidad de los datos relativos a la vigilancia de la salud de los trabajadores de cada una de las entidades contratantes relacionadas en la Cláusula 1.1 de este PCAP a la nueva empresa que desarrolle el servicio de vigilancia de la salud.

Cuando se produzca el cambio en la empresa que presta el servicio, de acuerdo con el artículo 23.1 d) de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, cada una de las entidades contratantes relacionadas en la Cláusula 1.1 de este PCAP se encuentra obligada a, “elaborar y conservar a disposición de la autoridad laboral” la documentación relativa a la “Práctica de los controles del estado de la salud de los trabajadores prevista en el artículo 22 de esta Ley y las conclusiones obtenidas de los mismos en los términos recogidos en el último párrafo del apartado 4 del mencionado artículo. No obstante, dado que se prohíbe la transmisión de la información médica obtenida al amparo de la Ley 31/1995 de prevención de riesgos laborales, a cualquier tercero diferente al “personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores”, con la única excepción de las conclusiones derivadas de dicho seguimiento en cuanto a la aptitud de los trabajadores (art. 22.4 párrafo tercero), los datos que se encuentren incluidos en la denominada historia clínica-laboral solo podrán ser entregados al personal sanitario o centro médico encargado de los servicios de prevención y directamente entre los servicios médicos de las empresas de prevención: una vez finalizada la relación contractual la entidad encargada entregará copia al nuevo servicio de prevención que se hará cargo de la vigilancia de la salud de aquellos datos que sean de interés para el seguimiento desde el punto de vista de la prevención de riesgos laborales con el objetivo de facilitar el seguimiento de la salud de los trabajadores, asegurando su continuidad. El servicio de prevención de destino será indicado por la entidad correspondiente de las entidades contratantes relacionadas en la Cláusula 1.1 de este PCAP. Durante este proceso hay que mantener en todo momento los sistemas de custodia que garantizan la confidencialidad de los datos.

La entidad encargada, tendrá que conservar la documentación clínica en las condiciones que garanticen su correcto mantenimiento y seguridad de acuerdo con el artículo 17 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y el artículo 12 de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente la salud y la autonomía del paciente, y la documentación clínica.

En cuanto a los datos de las revisiones de la Salud complementarías (ginecológicas y urológicas para hombres mayores de 45 años), el contratista, tendrá que conservar la documentación clínica en las condiciones que garanticen su correcto mantenimiento y seguridad de acuerdo con el artículo 17 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y el artículo 12 de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente la salud y la autonomía del paciente, y la documentación clínica.

El resto de documentación y apoyos que contengan datos personales tendrán que ser eliminadas al finalizar la prestación contractual de los equipos informáticos utilizados por la entidad encargada.

Una vez destruidas, la entidad encargada tiene que certificar la destrucción por escrito y tiene que de entregar el certificado al responsable del tratamiento.

Sin embargo, la entidad encargada puede conservar una copia, con los datos debidamente bloqueados, mientras se puedan derivar responsabilidades de la ejecución de la prestación. En este caso, hará falta que notifique al responsable que conservará una copia de los datos con este objetivo, indicando la motivación legal, el plazo de tiempo que está obligado a retenerlas bloqueadas y comprometiéndose en su destrucción una vez vencido este plazo de retención. La responsable le podrá pedir la aportación de un análisis de riesgos sobre su sistema de retención.

**5. Obligaciones de los responsables del tratamiento**

Corresponde a los responsables del tratamiento (entidades contratantes):

1. Entregar a la entidad encargada y permitir la recogida de los datos a las que se refiere la cláusula 2 de este documento.
2. En los casos que corresponda, hacer una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento que tiene que efectuar la entidad encargada.
3. Hacer las consultas previas que correspondan, tan solo en el supuesto que sea necesario.
4. Velar, antes y durante todo el tratamiento, para que la entidad encargada cumpla el RGPD, la LOPDGDD y el resto de normativa de protección de datos vigente.
5. Supervisar el tratamiento, incluida la ejecución de inspecciones y auditorías.
6. Autorizar a la entidad encargada del tratamiento a:
7. llevar a cabo el tratamiento de los datos personales en dispositivos portátiles de tratamiento de datos únicamente por los usuarios o perfiles de usuarios asignados a la prestación de servicios contratados.
8. llevar a cabo el tratamiento fuera de los locales de los responsables del tratamiento únicamente por los usuarios o perfiles de usuarios asignados a la prestación de servicios contratados.
9. la entrada y salida de los apoyos y documentos que contengan datos personales, incluidos los comprendidos y/o anexas en un correo electrónico, fuera de los locales bajo el control de los responsables del tratamiento.
10. la ejecución de los procedimientos de recuperación de datos que la entidad encargada del tratamiento se vea en la obligación de ejecutar.
11. tratar los datos en sus locales, ajenos a los de los responsables del tratamiento.

**6. Incumplimientos y responsabilidades**

El incumplimiento de lo que se establece en los apartados anteriores puede dar lugar a que la entidad o empresa encargada sea considerada responsable del tratamiento, a los efectos de aplicar el régimen sancionador y de responsabilidades previsto en la normativa.