**ANNEX 5**

Al plec de clàusules administratives particulars aplicable a la contractació del servei de vigilància de la salut i de diferents prestacions vinculades amb la salut de les persones empleades públiques adscrites a la Diputació de Barcelona i a altres entitats integrades en el seu sector públic adherides a aquest contracte.

**Expedient núm.: 2023/38632**

**PROTECCIÓ DE DADES PERSONALS**

1. **Objecte de l’encàrrec del tractament**

Mitjançant aquestes clàusules s’habilita el contractista, Encarregat del Tractament, per tractar per compte de cadascuna de les entitats contractants relacionades a la Clàusula 1.1 d’aquest PCAP, Responsables de Tractament, les dades personals necessàries per prestar el servei de vigilància de la salut i de diferents prestacions vinculades amb la salut dels treballadors de cadascuna d’elles respectivament.

Quan el tractament de les dades personals tingui per finalitat la prestació del servei de vigilància de la salut individual i servei mèdic d’empresa, en el marc d'execució d'aquest concret servei de prevenció, el contractista tindrà la consideració de Responsable del Tractament en relació amb totes les dades personals necessàries que el treballador li proporcioni en desenvolupament de la seva activitat. Les entitats contractants seran informades de les conclusions que es derivin dels reconeixements mèdics efectuats als seus treballadors, però sol i únicament de l'aptitud del treballador per a l'acompliment del seu lloc de treball, de conformitat amb el que s'estableix, en l'article 22 de la Llei 31/1995, de 8 de novembre de Prevenció de Riscos Laborals.

El contractista garanteix que l'accés a la informació mèdica i sanitària en el marc de la prestació d'aquest servei vigilància de la salut individual i servei mèdic d’empresa es limitarà al personal mèdic i a les pròpies autoritats sanitàries que duguin a terme la vigilància de la salut dels treballadors en els termes exigits pel RGPD.

**El tractament consistirà en:**

Concreció dels tractaments a realitzar:

 Acarament  Interconnexió

X Conservació  Limitació

X Consulta X Modificació

X Comunicació X Organització

X Comunicació per transmissió X Recollida

 Destrucció X Registre

 Difusió X Supressió

X Extracció X Utilització

**2. Identificació de la informació afectada**

Per executar les prestacions derivades del compliment de l’objecte d’aquest encàrrec, cadascuna de les entitats contractants relacionades a la Clàusula 1.1 d’aquest PCAP, Responsables del Tractament, posen a disposició i permeten la recollida per la contractista, entitat encarregada del tractament, la informació que es descriu a continuació:

* Dades identificatives i laborals dels treballadors usuaris dels serveis necessàries per a la prestació dels servei contractats (nom i cognoms, categoria, lloc de treball, funcions, ...).
* Dades relatives als resultats dels estudis d’avaluacions de riscos, en el marc dels serveis de vigilància de la salut col·lectiva prevista a l’apartat II.1.1.1.a) del Plec de Prescripcions Tècniques, amb el següent contingut mínim:
	+ 1. Descripció detallada del lloc de treball.
		2. Riscos detectats.
		3. Mesures preventives adoptades.

La informació sobre l'estat de salut de les persones treballadores, com ara proves diagnòstiques, cirurgies, malalties, discapacitats, medicaments, antecedents familiars etc., que constitueix l’anomenada “Història Clínica-laboral”, comprèn el conjunt de documents relatius als processos assistencials de cada persona i té com a finalitat principal facilitar l'assistència sanitària, deixant constància de totes les dades que, sota criteri mèdic, permetin el coneixement veraç i actualitzat de l'estat de salut. Aquesta informació sobre l'estat de salut de les persones treballadores podrà ser recollida per l’adjudicatari per la prestació del servei de vigilància de la salut individual i servei mèdic d’empresa, en qualitat de Responsable del Tractament, d’acord amb les resolucions de les Autoritats de Control.

**3. Durada**

Aquest annex té la durada prevista al punt 1.5 del present plec clàusules adm. particulars, sense perjudici del que es preveu a l’apartat r) de la clàusula 4 següent.

**4. Obligacions de l’entitat encarregada del tractament**

L’entitat encarregada del tractament i tot el seu personal s’obliga a:

1. Utilitzar les dades personals objecte de tractament, o les que reculli per a la seva inclusió, només per a la finalitat objecte d'aquest encàrrec. En cap cas pot utilitzar les dades per a finalitats pròpies o diferents de la referida a l’objecte d’aquest encàrrec.
2. Tractar les dades d’acord amb les instruccions dels responsables del tractament.

Si l'entitat encarregada del tractament considera que alguna de les instruccions infringeix el RGPD o qualsevol altra disposició en matèria de protecció de dades de la Unió o dels estats membres, l'entitat encarregada n’ha d’informar immediatament els responsables.

1. Portar, per escrit, un registre de totes les categories d’activitats de tractament efectuades per compte dels responsables, que contingui:
2. El nom i les dades de contacte de l'entitat encarregada (o encarregades) i de cada responsable per compte del qual actua l'entitat encarregada i, si escau, del representant del responsable o de l’entitat encarregada i del delegat de protecció de dades.
3. Les categories de dades personals de tractaments efectuats per compte de cada responsable.
4. Si escau, les transferències de dades personals a un tercer país o organització internacional, inclosa la identificació d’aquest país o aquesta organització internacional, i en el cas de les transferències indicades a l'article 49, apartat 1, paràgraf segon de l’RGPD, la documentació de garanties adequades.
5. Una descripció general de les mesures tècniques i organitzatives de seguretat relatives a:
* La pseudonimització i el xifrat de dades personals.
* La capacitat de garantir la confidencialitat, la integritat, la disponibilitat i la resiliència permanents dels sistemes i serveis de tractament.
* La capacitat de restaurar la disponibilitat i l’accés a les dades personals de forma ràpida, en cas d’incident físic o tècnic.
* El procés de verificació, avaluació i valoració regulars de l’eficàcia de les mesures tècniques i organitzatives que garanteixen l’eficàcia del tractament.

1. No comunicar les dades a terceres persones, tret que tingui l'autorització expressa dels responsables del tractament, en els supòsits legalment admissibles.

L'entitat encarregada pot comunicar les dades a altres entitats encarregades del tractament del mateix responsable, d'acord amb les instruccions d’aquest. En aquest cas, els responsables han d’identificar, prèviament i per escrit, l'entitat a la qual s'han de comunicar les dades, les dades a comunicar i les mesures de seguretat que cal aplicar per procedir a la comunicació.

Si l'entitat encarregada ha de transferir dades personals a un tercer país o a una organització internacional, en virtut del dret de la Unió o dels estats membres que li sigui aplicable, ha d’informar els responsables d'aquesta exigència legal de manera prèvia, tret que aquest dret ho prohibeixi per raons importants d'interès públic.

1. **Subcontractació**

S’autoritza l’entitat encarregada a subcontractar, amb les limitacions establertes al punt. 2.11 del present plec de clàusules administratives particulars.

Per subcontractar amb altres empreses, l'entitat encarregada ha de comunicar aquest fet per escrit als responsables i identificar de forma clara i inequívoca els tractaments que es pretén subcontractar, l'entitat subencarregada i les seves dades de contacte. La subcontractació es pot dur a terme si els responsables no hi manifesten oposició en el termini establert.

La subcontractista/subentitat encarregada, que també té la condició d'entitat encarregada del tractament, està obligada igualment a complir les obligacions que aquest document estableix per a l'entitat encarregada del tractament i les instruccions que dictin els responsables. Correspon a l'entitat encarregada inicial regular la nova relació, de manera que la nova entitat encarregada quedi subjecte a les mateixes condicions (instruccions, obligacions, mesures de seguretat…) i amb els mateixos requisits formals que ella, pel que fa al tractament adequat de les dades personals i a la garantia dels drets de les persones afectades. Si la subencarregada ho incompleix, l'entitat encarregada inicial continua sent plenament responsable davant els responsables pel que fa al compliment de les obligacions.

1. Mantenir el deure de secret respecte de les dades personals a les quals hagi tingut accés en virtut d’aquest encàrrec, fins i tot després que en finalitzi l’objecte.
2. Garantir que les persones autoritzades per tractar dades personals es comprometen, de forma expressa i per escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents, de les quals cal informar-los convenientment.
3. Mantenir a disposició dels responsables la documentació que acredita que es compleix l'obligació que estableix l'apartat anterior.
4. Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per a tractar dades personals.
5. Assistir el responsable del tractament en la resposta a l'exercici dels drets següents:
6. Accés, rectificació, supressió i oposició
7. Limitació del tractament
8. Portabilitat de dades

L'entitat encarregada del tractament ha de resoldre, per compte dels responsables i dins del termini establert, les sol·licituds d'exercici dels drets d'accés, rectificació, supressió i oposició, limitació del tractament i portabilitat de dades, en relació amb les dades objecte de l'encàrrec.

L’entitat encarregada del tractament haurà de comunicar-ho als responsables del contracte que s’han indicat al punt 2.18 del present plec de clàusules administratives particulars, segons pertoqui, les sol·licituds rebudes i les resolucions efectuades per al seu coneixement.

1. Dret d’informació i consentiment

L'entitat encarregada del tractament ha de facilitar, en el moment de recollir les dades, la informació relativa als tractaments de dades que es duran a terme i, quan s’escaigui, recollir el consentiment. La redacció i el format en què es facilitarà la informació i es prestarà el consentiment s'ha de consensuar amb els responsables, abans d’iniciar la recollida de les dades.

1. **Notificació de violacions de la seguretat de les dades.**
2. **L'entitat encarregada del tractament ha d’informar i comunicar el responsable del tractament** que pertoqui, sense dilació indeguda i en qualsevol cas abans del termini màxim de 24 hores, de les violacions de la seguretat de les dades personals al seu càrrec que constitueixin un risc per als drets i llibertats de les persones físiques (en els termes previstos al bloc normatiu de protecció de dades personals d’aplicació en cada moment) de les quals tingui coneixement, juntament amb tota la informació rellevant per documentar i comunicar la incidència.

Si se’n disposa, cal facilitar, com a mínim, la informació següent:

1. Descripció de la naturalesa de la violació de la seguretat de les dades personals, incloses, quan sigui possible, les categories de dades i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats.
2. Nom i dades de contacte del delegat de protecció de dades o d'un altre punt de contacte en el qual es pugui obtenir més informació.
3. Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.
4. Descripció de les mesures adoptades o proposades per posar remei a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar els possibles efectes negatius.

Si no és possible facilitar la informació simultàniament, i en la mesura en què no ho sigui, la informació s’ha de facilitar de manera gradual sense dilació indeguda.

1. **Si la violació de seguretat es produeix en el tractament de les dades personals de la prestació del servei de vigilància de la salut individual i servei mèdic d’empresa**, en el que l’empresa contractista té la consideració de Responsable del Tractament, **correspon a aquesta comunicar les violacions de la seguretat de les dades personals a l'Autoritat de Control que pertoqui** pels canals previstos per la pròpia Autoritat i en els termes previstos al bloc normatiu de protecció de dades personals d’aplicació en cada moment. Així mateix, haurà d’informar al Delegat de Protecció de Dades l’entitat contractant relacionada a la Clàusula 1.1 d’aquest PCAP que es vegi afectada en el moment de conèixer l’esmentada violació. En aquest àmbit, correspon també a la contractista comunicar en el menor temps possible als interessats les violacions de la seguretat de les dades personals, quan sigui probable que la violació suposi un alt risc per als drets i les llibertats de les persones físiques. Altrament, haurà d’informar i lliurar còpia de la comunicació als interessats al Delegat de Protecció de Dades l’entitat contractant relacionada a la Clàusula 1.1 d’aquest PCAP que es vegi afectada.
2. Donar suport als responsables del tractament a l’hora de fer les avaluacions d'impacte relatives a la protecció de dades, quan escaigui.
3. Donar suport als responsables del tractament a l’hora de fer les consultes prèvies a l'autoritat de control, quan escaigui.
4. Posar a disposició dels responsables tota la informació necessària per demostrar que compleix les seves obligacions, així com per realitzar les auditories o les inspeccions que efectuïn la responsable o un altre auditor autoritzat per ella.
5. **Seguretat de la informació.**

La seguretat de la informació ha d’haver-se pensat des del disseny del servei d’informació i per tant es tracta d’un requeriment funcional que el contractista es troba obligat a considerar, especialment si es fa ús de portals d’accés web o solucions cloud.

En tot cas, la contractista està obligada:

* al compliment normatiu del “Reglament europeu 2016/679, de 27 d’abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (RGPD)”i la normativa sectorial que sigui d’aplicació.
* a implementar les mesures de seguretat necessàries per donar compliment al que estableixen la Disposició addicional primera de la Llei orgànica 3/2018, de 5 de desembre, de Protecció de dades Personals i garantia dels drets digitals, sobre Mesures de seguretat a l’àmbit del sector públic, i el Reial Decret 311/2022, de 3 maig, pel que es regula l’Esquema Nacional de Seguretat (ENS).

De la mateixa manera l’empresa contractista vetllarà per l’acompliment de les obligacions de confidencialitat i deure de secret del seu personal pel que fa a les dades personals als sistemes d’informació i a qualsevol altre informació o recurs corporatiu que hi puguin tenir accés en el decurs del present contracte.

Si s’escau, tots els dispositius que intervinguin en l’execució d’aquest contracte hauran d’estar configurats per a l’eliminació d’arxius de dades temporals, permetent eliminar els residus del material confidencial que s’originen a l’hora de digitalitzar, imprimir, copiar i enviar correu-e diàriament.

A petició de qualsevol entitat contractant relacionada a la Clàusula 1.1 d’aquest PCAP, de forma puntual o periòdica, l’empresa contractista (entitat encarregada) haurà d’efectuar una autoavaluació de compliment de l’ENS, que haurà d’estar signada pel responsable de seguretat de l’entitat encarregada o, cas de no tenir-ne, pel DPD.

Així mateix, haurà d’adoptar totes aquelles mesures i mecanismes per a:

1. Garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament.
2. Restaurar la disponibilitat i l'accés a les dades personals de forma ràpida, en cas d'incident físic o tècnic.
3. Verificar, avaluar i valorar, de forma regular, l'eficàcia de les mesures tècniques i organitzatives implantades per garantir la seguretat del tractament.
4. Pseudonimitzar i xifrar les dades personals, si escau.

L'adhesió a codis de conducta o la possessió d'una certificació són elements que serveixen per a demostrar el compliment dels requisits indicats anteriorment. Cal facilitar la informació sobre aquestes certificacions.

1. Tenir designat un delegat de protecció de dades i comunicar-ne la identitat i les dades de contacte als responsables del tractament.
2. Destí de les dades

Lliurar a l'entitat encarregada que els responsables del tractament designin per escrit, les dades personals necessàries per la prestació del servei i, si escau, els suports on constin, una vegada complerta la prestació.

L’entitat encarregada una vegada complerta la prestació contractual, garantirà la portabilitat de les dades relatives a la vigilància de la salut dels treballadors de cadascuna de les entitats contractants relacionades a la Clàusula 1.1 d’aquest PCAP a la nova empresa que desenvolupi el servei de vigilància de la salut.

Quan es produeixi el canvi en l’empresa que presta el servei, d’acord amb l’article 23.1 d) de la Llei 31/1995, de 8 de novembre, de Prevenció de Riscos Laborals, cadascuna de les entitats contractants relacionades a la Clàusula 1.1 d’aquest PCAP es troba obligada a, “elaborar i conservar a disposició de la autoritat laboral” la documentació relativa a la “Pràctica dels controls de l’estat de la salut dels treballadors prevista a l’article 22 d’aquesta Llei i les conclusions obtingudes dels mateixos en els termes recollits al darrera paràgraf de l’apartat 4 de l’esmentat article. No obstant, atès que es prohibeix la transmissió de la informació mèdica obtinguda a l’empara de la Llei 31/1995 de prevenció de riscos laborals, a qualsevol tercer diferent del “personal mèdic i a les autoritats sanitàries que portin a terme la vigilància de la salut dels treballadors”, amb l’única excepció de les conclusions derivades de dit seguiment quant a l’aptitud dels treballadors (art. 22.4 paràgraf tercer), les dades que es trobin incloses en la denominada història clínica-laboral només podran ser lliurades al personal sanitari o centre mèdic encarregat dels serveis de prevenció i directament entre els serveis mèdics de les empreses de prevenció: un cop finalitzada la relació contractual l’entitat encarregada lliurarà còpia al nou servei de prevenció que es farà càrrec de la vigilància de la salut d’aquelles dades que siguin d’interès per al seguiment des del punt de vista de la prevenció de riscos laborals amb l’objectiu de facilitar el seguiment de la salut dels treballadors, assegurant la seva continuïtat. El servei de prevenció de destí serà indicat per per l’entitat corresponent de les entitats contractants relacionades a la Clàusula 1.1 d’aquest PCAP). Durant aquest procés cal mantenir en tot moment els sistemes de custòdia que garanteixen la confidencialitat de les dades.

L’entitat encarregada, haurà de conservar la documentació clínica en les condicions que garanteixin el seu correcte manteniment i seguretat d’acord amb l’article 17 de la Llei 41/2002, de 14 de novembre, bàsica reguladora de l’autonomia del pacient i de drets i obligacions en matèria d’informació i documentació clínica i l’article 12 de la Llei 21/2000, de 29 de desembre, sobre els drets d’informació concernent la salut i l’autonomia del pacient, i la documentació clínica.

Pel que fa a les dades de les revisions de la Salut complementaries (ginecològiques i urològiques per a homes majors de 45 anys), el contractista, haurà de conservar la documentació clínica en les condicions que garanteixin el seu correcte manteniment i seguretat d’acord amb l’article 17 de la Llei 41/2002, de 14 de novembre, bàsica reguladora de l’autonomia del pacient i de drets i obligacions en matèria d’informació i documentació clínica i l’article 12 de la Llei 21/2000, de 29 de desembre, sobre els drets d’informació concernent la salut i l’autonomia del pacient, i la documentació clínica.

La resta de documentació i suports que contingui dades personals hauran de ser eliminades en finalitzar la prestació contractual dels equips informàtics utilitzats per l'entitat encarregada.

Una vegada destruïdes, l’entitat encarregada n’ha de certificar la destrucció per escrit i ha de de lliurar el certificat al responsable del tractament.

No obstant això, l'entitat encarregada pot conservar-ne una còpia, amb les dades degudament bloquejades, mentre es puguin derivar responsabilitats de l'execució de la prestació. En aquest cas, caldrà que notifiqui al responsable que conservarà una còpia de les dades amb aquest objectiu, indicant la motivació legal, el termini de temps que està obligat a retenir-les bloquejades i comprometent-se a la seva destrucció un cop vençut aquest termini de retenció. La responsable li podrà demanar l’aportació d’una anàlisi de riscos sobre el seu sistema de retenció.

**5. Obligacions dels responsables del tractament**

Correspon als responsables del tractament (entitats contractants):

1. Lliurar a l'entitat encarregada i permetre la recollida de les dades a les quals es refereix la clàusula 2 d'aquest document.
2. En els casos pertoqui, fer una avaluació de l'impacte en la protecció de dades personals de les operacions de tractament que ha d’efectuar l'entitat encarregada.
3. Fer les consultes prèvies que correspongui, tan sols en el cas que pertoqui.
4. Vetllar, abans i durant tot el tractament, perquè l’entitat encarregada compleixi el RGPD, la LOPDGDD i la resta de normativa de protecció de dades vigent.
5. Supervisar el tractament, inclosa l’execució d’inspeccions i auditories.
6. Autoritzar a l’entitat encarregada del tractament a:
7. dur a terme el tractament de les dades personals en dispositius portàtils de tractament de dades únicament pels usuaris o perfils d’usuaris assignats a la prestació de serveis contractada.
8. dur a terme el tractament fora dels locals dels responsables del tractament únicament pels usuaris o perfils d’usuaris assignats a la prestació de serveis contractada.
9. l’entrada i sortida dels suports i documents que continguin dades personals, inclosos els compresos i/o annexes a un correu electrònic, fora dels locals sota el control dels responsables del tractament.
10. l’execució dels procediments de recuperació de dades que l’entitat encarregada del tractament es vegi en l’obligació d’executar.
11. tractar les dades en els seus locals, aliens als dels responsables del tractament.

**6. Incompliments i responsabilitats**

L’incompliment del que s’estableix en els apartats anteriors pot donar lloc a que l’entitat o empresa encarregada sigui considerada responsable del tractament, als efectes d’aplicar el règim sancionador i de responsabilitats previst a la normat