FITXES DEL DPD **Ref. 10/2021**

Contractació i encarregats de tractament

Tractament de dades personals de l'adjudicatari per compte de l'entitat pública contractant

L'adjudicació de contractes del sector públic pot comportar que el contractista tracti dades personals per conte del responsable, l'entitat contractant.

El Reial Decret 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions, que modifica la llei de contractes de sector públic, estableix diverses mesures en matèria de contractació pública, totes elles, segons es disposa en la seva exposició de motius, dirigides a reforçar el compliment de la normativa sobre protecció de dades personals i la protecció de la seguretat pública en aquest àmbit.

Responsable de tractament

- És qui determina la **finalitat** del tractament (és a dir, per a què es realitza el tractament?).
- És qui determina els **elements essencials** del tractament (és a dir com es realitza el tractament?).
- Té la **responsabilitat principal** de garantir el compliment de la normativa.
- Té el **control** sobre els tractament, tot i que per ser considerat responsable **no és necessari que tingui un control total**.

Encarregat de tractament

- Tracta les dades **en nom del responsable.**
- Ha de **seguir les instruccions** del responsable, i està **vinculat a les finalitats i als elements de tractament** que el responsable hagi inclòs.
- Pot determinar els **elements no essencials** del tractament.
- És **responsable del compliment de la part encarregada** i de **fer-ho seguint les instruccions** del responsable.
- Té obligació de **col·laborar amb el responsable**.

"Els contractistes del sector públic manegen en ocasions, per a l'execució dels respectius contractes, un ingent volum de dades personals, l'ús inadequat pot, al seu torn, plantejar riscos per a la seguretat pública.

Per això, resulta necessari assegurar normativament la seva submissió a certes obligacions específiques que garanteixin tant el compliment de la normativa en matèria de protecció de dades personals com la protecció de la seguretat pública."

L'adjudicatari com a encarregat de tractament

Quan el contracte que s'adjudica comporta tractament de dades, l'entitat contractant actua com a responsable de tractament, en tant que determina els fins i mitjans de tractament (art. 4.7 RGPD[1]) i l'adjudicatari serà l'encarregat de tractament, ja que és qui tractaria les dades personals per compte del responsable de tractament (art. 4.8 RGPD).

Al punt 2 de la Disposició addicional vint-i-cinquena LSCP[2] es confirma aquesta condició i disposa:

- *"Per al cas que la contractació impliqui l'accés del contractista a dades de caràcter personal, el tractament de la qual sigui responsable l'entitat contractant, aquell tindrà la consideració d'encarregat de el tractament."*

I. Adjudicació » **II. Formalització** » **III. Finalització**

I. ADJUDICACIÓ

Per tal de garantir que en el tractament de dades que es deriva del contracte que s'adjudica, es dona compliment als requeriments de la normativa de protecció de dades, l'entitat contractant en la seva qualitat de responsable de tractament ha de seleccionar únicament a aquell adjudicatari que doni garanties suficients per aplicar les mesures tècniques i organitzatives apropiades.

Tingues en compte!

El responsable de tractament ha de triar únicament un encarregat que ofereixi garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme i garanteixi la protecció dels drets dels interessats.

[1] Reglament general de protecció de dades
[2] Llei de contractes del sector públic

ATENCIÓ!!!!!

L'**adhesió** de l'encarregat de tractament a un **codi de conducta** aprovat d'acord amb l'article 40 de l'RGPD, o un **mecanisme de certificació** aprovat d'acord amb l'article 42 RGPD, es pot utilitzar com a element per demostrar **l'existència de les garanties suficients**, però això no vol dir que no es puguin fer servir altres mètodes per acreditar l'existència d'aquestes garanties.

Mesures de seguretat

El Reial Decret 3/2010 de 8 de gener, regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica. **L'Esquema Nacional de Seguretat (ENS)** està constituït pels principis bàsics i requisits mínims requerits per a una protecció adequada de la informació. Serà aplicat per les administracions públiques per assegurar l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informacions i serveis utilitzats en mitjans electrònics que gestionin en l'exercici de les seves competències.

En el cas de tractament de dades personals, l'àmbit d'aplicació de l'ENS ha estat ampliat per la disposició addicional primera de la LOPDGDD que estableix:

"1. L'Esquema Nacional de Seguretat inclourà les mesures que s'hagin d'implantar en cas de tractament de dades personals per evitar la seva pèrdua, alteració o accés no autoritzat, adaptant els criteris de determinació de el risc en el tractament de les dades al que estableix l'article 32 del Reglament (UE) 2016/679.

2. Els responsables enumerats en l'article 77.1 d'aquesta llei orgànica d'aplicar als tractaments de dades personals les mesures de seguretat que corresponguin de les previstes en l'Esquema Nacional de Seguretat, així com impulsar un grau d'implementació de mesures equivalents a les empreses o fundacions vinculades als mateixos subjectes a dret privat."

Si els sistemes són de categoria bàsica, el contractista haurà d'aportar:

Una **declaració de conformitat de l'ENS** que verifiqui el compliment dels requeriments previstos en l'ENS, almenys cada dos anys. Aquesta autoavaluació pot ser desenvolupada pel mateix personal que administra el sistema d'informació o en qui aquest delegui.

I es completarà amb un **distintiu de declaració de conformitat.**

Si els sistemes són de categoria mitjana o alta, el contractista haurà d'aportar:

Una certificació de conformitat. Una auditoria formal que verifiqui el compliment dels requeriments previstos a l'ENS, almenys cada dos anys, expedida per una entitat certificadora.

I es completarà mitjançant un **distintiu de certificació de conformitat.**

Tingues en compte!

L'ENS és una norma d'obligat compliment per a tots els Sistemes d'Informació de les administracions públiques, independentment de la seva ubicació. Per tant, és també exigible el compliment de l'ENS als Sistemes d'Informació que operats per tercers - fins i tot, en dependències de tercers- desenvolupen funcions, missions, comesos o serveis per a les administracions públiques.

Transferències internacionals

Pel que fa a les transferències internacionals, cal tenir en compte l'article 4 del Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions que modifica la Llei 40/2015, 1 d'octubre, de Règim Jurídic del Sector Públic i s'introdueix un nou article 46 bis que queda redactat de la següent manera:

Artículo 46 bis. "Ubicación de los sistemas de información y comunicaciones para el registro de datos.

Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ***ubicarse y prestarse dentro del territorio de la Unión Europea****.*

Los datos a que se refiere el apartado anterior ***no podrán ser objeto de transferencia*** *a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una* ***decisión de adecuación de la Comisión Europea*** *o cuando así lo exija el cumplimiento de las* ***obligaciones internacionales*** *asumidas por el Reino de España."*

Tingues en compte!

On estan allotjats els servidors

Amb la finalitat de facilitar el procés de selecció de l'adjudicatari que més garanties ofereixi, es recomana verificar les mateixes mitjançant mecanismes que permetin a l'entitat contractant valorar el grau de compliment dels candidats en relació a la normativa de protecció de dades.

Podeu trobar com Annex 1 un **Model de llista de verificació per a contractació menor** i un **Model de llista de verificació estandarditzat de contractació.**

En la llista de verificació es **valora el nivell d'adaptació del candidat a encarregat de tractament** al RGPD, el nivell de compliment de les seves obligacions, si té subcontractada part de la seva activitat de tractament, l'existència o no de mitjans per garantir que el subencarregat compleix les instruccions del responsable, la seguretat del tractament amb l'adopció de mesures tècniques i organitzatives per garantir la seguretat de les dades i si es realitzen o no transferències internacionals de dades amb les garanties del RGPD.

II. FORMALITZACIÓ

Els contractes del sector públic queden perfeccionats mitjançant la formalització del contracte per escrit, excepte en els casos dels contractes menors, els contractes basats en un acord marc i els contractes específics en el marc d'un sistema dinàmic d'adquisició els quals es perfeccionen amb l'adjudicació.

No obstant, en cas d'haver-hi un tractament de dades per compte de l'entitat contractant en aquest moment de perfeccionament del contracte, s'ha de formalitzar també **l'acord d'encàrrec de tractament** amb l'empresa adjudicatària que tindrà accés a les dades personals responsabilitat de l'entitat.

Què ha d'incloure l'acord d'encàrrec de tractament?

Aquest **acord d'encàrrec** de tractament ha de tenir un contingut mínim, regulat expressament a l'article 28 del RGPD, i ha de fer referència a aspectes com:

- Objecte del contracte
- Durada
- Naturalesa i finalitat del tractament.
- Tipologia de dades personals tractades.
- Categories d'interessats afectats.
- Obligacions i drets del responsable.

A més, l'acord d'encàrrec del tractament haurà de regular específicament:

- Les instruccions definides pel responsable de tractament sobre com haurà de tractar l'encarregat les dades personals a les que tindrà accés.
- L'obligació de l'encarregat d'adoptar les mesures de seguretat determinades pel responsable de tractament i definides als plecs.
- La forma en que l'encarregat de tractament donarà suport al responsable en la tramitació de les peticions dels interessats relacionades amb l'exercici de drets.
- La forma en que l'encarregat de tractament haurà de donar suport al responsable per complir amb les obligacions en matèria de protecció de dades com poden ser la comunicació de les violacions de seguretat, la realització d'avaluacions d'impacte o bé, la realització de consultes prèvies.
- El destí de les dades personals tractades per l'encarregat, un cop finalitzada la relació contractual principal.
- El règim de subcontractació de proveïdors per desenvolupar l'objecte del contracte.
- L'obligació de l'encarregat de col·laborar amb el responsable per demostrar quan resulti necessari el compliment de les obligacions així com la realització d'auditories o inspeccions.

ATENCIÓ!!!!!

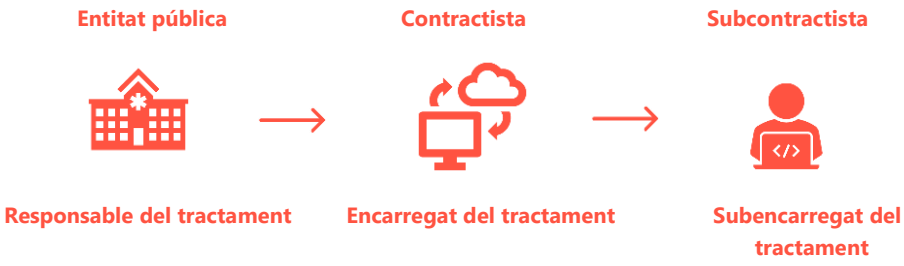
Es tracta de regular **per escrit** mitjançant un document vinculant **la relació entre el responsable i l'encarregat de tractament** en relació al tractament de dades personals en el curs de l'execució del contracte principal.

Podeu trobar com Annex 2 un **Model d'acord d'encàrrec de tractament.** Haureu de tenir en compte que es tracta d'una plantilla que haurà de ser modificada per tal d'ajustar-la a les necessitats concretes de cada contracte licitat.

En cas de **no produir-se un tractament de dades** però de l'activitat es pugui derivar un accés incidental a les mateixes, recomanem la signatura d'un **compromís de confidencialitat**.

Podeu trobar com Annex 3 un **Model de compromís de confidencialitat.**

En aquells casos en que el contractista vulgui comptar amb un tercer perquè realitzi parcialment la prestació contractada, sempre i quan es trobi degudament prevista aquesta possibilitat per l'entitat contractant, serà necessari regular aquesta relació amb el tercer mitjançant un **contracte de subencarregat** de tractament.



És important tenir en compte que **el subencarregat quedarà igualment sotmès a les mateixes condicions que s'hagin definit per l'encarregat de tractament en tot allò relatiu a la seguretat de les dades personals.** Resultant per tant, també subjecte obligat al compliment dels deures en matèria de protecció de dades i a oferir les garanties necessàries per la seguretat de les dades personals a les que tindrà accés a raó de la prestació realitzada en qualitat de subencarregat de tractament.

Aquesta relació amb el subencarregat, haurà de ser degudament formalitzada mitjançant el corresponent contracte de subencarregat de tractament.

III. FINALITZACIÓ

Un cop el contractista ha realitzat la totalitat de la prestació objecte del contracte entenem que s'ha complert amb el contracte i es dona per finalitzada la relació establerta amb el contractista tant en relació amb el contracte principal com amb l'acord d'encàrrec de tractament.

Per tant, el contractista ja no haurà de tractar les dades per compte del responsable de tractament i **haurà de procedir a realitzar el retorn o la destrucció de les dades personals segons hagi indicat expressament el responsable de tractament.**

Per tal d'acreditar l'efectiu compliment d'aquesta obligació final, l'encarregat de tractament haurà de **certificar l'efectiva devolució o destrucció de les dades personals.**

Podeu trobar com Annex 4 un **Model de certificació del retorn o destrucció de dades.**

En cas de dubte, pots posar-te en contacte amb el DPD

dpd@ticsalutsocial.cat

ANNEX 1 Model de llistat de verificació

1.1 Model per a contractació menor

En/Na .....(nom i cognoms)..... en qualitat de .....(càrrec)....., en representació de l'entitat ..... (nom de l'entitat).....que actua com encarregada del tractament de.....

DECLARO que son certes les circumstàncies reflexades a continuació que s'aporten per a la formalització de la contractació.

I- ADEQUACIÓ DE L'ENCARREGAT DE TRACTAMENT AL RGPD			
PREGUNTES	SI	NO	OBSERVACIONS
Com a ENCARREGAT, t'has adaptat al RGPD?			
Has elaborat i portes per escrit un registre de totes les categories d'activitats de tractament efectuades per compte del RESPONSABLE?			
Has nomenat un Delegat de Protecció de Dades?			
Has realitzat un anàlisi de riscos en protecció de dades i en matèria de seguretat informàtica per als SI dels quals ets responsable?			
II- OBLIGACIONS DE L'ENCARREGAT DE TRACTAMENT (ET)			
PREGUNTES	SI	NO	OBSERVACIONS
Limitació de l'ús de les dades: Com a ET, tractes les dades personals únicament per a les finalitats específiques del tractament indicat en el contracte d'ET?			
Instruccions: Com a ET, tractes les dades personals seguint únicament les instruccions documentades del RT?			
Limitació de l'accés a les dades: S'ha limitat l'accés al personal a la informació necessària per a l'execució/gestió/seguiment de l'encàrrec.			
Confidencialitat i deure de secret: el personal ha signat normes d'ús de les TIC i compromís de confidencialitat?			
Documentació i compliment: Com a ET, pots demostrar el compliment de les clàusules previstes en el contracte d'encàrrec de tractament?			
Suport al RESPONSABLE de tractament: Com a ET, pots assistir al responsable en les seves obligacions com: exercici dels drets, avaluacions d'impacte, notificacions de violacions de seguretat, etc?			
Dades sensibles: Com a ET, apliques restriccions específiques i/o garanties addicionals en el tractament de dades sensibles (dades relatives a la salut, dades genètiques)?			

III- RECURS A SUBENCARREGATS			
PREGUNTES	SI	NO	OBSERVACIONS
Com a ET, subcontractes part de l'activitat(s) de tractament?			
Com a ET, has previst els mitjans per garantir que el subencarregat compleix les instruccions del RESPONSABLE?			
IV- SEGURETAT DEL TRACTAMENT: MESURES TÉCNIQUES I ORGANITZATIVES PER GARANTIR LA SEGURETAT DE LES DADES			
PREGUNTES	SI	NO	OBSERVACIONS
S'implementen mesures per garantir la confidencialitat, integritat, disponibilitat i resiliència permanent dels sistemes i serveis de tractament?			
S'implementen mesures per a la identificació i autorització dels usuaris?			
Com a ET, has superat una auditoria en matèria de seguretat de la informació realitzada per un tercer?			
Com a ET, apliques a les dades tractades del responsable mesures com la pseudonimització o el xifrat?			
Com a ET, disposes d'algun Sistema de Gestió de la Seguretat de la Informació i/o Sistema de Gestió de la Informació?			
Com a ET, disposes d'alguna certificació de seguretat (ISO 27001 o ENS) o està adherit a algun codi de bones pràctiques de protecció de dades?			
Com a ET, proporciones un punt de contacte efectiu pels assumptes relacionats amb la protecció de dades (no únicament una adreça de e-mail)?			
Serveis informàtics: L'ET proporciona contractualment uns nivells de servei mínims davant interrupcions o talls del servei com l'SLA?			
Com a ET, tens dependència dels seus subencarregats (per exemple, aportem una plataforma de hosting)?			
V- TRANSFERENCIES INTERNACIONALS PER PART DE L'ET			
PREGUNTES	SI	NO	OBSERVACIONS
Com a ET, allotges les dades del responsable (o còpies de seguretat), en països fora de l'EEE?			
Com a ET, ho fas seguint les instruccions documentades del responsable o en virtut d'una exigència legal que li sigui aplicable?			
Com a ET, ho fas amb les garanties del RGPD?			

1.2 Model estandarditzat de contractació

En/Na .....(nom i cognoms)..... en qualitat de .....(càrrec)....., en representació de l'entitat ..... (nom de l'entitat).....que actua com encarregada del tractament de.....

DECLARO que son certes les circumstàncies reflexades a continuació que s'aporten per a la formalització de la contractació.

I- ADEQUACIÓ DE L'ENCARREGAT DE TRACTAMENT AL RGPD			
PREGUNTES	SI	NO	OBSERVACIONS
Com a ENCARREGAT, t'has adaptat al RGPD? *Enviar documentació que ho acrediti.*			
Has elaborat i portes per escrit un registre de totes les categories d'activitats de tractament efectuades per compte del RESPONSABLE? *Enviar còpia.*			
Has nomenat un Delegat de Protecció de Dades? *Enviar còpia de la notificació realitzada en la seu electrònica de l'autoritat de control competent.*			
Has realitzat un anàlisi de riscos en protecció de dades i en matèria de seguretat informàtica per als SI dels quals ets responsable? *Enviar l'informe amb els resultats que afectin al tractament realitzat pel responsable.*			
II- OBLIGACIONS DE L'ENCARREGAT DE TRACTAMENT (ET)			
PREGUNTES	SI	NO	OBSERVACIONS
Limitació de l'ús de les dades: Com a ET tractes les dades personals únicament per a les finalitats específiques del tractament indicat en el contracte d'ET? *Enviar documentació que ho acrediti.*			
Instruccions: Com a ET, tractes les dades personals seguint únicament les instruccions documentades del RT?			
Limitació de l'accés a les dades: S'ha limitat l'accés al personal a la informació necessària per a l'execució/gestió/seguiment de l'encàrrec.			
Confidencialitat i deure de secret: el personal ha signat normes d'ús de les TIC i compromís de confidencialitat?			
Personal aliè a la plantilla, si escau (estudiants en pràctiques, autònoms, etc.): se'ls hi aplica els mateixos requisits que al personal de l'ET?			

Documentació i compliment: Com a ET, pots demostrar el compliment de les clàusules previstes en el contracte d'encàrrec de tractament?			
Documentació i compliment: Com a ET, disposes de protocols/procediments per donar resposta sense dilacions i de forma adequada a les consultes del RESPONSABLE relacionades amb el tractament?			
Formació en matèria de protecció de dades: Com a ET, has proporcionat el nivell requerit de formació, experiència professional o certificació de les persones involucrades en el tractament de dades personals i aquestes coneixen que tracten dades responsabilitat de tercers?			
Suport al RESPONSABLE de tractament: Com a ET, pots assistir al responsable en la resposta a l'exercici dels drets (d'accés, rectificació, supressió, oposició, limitació i a no ser objecte de decisions individualitzades automatitzades) de les persones afectades?			
Suport al RESPONSABLE de tractament: Com a ET, pots assistir al responsable en l'obligació de realitzar una avaluació d'impacte de les operacions de tractament en la protecció de dades personals?			
Suport al RESPONSABLE de tractament: Com a ET, pots assistir al responsable en l'obligació de consultar a l'autoritat de control abans de començar el tractament de dades?			
Suport al RESPONSABLE de tractament: Com a ET, pots assistir al responsable en l'obligació de garantir que les dades personals siguin exactes i estiguin actualitzades?			
Dades sensibles: Com a ET, apliques restriccions específiques i/o garanties addicionals en el tractament de dades sensibles (dades relatives a la salut, dades genètiques)?			
Notificacions de violacions de seguretat de les dades: Quan es tracta d'una violació de les dades tractades pel responsable: disposes d'un procediment per col·laborar amb el responsable i ajudar-lo a donar compliment a les obligacions que li atribueix el RGPD?			
Notificacions de violacions de seguretat de les dades: Quan es tracta d'una violació de les dades tractades pel propi encarregat: disposes d'un procediment per informar al responsable sense dilació indeguda i facilitar la informació requerida pel RGPD?			
III- RECURS A SUBENCARREGATS			
PREGUNTES	SI	NO	OBSERVACIONS
Com a ET subcontractes part de l'activitat(s) de tractament? *Identificar els subcontractes.*			
La part subcontractada és part fonamental de l'encàrrec de tractament?			

Els subencarregats formen part d'una llista tancada o es tracta de cadenes de subcontractació no definides en l'acord d'encàrrec de tractament? *Enviar llista de subencarregats*			
Com a ET, has previst els mitjans per garantir que el subencarregat compleix les instruccions del RESPONSABLE? *Acreditació de l'encàrrec*			
IV- SEGURETAT DEL TRACTAMENT: MESURES TÉCNIQUES I ORGANITZATIVES PER GARANTIR LA SEGURETAT DE LES DADES			
PREGUNTES	SI	NO	OBSERVACIONS
S'implementen mesures per garantir la confidencialitat, integritat, disponibilitat i resiliència permanent dels sistemes i serveis de tractament? *Acreditació mitjançant documentació on s'especifiquin les mesures de seguretat implementades*			
S'implementen processos de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament? *Acreditació mitjançant documentació on s'especifiquin els processos de seguretat implementats*			
S'implementen mesures per a la identificació i autorització de l'usuari? *Acreditació mitjançant documentació*			
S'implementen mesures per a la protecció de les dades durant la transmissió i l'emmagatzematge? *Acreditació mitjançant documentació*			
S'implementen mesures per garantir la configuració del sistema i el registre d'incidents? *Acreditació mitjançant documentació*			
S'implementen mesures per garantir la minimització, qualitat, i retenció limitada de les dades? *Acreditació mitjançant documentació*			
S'implementen mesures per poder permetre la portabilitat de les dades i garantir la supressió? *Acreditació mitjançant documentació*			
El RESPONSABLE ha definit per escrit les funcions dels perfils laborals implicats en el tractament de les dades? *Acreditació mitjançant còpia del document de definició de perfils*			
Com a ET, has superat una auditoria en matèria de seguretat de la informació realitzada per un tercer? Has proporcionat una còpia de les conclusions de la mateixa al RESPONSABLE? Es fa de forma periòdica?			

Acreditació mitjançant còpia del document amb els resultats de l'auditoria.			
Com a ET, apliques a les dades tractades del responsable mesures com la pseudonimització o el xifrat? *Descripció del mecanisme o aplicació informàtica utilitzada*			
Com a ET, disposes d'algun Sistema de Gestió de la Seguretat de la Informació i/o Sistema de Gestió de la Informació? *Acreditació mitjançant còpia del document d'implementació del SGSI*			
Com a ET, disposes d'alguna certificació de seguretat (ISO 27001 o ENS) o està adherit a algun codi de bones pràctiques de protecció de dades? *Acreditació mitjançant còpia del certificat o document*			
Com a ET, disposes de protocols i procediments de seguretat aplicables als tractaments en paper? *Acreditació mitjançant còpia del protocol o procediment*			
En algun moment s´ha fet pública la implicació de l'ET en alguna bretxa de seguretat o incident de protecció de dades?			
Com a ET, proporciones un punt de contacte efectiu pels assumptes relacionats amb la protecció de dades (no únicament una adreça de e-mail)? *Especificar els canals de comunicació establerts*			
Serveis informàtics: L'ET proporciona contractualment uns nivells de servei mínims davant interrupcions o talls del servei com l'SLA?			
Com a ET, tens dependència dels seus subencarregats (per exemple, aportem una plataforma de hosting)?			
L'ET disposa d'una assegurança de Responsabilitat Civil, Ciberseguretat o de Protecció de Dades que doni cobertura al servei?			
V- TRANSFERENCIES INTERNACIONALS PER PART DE L'ET			
PREGUNTES	SI	NO	OBSERVACIONS
Com a ET, allotges les dades del responsable (o còpies de seguretat), en països fora de l'EEE?			
Com a ET, ho fas seguint les instruccions documentades del responsable o en virtut d'una exigència legal que li sigui aplicable?			
Com a ET, ho fas amb les garanties del RGPD?			

ANNEX 2 Model d'encarregat de tractament

ACORD D'ENCÀRREC DE TRACTAMENT DE DADES DE CARÀCTER PERSONAL ENTRE ..... I .....

REUNITS

D'una banda, ..., com a responsable dels tractaments de protecció de dades de ....., mitjançant.....de ..... de .....de 2021, entre els qual s'inclou el tractament relatiu a ..... *(indicar nom del tractament)*....., en l'exercici de les funcions que li confereix el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en allò que fa referència al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD), i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

I de l'altra, el/la senyor/a .....*(nom i cognoms)* ....., ...*(especificar càrrec)*....., en representació de ..... *(nom de l'entitat)* ....., d'acord amb .....*(justificar representació)*, ... , com a encarregat de tractament,

Ambdues parts, en l'exercici de les funcions que els estan legalment assignades, reconeixent-se recíprocament la capacitat legal necessària per obligar-se de comú acord,

MANIFESTEN

I. Que....., d'acord amb les competències que té atribuïdes, li correspon la realització de ..... *(especificar les competències en les quals es troba inclòs l'objecte del tractament)* .....

II. Que l'empresa contractista ..... té per objecte .....

III. *(Referència al contracte que fa necessari signar l'acord i altra informació que sigui necessària; incloure, si escau, el núm. d'expedient contracte. Exemple: Ambdues parts han signat un contracte per X, amb expedient X)*

IV. Atès que l'execució del contracte esmentat per part de (empresa contractista) comporta tractar dades personals de les quals és responsable (òrgan de contractació), (empresa contractista) té la consideració d'encarregada del tractament, d'acord amb el RGPD i LOPDGDD.

V. Que *(empresa contractista)* disposa de la capacitat i els recursos necessaris per tal de garantir que, en la seva qualitat d'encarregat de tractament, aplica les mesures tècniques i organitzatives apropiades per complir amb el que estableix la legislació de protecció de dades esmentada.

VI. La necessitat de signar un acord d'encàrrec de tractament de dades de caràcter personal en relació amb el contracte esmentat, en els termes que estableixen els articles 28 del RGPD i 33 de la LOPDGDD.

CLÀUSULES

Primera.- Objecte de l'acord d'encàrrec

Mitjançant aquest acord d'encàrrec s'habilita l'entitat ....., en qualitat d'encarregat de tractament (en endavant, l'encarregat), per tractar per compte de.....(en endavant, el responsable) les dades de caràcter personal necessàries per a la realització de ..... *(objecte encarregat)*.....

El tractament consistirà en .....(*descripció detallada del tractament i de les actuacions concretes a realitzar*)

Segona.- Identificació de la informació afectada

Per executar les prestacions derivades del compliment de l'objecte d'aquest acord d'encàrrec, el responsable posa a disposició de l'encarregat la informació

Opció A

(Especificar tipus/categories de dades: (identificatives, de característiques personals, dades de salut: clíniques, etc).

Especificar categories de persones interessades: (col·lectius vulnerables, pacients, professionals sanitaris, ciutadans, etc).

..... que es descriu a continuació:

Opció B

(En el cas que l'objecte del contracte comporti el tractament de moltes categories de dades personals i/o de persones interessades, és millor remetre's a un annex en el qual constin. Es proposa redactat següent.).

..... corresponent als tractaments que es relacionen a l'annex 1.

Tercera.- Durada

La vigència d'aquest acord d'encàrrec queda vinculada a la durada del contracte subscrit que s'ha identificat en serà de ..... *(indicar vigència i fonamentar-la)*.....

Quarta.- Obligacions de l'encarregat de tractament

L'encarregat de tractament i tot el seu personal s'obliguen a:

a) Utilitzar les dades personals objecte de tractament, o les que reculli per a la seva inclusió, només per a la finalitat objecte d'aquest acord d'encàrrec. En cap cas poden utilitzar les dades per a finalitats pròpies.

b) Tractar les dades únicament d'acord amb les instruccions documentades del responsable de tractament.

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

c) Limitar l'accés a les dades personals tractades als membres del seu personal en la mesura que sigui estrictament necessari per a l'execució, la gestió i el seguiment de l'encàrrec. L'encarregat ha de garantir que les persones autoritzades per tractar les dades personals s´han compromès a respectar la confidencialitat o estan subjectes a una obligació de confidencialitat de naturalesa estatutària, així com a complir les mesures de seguretat corresponents, de les quals cal informar-los convenientment.

Mantenir a disposició del responsable la documentació que acredita el seu compliment.

d) Mantenir el deure de secret respecte de les dades personals a les quals hagin tingut accés en virtut d'aquest acord d'encàrrec, fins i tot després que en finalitzi l'objecte.

e) No comunicar les dades a terceres persones, tret que tingui l'autorització expressa del responsable de tractament en els supòsits legalment admissibles.

L'encarregat pot comunicar les dades a altres encarregats de tractament del mateix responsable, d'acord amb les instruccions del responsable. En aquest cas, el responsable ha d'identificar, prèviament i per escrit, l'entitat a la qual s'han de comunicar les dades, la finalitat, les dades a comunicar i les mesures de seguretat que cal aplicar per procedir a la comunicació.

f) Les transferències de dades a un tercer país o a una organització internacional per part de l'encarregat, únicament es poden realitzar seguint instruccions documentades del responsable o en virtut d'una exigència expressa del dret de la Unió o d'un estat membre al qual estigui subjecte l'encarregat.

g) Subcontractació

(Escollir una de les opcions)

Opció A:

No es poden subcontractar cap dels tractaments de dades inclosos en les prestacions que formen part de l'objecte d'aquest encàrrec.

Opció B:

Es poden subcontractar alguns dels tractaments de dades previstos en l'objecte d'aquest encàrrec.

Si cal subcontractar algun tractament, aquest fet s'ha de comunicar prèviament i per escrit al responsable, amb una antelació de ..... . Cal indicar els tractaments que es pretén subcontractar i identificar de forma clara i inequívoca l'empresa subcontractista i les seves dades de contacte. La subcontractació es pot dur a terme si el responsable no manifesta la seva oposició en el termini establert.

El subcontractista, que també té la condició d'encarregat de tractament, està obligat igualment a complir les obligacions que aquest document estableix per a l'encarregat de tractament i les instruccions que dicti el responsable. Correspon a l'encarregat inicial regular la nova relació, de manera

que el nou encarregat quedi subjecte a les mateixes condicions (instruccions, obligacions, mesures de seguretat...) i amb els mateixos requisits formals que ell, pel que fa al tractament adequat de les dades personals i a la garantia dels drets de les persones afectades. Si el subencarregat ho incompleix, l'encarregat inicial continua sent plenament responsable davant el responsable pel que fa al compliment de les obligacions.

En tot cas, el responsable ha d'estar informat de tota la cadena de subcontractació.

h) Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per tractar dades personals.

i) Assistir al responsable de tractament en la resposta a l'exercici dels drets següents:

1. Accés, rectificació, supressió i oposició.
2. Limitació del tractament.
3. Portabilitat de dades.
4. A no ser objecte de decisions individualitzades automatitzades (inclosa l'elaboració de perfils).

Quan les persones afectades exerceixin els drets d'accés, rectificació, supressió i oposició, limitació del tractament i a no ser objecte de decisions individualitzades automatitzades davant l'encarregat de tractament, aquest ho ha de comunicar per correu electrònic a l'adreça indicada a la clàusula vuitena d'aquest acord d'encàrrec. La comunicació s'ha de fer de forma immediata i en cap cas més enllà de l'endemà del dia en què s'ha rebut la sol·licitud, tenint en compte que si s'ha rebut en un dia no laborable, s'entendrà rebuda el primer dia laborable següent, juntament, si escau, amb altres informacions que puguin ser rellevants per resoldre la sol·licitud.

L'encarregat no ha de donar resposta per si mateix a dites sol·licituds llevat que hagi estat autoritzat pel responsable.

j) Dret d'informació.

(Escollir una de les opcions)

Opció A

L'encarregat de tractament ha de facilitar, en el moment de recollir les dades, la informació relativa als tractaments de dades que es duran a terme. La redacció i el format en què es facilitarà la informació s'ha de consensuar amb el responsable, abans d'iniciar la recollida de les dades.

Opció B

Correspon al responsable facilitar el dret d'informació en el moment de recollir les dades

k) L'encarregat també ha d'assistir al responsable a garantir el compliment de les següents obligacions tenint en compte la naturalesa del tractament i la informació de què disposi:

1. L'obligació de realitzar una avaluació d'impacte de les operacions de tractament en la protecció de dades personals, quan sigui probable que un determinat tractament suposi un alt risc per als drets i les llibertats de les persones físiques.

2. L'obligació de consultar a l'autoritat de control abans de començar el tractament, quan l'avaluació d'impacte relativa a la protecció de dades evidencii que el tractament comporta un alt risc si el responsable no adopta les mesures necessàries per a mitigar-lo.

3. L'obligació de garantir que les dades personals siguin exactes i estiguin actualitzades.

l) Posar a disposició del responsable tota la informació necessària per demostrar que compleix les seves obligacions, així com per realitzar les auditories o les inspeccions que efectuïn el responsable o un altre auditor autoritzat per ell.

m) Notificació de violacions de la seguretat de les dades.

En el supòsit de violació de la seguretat de les dades personals, l'encarregat ha de col·laborar amb el responsable i ajudar-lo a donar compliment a les obligacions que li atribueix el RGPD, de la manera següent:

1. Quan es tracti d'una violació de la seguretat de dades personals tractades pel responsable, l'encarregat ha d'assistir al responsable en les següents accions:

a) Notificar la violació de seguretat de les dades personals a l'autoritat de control sense dilació indeguda des què tingui constància, si escau.

b) Preparar tota la informació rellevant per documentar i comunicar la incidència, i que ha d'incloure com a mínim:

- Descripció de la naturalesa de les dades personals, incloses, quan sigui possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats.

- Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.

- 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.

c) Comunicar la violació de seguretat de les dades personals a l'interessat sense dilació indeguda des què tingui constància, si escau.

2. Quan es tracti d'una violació de la seguretat de dades personals tractades per l'encarregat:

   Ha d'informar el responsable de tractament, sense dilació indeguda i en qualsevol cas abans de 24 hores des que tingui constància, de les violacions de la seguretat de les dades personals al seu càrrec de les quals tingui coneixement, juntament amb tota la informació rellevant per documentar i comunicar la incidència, per correu electrònic a l'adreça indicada a la clàusula vuitena d'aquest acord d'encàrrec.

   Si se'n disposa, cal facilitar, com a mínim, la informació especificada en l'apartat b) del punt 1 i, addicionalment, el nom i les dades d'un punt de contacte en el qual es pugui obtenir més informació.

   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.

n) Implantar les mesures de seguretat escaients d'acord amb el nivell de risc determinat per a cada tractament objecte de l'encàrrec que es deriven de l'aplicació de l'Esquema Nacional de Seguretat (ENS) *(seria recomanable especificar les mesures de seguretat que s'apliquen descrites de manera concreta en un annex a aquest acord)*

   En tot cas, cal implantar mecanismes per:

   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. Seudonimitzar i xifrar les dades personals, si escau.

   També ha d'adoptar totes aquelles altres mesures que, tenint en compte el conjunt de tractaments que duu a terme, siguin necessàries per garantir un nivell de seguretat adequat al risc.

   La documentació relacionada amb la gestió dels riscos, incloent el resultat de les auditories periòdiques que es realitzin, pot ser sol·licitada en qualsevol moment pel responsable de tractament.

o) Designar un delegat de protecció de dades, si l'encarregat es troba inclòs en un dels supòsits previstos en l'article 37.1 del Reglament, i comunicar-ne la identitat i les dades de contacte al responsable.

p) Destinació de les dades

   Retornar al responsable de tractament les dades de caràcter personal i, si escau, els suports on constin, una vegada complerta la prestació.

   La devolució ha de comportar l'esborrat total de les dades existents en els equips informàtics utilitzats per l'encarregat i la supressió de totes les còpies existents.

No obstant això, l'encarregat pot conservar-ne una còpia, amb les dades degudament bloquejades, mentre es puguin derivar responsabilitats de l'execució de la prestació.

q) En el cas d'ús de servidors, comunicar el lloc on estaran ubicats i des d'on es prestaran el serveis associats a aquests, així com qualsevol canvi que es produeixi en relació amb aquesta informació.

r) Incorporar els tractaments que duu a terme en execució d'aquest contracte al seu registre d'activitats del tractament efectuades per compte d'un responsable, amb el contingut de l'article 30.2 de l'RGPD.

(*Aquesta obligació no és exigible a les empreses o organitzacions que ocupen menys de 250 persones llevat que concorri alguna de les circumstàncies següents:*

a) Si és probable que hi hagi un risc per a drets i llibertats dels subjectes.

b) Si el tractament no és ocasional

c) Si inclou categories especials de dades (art.9 RGPD) o infraccions i condemnes penals.

En aquests casos l'encarregat sí ha d'incloure al seu RAT aquests tractaments).

Cinquena.- Obligacions del responsable de tractament

Correspon al responsable de tractament:

a) Lliurar a l'encarregat les dades a les quals es refereix la clàusula segona d'aquest acord d'encàrrec.

b) Fer una avaluació de l'impacte sobre la protecció de dades personals de les operacions de tractament que ha d'efectuar l'encarregat, si fos preceptiu.

c) Fer les consultes prèvies que correspongui.

d) Vetllar, abans i durant tot el tractament, perquè l'encarregat compleixi la normativa en matèria de protecció de dades.

e) Supervisar el tractament, inclosa l'execució d'inspeccions i auditories.

Sisena.- Drets del responsable de tractament:

El responsable de tractament té dret a:

a) Obtenir de l'encarregat tota la informació que consideri necessària relativa a les dades i els tractaments que es descriuen a la clàusula segona, per tal que pugui complir amb les seves obligacions com a responsable.

b) Obtenir l'assistència de l'encarregat per atendre les peticions i inspeccions de qualsevol autoritat de control quan els tractaments objecte d'aquelles siguin els que porta a terme l'encarregat.

c) Ser compensat per l'encarregat pels danys i perjudicis que suporti com a conseqüència de l'incompliment de les obligacions de l'encarregat o dels seus subcontractats.

Setena.- Modificació de l'acord d'encàrrec

Aquest acord d'encàrrec de tractament de dades personals es podrà modificar de manera expressa i de comú acord entre les parts, mitjançant la signatura de l'addenda corresponent.

Vuitena.- Comunicacions i notificacions

a) Les comunicacions adreçades al responsable de tractament s'enviaran a:

(determinar per el responsable adreça postal i correu electrònic)

b) Les comunicacions adreçades a l'encarregat de tractament s'enviaran a:

(determinar per l'encarregat adreça postal i correu electrònic)

c) Les comunicacions en els casos de vulneracions de seguretat s'adreçaran, amb còpia al responsable funcional de què es tracti, a l'adreça electrònica següent:

(determinar per el responsable correu electrònic)

En prova de conformitat, ambdues parts signen aquest acord d'encàrrec.

(nom i cognoms)	**(nom i cognoms)**
Representant del responsable	Representant de l'encarregat

Annex 1. Identificació de la informació afectada

Annex 2. Descripció de les mesures de seguretat.

ANNEX 3 Model de compromís de confidencialitat

COMPROMÍS DE CONFIDENCIALITAT

L'execució de l'objecte del contracte *(referència al contracte – núm. d'expedient)* relatiu al servei *(identificar la finalitat del servei)* no implica el tractament de dades personals, per la qual cosa ni el seu personal ni, en el seu cas, les empreses subcontractades, poden accedir als arxius, documents i sistemes informàtics en què figurin dites dades. No obstant això, en cas de tractament incidental, o en cas que el personal de *(empresa contractista)*, que per a la realització del treball, requereixi tractar alguna dada del personal al servei de l'administració pública, quedarà subjecte al compliment de tot allò que estableix el Reglament (UE) 2016/679, del Parlament Europeu i del Consell, 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 i pel qual es deroga la Directiva 95/46/CE (d'ara endavant RGPD) i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (d'ara endavant LOPDGDD) i la normativa de desenvolupament.

No obstant això, quan el personal de *(empresa contractista)* i, en el seu cas, el de les empreses subcontractades accedeixi a dades personals, estarà obligat a guardar secret fins i tot després de la finalització de la relació contractual, sense que en cap cas pugui utilitzar les dades ni revelar-les a tercers.

El personal de *(empresa contractista)* i, en el seu cas el de les empreses subcontractades, tot i que no siguin encarregades del tractament, han de respectar les mesures de seguretat que hagi establert l'*(òrgan de contractació)*, responsable de tractament. En particular, ha de tenir en compte el següent:

- El personal propi i, en el seu cas, el de les empreses subcontractades ha de conèixer i complir la confidencialitat de la informació referent a la tasca realitzada i estarà obligat a mantenir absoluta reserva respecte a qualsevol dada o informació a què pugui accedir de forma extraordinària durant el compliment del contracte.
- No es podran emprar les dades i informacions derivades de l'execució del contracte per a finalitats diferents de les necessàries per al compliment d'aquest contracte, ni podran cedir-se a tercers, ni copiar-se o reproduir-se, excepte en la forma i condicions necessàries per a garantir la seguretat de les mateixes i la recuperació de la informació davant de fallides o accidents.
- En tot el procés d'execució de les tasques pròpies del contracte, *(empresa contractista)* i, en el seu cas, les empreses subcontractades han de complir estrictes normes de seguretat a fi d'assegurar en tot moment la confidencialitat, la integritat i la disponibilitat de la informació referent a les tasques executades.
- Igualment, caldrà garantir la seguretat i la confidencialitat de la informació continguda en la documentació dels registres i seguiments duts per *(empresa contractista)* respecte al procés d'execució.

L'*(empresa contractista)* ha de posar en coneixement dels treballadors afectats les mesures establertes a la clàusula anterior i conservar l'acreditació de la comunicació d'aquest deure.

Així mateix, *(empresa contractista)* ha de posar en coneixement del responsable de tractament, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de les dades personals afectades per aquest incident.

L'*(empresa contractista)* haurà de retornar tots aquells suports o materials que continguin dades personals a l'*(òrgan de contractació)* o destruir-los, immediatament després de la finalització de les tasques que n'han originat l'ús temporal, i en qualsevol cas, a la finalització del projecte o de la relació laboral.

L'incompliment del que s'estableix en els apartats anteriors pot donar lloc a què *(empresa contractista)* sigui considerada responsable de tractament, als efectes d'aplicar el règim sancionador i de responsabilitats previst a la normativa de protecció de dades.

I perquè consti ho signo
Signatura

Data.....

ANNEX 4 Model de certificat de destrucció/retorn de dades

CERTIFICAT D'ELIMINACIÓ DE DADES I SUPORTS A LA FINALITZACIÓ D'UN ENCÀRREC DE TRACTAMENT

En/Na ..... (nom i cognoms) ..... en qualitat de ..... (càrrec) ....., en representació de l'entitat ..... (nom de l'entitat) .....

CERTIFICO:

- Que en data ..... l'entitat va subscriure com encarregada de tractament un acord amb ..... (l'entitat responsable de tractament) ..... amb la finalitat de .....

- Que per executar les prestacions derivades del compliment de l'esmentat acord d'encàrrec el responsable de tractament va posar a disposició de l'entitat encarregada la informació corresponent als tractaments següents:

- Que en l'acord d'encàrrec de tractament subscrit consta que a la seva finalització les dades i, si escau, els suports on constin, serien eliminats al responsable de tractament.

- Que, atès que l'encàrrec de tractament ha finalitzat, el dia ....., s'ha procedit a l'eliminació de la informació i a la destrucció dels suports següents:

- Que les dades i els suports s'han eliminat amb garantia de confidencialitat mitjançant el mètode següent:

- Que no resta en poder de l'entitat encarregada cal altra informació i suports del responsable de tractament, amb excepció d'una còpia de la informació i suports que s'indiquen a continuació, que es conservaran degudament bloquejades mentre es puguin derivar responsabilitats de l'execució de la prestació.

I perquè consti ho signo

Signatura

Data .....

CERTIFICAT DE RETORN DE DADES I SUPORTS A LA FINALITZACIÓ D'UN ENCÀRREC DE TRACTAMENT

En/Na ..... (nom i cognoms) ..... en qualitat de ..... (càrrec) ....., en representació de l'entitat ..... (nom de l'entitat) .....

CERTIFICO:

- Que en data..... l'entitat va subscriure com encarregada de tractament un acord amb ..... (l'entitat responsable de tractament) ..... amb la finalitat de .....

- Que per executar les prestacions derivades del compliment de l'esmentat acord d'encàrrec el responsable de tractament va posar a disposició de l'entitat encarregada la informació corresponent als tractaments següents:

- Que en l'acord d'encàrrec de tractament subscrit consta que a la seva finalització les dades i, si escau, els suports on constin, serien retornats al responsable de tractament.

- Que, atès que l'encàrrec de tractament ha finalitzat, el dia ....., s'ha procedit al retorn de la informació i dels suports següents:

- Que no resta en poder de l'entitat encarregada cal altra informació i suports del responsable de tractament, amb excepció d'una còpia de la informació i suports que s'indiquen a continuació, que es conservaran degudament bloquejades mentre es puguin derivar responsabilitats de l'execució de la prestació.

I perquè consti ho signo

Signatura

Data .....