

PLEC DE CLÀUSULES TÈCNIQUES

Codi: **FS207_2023**

Concepte: Contractació mitjançant procediment obert no harmonitzat del servei de delegat de protecció de dades i servis connexos relacionats amb l'assessorament, consultoria i gestió en matèria de protecció de dades per a Figueres de Serveis, SA

CLÀUSULA 1.- OBJECTE DEL CONTRACTE

CLÀUSULA 2.- ABAST DEL SERVEI

CLÀUSULA 3. OBLIGACIONS DEL CONTRACTISTA I DESPLEGAMENT DEL SERVEI

CLÀUSULA 4. EQUIP DE TREBALL

Clàusula 1.- OBJECTE DEL CONTRACTE

L'objecte d'aquest contracte és la contractació mitjançant procediment obert no harmonitzat del servei de delegat de protecció de dades i servis connexos relacionats amb l'assessorament, consultoria i gestió en matèria de protecció de dades per a Figueres de Serveis, SA.

Clàusula 2.- ABAST DEL SERVEI

2.1. El servei objecte d'aquesta licitació comprèn dos aspectes:

- a) Servei de Delegat de Protecció de Dades.
- b) Servei d'assessorament, consultoria i gestió en matèria de protecció de dades de caràcter personal.

2.2. Tasques pròpies del servei de DPD

Pel que respecta a la designació del Delegat de Protecció de Dades (en endavant, DPD) i d'acord amb l'article 37 del RGPD i 34 de la LOPD, els responsables o encarregats del tractament hauran de designar un DPD sempre que el tractament el porti a terme una autoritat o organisme públic, les activitats principals de l'empresa consisteixin en operacions de tractament que, per raó de la seva naturalesa, abast i / o fins, requereixin una observació habitual i sistemàtica d'interessats a gran escala, les activitats principals de l'empresa consisteixin en el tractament a gran escala de categories especials de dades personals o de dades relatives a condemnes i infraccions penals, i es duguin a terme alguna de les activitats recollides en l'art. 34.1 de la LOPD.

Les funcions genèriques del DPD seran les previstes a l'article 39 del RGPD i als articles 36 i següents de la LOPD i en concret les que es relacionen a continuació:

- Informar i assessorar a Figueres de Serveis, SA del tractament de les dades, així com a tots els empleats que s'ocupin del tractament i de les obligacions, regulades en el RGPD i de la resta de la normativa aplicable en matèria de protecció de dades.
- Supervisar el compliment del RGPD i de la resta de la normativa aplicable en matèria de protecció de dades, i de les polítiques que dugui a terme Figueres de Serveis, SA en aquesta matèria, inclosa l'assignació de responsabilitats, la conscienciació i la formació del personal que participa en operacions de tractament, i les auditories corresponents.
- Oferir l'assessorament que es sol·liciti envers l'avaluació de l'impacte, relatiu a la protecció de dades i supervisar la seva aplicació, d'acord amb les prescripcions regulades a l'article 35 del propi RGPD.
- Cooperar amb les autoritats de control i, concretament, amb l'Autoritat Catalana de Protecció de Dades i l'Agència Estatal de Protecció de Dades.
- Actuar com a punt de contacte de l'autoritat de control per qüestions relatives al tractament, inclosa la consulta prèvia regulada a l'article 35 del RGPD, en cas que el tractament de les dades pogués comportar un alt risc o pogués infringir el propi RGPD.
- Compliment de principis relatius al tractament, com els de limitació de finalitat, minimització o exactitud de dades.
- Identificació de les bases jurídiques dels tractaments.
- Anàlisi de la situació en matèria de protecció de dades.
- Valoració de compatibilitat de les finalitats que van originar la recollida inicial de dades i adequació a la normativa si s'escau.

- Existència de normativa sectorial que pugui determinar condicions de tractament específiques diferents de les establertes per la normativa general de protecció de dades. Per exemple, normativa sobre transparència que afecta a les entitats que integren el sector públic.
- Disseny i implantació de mesures d'informació als afectats pels tractaments de dades.
- Establiment de mecanismes de recepció i gestió de les sol·licituds d'exercici de drets per part de les persones interessades.
- Valoració de les sol·licituds d'exercici de drets per part dels interessats.
- Disseny i implantació de polítiques de protecció de dades i actualització als canvis de normativa en protecció de dades.
- Auditoria de protecció de dades.
- Establiment i gestió dels registres d'activitats de tractament.
- Anàlisi de risc dels tractaments realitzats.
- Implantació de les mesures de protecció de dades.
- Implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments.
- Establiment de procediments de gestió de violacions de seguretat de les dades, inclosa l'avaluació del risc per als drets i llibertats dels afectats i els procediments de notificació a les autoritats de supervisió als afectats.
- Determinació de la necessitat de realització d'avaluacions d'impacte sobre la protecció de dades.
- Realització d'avaluacions, si és necessari.
- Programes de formació i sensibilització del personal en matèria de protecció de dades.
- La participació de forma adequada i en temps oportú, en totes les qüestions relatives a la protecció de dades de caràcter personal.
- Creació, modificació i eliminació de fitxers de dades personals.
- Redacció, revisió i adaptació dels formularis, sol·licituds d'interessats i documents emesos per l'ens de què es tracti.
- Revisió i adaptació de contractes, convenis i altres encàrrecs amb tercers que tenen incidència sobre les dades.
- Revisió del compliment de la normativa de transparència en matèria de protecció de dades.
- Registre de les activitats de tractament.
- Informe d'avaluació d'impacte i document descriptiu de les mesures de seguretat.
- Seguiment i manteniment de les mesures de compliment de la normativa durant l'exercici que correspongui.
- Assessorament continu a la corporació de què es tracti, designant una persona i un contacte de referència.
- Assistència online i telefònica.
- Elaborar els informes que legalment corresponguin en cas de qualsevol reclamació i/o incidència en matèria de protecció de dades.

El contractista té l'obligació de comunicar a Figueres de Serveis, SA qualsevol incidència que es produeixi en el servei.

2.3. Tasques relatives al servei d'assessorament, consultoria i gestió en matèria de protecció de dades de caràcter personal

L'adaptació i compliment del RGPDUE requereix la realització de tot un conjunt de tasques i actuacions per tal d'adequar l'activitat empresarial al nou precepte legal, així com garantir la funció proactiva que s'assenyala en el propi RGPDUE respecte a disposar de la documentació necessària que acrediti el seu compliment, tant en els serveis existents com en el desenvolupament i implantació de nous serveis.

També s'haurà de donar suport a les àrees i departaments de Figueres de Serveis, SA en les tasques de gestió relacionades amb els tractament de dades personals.

Les tasques que cal portar a terme són les següents:

- Mantenir actualitzat el Registre d'Activitats de Tractament.
- Identificar els contractes que impliquin tractament de dades de caràcter personal i garantir que el Contractes d'Encarregat de Tractament es signen i es compleixen.
- Elaborar la informació dels tràmits i procediments per tal d'atendre en temps i forma, els nous drets dels afectats, el dret d'accés, rectificació, supressió («dret a l'oblit»), oposició i limitació al seu tractament.
- Elaborar l'anàlisi de riscos per als drets i llibertats de la ciutadania de tots els tractaments de dades que es desenvolupin quan el nivell de risc ho aconselli i revisar les mesures de seguretat que s'apliquen als tractaments en base a aquest anàlisi.
- Elaborar i implementar el procediment d'avaluació d'impacte en la protecció de dades i supervisar-ne la seva realització i compliment.
- Assegurar l'existència, revisió i actualització de tota la documentació relacionada per tal de garantir el compliment del RGPDUE (document de seguretat, política de seguretat, manual de funcions i obligacions dels usuaris, nous procediments, ...).
- Supervisió de la gestió i notificació a l'autoritat de les violacions de seguretat de les dades personals a l'autoritat de control, elaborant un informe semestral sobre l'estat dels incidents i violacions de seguretat produïts.
- Formació en matèria de protecció de dades.
- Respondre les consultes que realitzin les diferents àrees de Figueres de Serveis, SA referents a la gestió i tractament de dades de caràcter personal. Realització anual d'auditories "internes" de compliment de la normativa de protecció de dades.
- Detecció de no conformitats, proposta de mesures correctives i supervisió de la seva aplicació.

Clàusula 3. Obligacions del contractista i desplegament del servei

1. Les empreses o els professionals contractistes hauran de realitzar com a mínim 10 hores de formació al personal de Figueres de Serveis, SA en matèria general de protecció de dades, així com aquella que tingui vinculació directa amb les seves àrees de treball.

Es mantindran un mínim de 3 reunions anuals formals presencials de coordinació amb la Unitat encarregada del seguiment i execució del servei (1 cada quadrimestre) per a realitzar el seguiment del servei conforme a les previsions establertes en els punts següents. S'aixecarà acta dels temes tractats en la reunió. La realització de l'acta anirà a càrrec de l'empresa contractista adjudicatària.

Com a punt de partida, el contractista haurà de realitzar un informe-avaluació sobre la situació en què es troba el servei, amb identificació de les mancances més rellevants i definició d'un programa d'actuació degudament agendat. Aquest estudi-programa caldrà tenir-lo enllestit en un termini de dos mesos a comptar de la data d'inici dels serveis.

De forma quadrimestral el contractista emetrà un informe detallant quantitativament i qualitativament els serveis prestats prenent com a punt de partida la situació existent a l'inici de la prestació, la qual cosa permetrà fer una avaluació efectiva del servei. Aquest informe es presentarà i analitzarà durant la reunió de coordinació.

Addicionalment, a petició de qualsevol de les parts, es podran organitzar reunions puntuals per a abordar assumptes d'interès que hagin de ser tractats abans de la següent reunió periòdica dins l'abast de l'objecte del contracte.

Totes les comunicacions, gestions i documentació es realitzaran per mitjans exclusivament electrònics amb l'ús d'eines telemàtiques i certificats digitals per part del contractista.

2. La disponibilitat del DPD (ja sigui físicament a les dependències de FISERSA ja sigui en línia o mitjançant altres mitjans segurs de comunicació) és fonamental per garantir que es pugui contactar amb ell.

En relació amb el suport a la seva labor (amb total autonomia en l'exercici de les seves funcions, que pugui relacionant-se amb el nivell superior de responsabilitat en la Protecció de Dades), és obligatori que el responsable del tractament faciliti al DPD tots els recursos necessaris per desenvolupar la seva activitat.

L'article 38, apartat 2, del RGPD preveu que l'organització recolzi al DPD "facilitant els recursos necessaris per a l'acompliment de les seves funcions i l'accés a les dades personals i a les operacions de tractament, i per al manteniment dels seus coneixements especialitzats".

En aquest sentit, el responsable del tractament s'ocuparà de donar:

- ☐ Suport actiu a la labor del DPD per part de l'alta direcció
- ☐ Concedir temps suficient per tal que el DPD compleixi amb les seves funcions.
- ☐ Suport adequat quant a recursos financers, infraestructura i personal, segons es requereixi.
- ☐ Comunicació oficial de la designació del DPD a tot el personal per garantir que la seva existència i funció es coneguin dins de l'organització.
- ☐ Accés necessari a altres serveis, com a recursos humans, TIC, seguretat, etc., de manera que el DPD pugui rebre suport essencial, aportacions i informació d'aquests serveis.
- ☐ Formació contínua del personal.

3.- Termini de resposta

L'adjudicatari haurà de donar resposta a les qüestions formulades a efectes d'assessorament en un termini màxim de 2 dies hàbils.

Per les actuacions d'avaluacions de risc, d'impacte, realització/supervisió del registre de tractaments i qualsevol altre que requereixin entrevistes o estudis previs, la seva durada es definirà a l'oferta tècnica.

4.- Registre de les activitats de tractament

Sense perjudici de les funcions i obligacions del DPD descrites abans, es concreta que en virtut de l'article 30, apartats 1 i 2, del RGPD és el responsable o l'encarregat del tractament, i no el DPD, qui està obligat a portar un Registre de les activitats de Tractament efectuades sota la seva responsabilitat, però el DPD en relació amb aquest Registre s'ocuparà de donar les instruccions oportunes i realitzar les actuacions corresponents per mantenir-ho actualitzat. Aquesta tasca es fonamentarà en la informació que li proporcionin les diferents Àrees i Unitats responsables del tractament de dades de FISERSA.

Aquest Registre ha de considerar-se una de les eines que permeten al DPD realitzar les seves funcions de supervisió de l'observança de les normes i d'informació i assessorament al responsable o a l'encarregat del tractament.

5.- Anàlisi del risc (AR) i Avaluació d'impacte de les operacions de tractament de dades personals (AIPD)

De conformitat amb l'article 35.1 i 39 del RGPD, és el responsable o l'encarregat del tractament, i no el DPD, qui està obligat a portar a terme una avaluació d'impacte de les operacions de tractament de dades personals, però el DPD en relació amb l'AR i l'AIPD s'ocuparà de:

-Portar a terme l'AR i d'assessorar al responsable del tractament sobre quina metodologia usar quan es realitzi una anàlisi de riscos relativa a la protecció de dades, quins àmbits han

de ser objecte d'una auditoria de protecció de dades interna o externa, quines activitats de formació internes proporcionar al personal o als encarregats de les activitats de protecció de dades i a quines operacions de tractament dedicar més temps i recursos

- Oferir el seu assessorament al Responsable del tractament o elaborar informe previ al tractament a iniciativa pròpia sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar la seva aplicació

- Determinar si s'ha de dur a terme o no una avaluació d'impacte relativa a la protecció de dades

- Determinar quina metodologia ha de seguir-se en dur a terme una avaluació d'impacte

- Proposar si ha de realitzar-se l'avaluació d'impacte en la pròpia organització o contractar-se externament.

- Determinar quines garanties (incloses mesures tècniques i organitzatives) han d'aplicar-se per mitigar qualsevol risc per als drets i interessos dels interessats.

Clàusula 4. Equip de treball

Per a la designació del DPD i de conformitat amb l'article 35 de la LOPD i en compliment dels requisits de l'article 37.5 del RGPD, les persones físiques que formin part de l'equip de treball hauran de tenir titulacions universitàries que acreditin coneixements especialitzats en Dret i la pràctica en matèria de Protecció de Dades, en concret:

- un consultor amb un perfil jurídic amb la certificació de Delegat de Protecció de Dades Certificat en l'esquema AEPD-DPD

- un consultor amb perfil tecnològic amb la certificació CISA (Certified Information Security Auditor), certificat atorgat per ISACA

L'equip de treball estarà format per com a mínim 2 consultors (un amb perfil jurídic i un altre amb perfil tecnològic, amb les certificacions referides). Els consultors realitzaran un mínim de 12 hores/trimestrals, incloent visites als centres de treball de FISERSA, per realitzar les seves tasques de supervisió de l'observança de les normes i d'informació i assessorament al responsable.

L'equip que prestarà el servei haurà d'estar degudament format i acreditar experiència en els diferents marcs normatius i estàndards sobre els quals es desenvolupa el projecte.

L'empresa adjudicatària haurà de dotar el seu personal de totes les eines necessàries amb la finalitat d'executar les tasques amb la major eficàcia.

Al personal de l'adjudicatària del contracte, que durant la prestació dels seus serveis tingui accés a fitxers que continguin dades de caràcter personal dels que sigui titular Figueres de Serveis, S.L., els serà d'aplicació allò que estableix la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, i el RGPD o normativa que els substitueixi.

Els serveis prestats s'ajustaran en tot moment a les exigències establertes per la normativa vigent aplicable.

El DPD exercirà les seves funcions prestant la deguda atenció als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i finalitats del tractament de dades.

Figueres, 13 de març de 2023

DILIGÈNCIA: Per a fer constar que aquest Plec de Clàusules Tècniques, que consta de 7 pàgines, ha estat aprovat pel Director gerent i el Conseller delegat de Figueres de Serveis, SA, de data 8 de març de 2023.

Dono fe,

La Secretaria del Consell d'Administració
de Figueres de Serveis, SA

El dia que signo,