SPAC
auditoria i consultoria

# AUDITORIA DE VERIFICACIÓ DE L'ACOMPLIMENT DE PROCEDIMENTS I INSTRUCCIONS EN MATERIA DE PROTECCIO DE DADES

FUNDACIO INTERNACIONAL JOSEP CARRERAS PER A LA LLUITA CONTRA LA LEUCÈMIA

**Barcelona, desembre 2015**

Hem procedit a l'actuació professional que resulta del present document a requeriment de la FUNDACIÓ INTERNACIONAL JOSEP CARRERAS PER A LA LLUITA CONTRA LA LEUCÈMIA.

Per l'encàrrec, es sol·licita un informe d'auditoria que verifiqui el compliment dels procediments i instruccions vigents en matèria de protecció de dades corresponents als fitxers als que cal aplicar un nivell alt de seguretat, segons l'article 96 del R. D. 1720/2007 de 11 de desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal i que es corresponen als fitxers REDMO i RECEPTORS.

D'acord a la darrera versió del document de seguretat, els fitxers amb dades de caràcter personal que disposa l'entitat són:

a) **R.E.D.M.O.**, de registre de donants de medul·la òssia, inscrit a l'Agencia de Protecció de Dades amb el codi Nº 1942245789.

b) **DONANTES**, de donants econòmics de la fundació, inscrit a l'Agencia de Protecció de Dades amb el codi Nº 1960190024.

c) **NOMINA**, de les dades del personal assalariat de la Fundació, inscrit a l'Agencia de Protecció de Dades amb el codi Nº 1942534821.

d) **FIJC**, de les dades dels clients i proveïdors de la fundació, inscrit a l'Agencia de Protecció de Dades amb el codi Nº 2023470076.

e) **RECEPTOR**, de les dades dels receptors de medul·la òssia de donant no emparentat, inscrit a l'Agencia de Protecció de Dades amb el codi Nº 2030270031.

f) **POSIBLES**, de les dades de les persones físiques i jurídiques que són potencials donants econòmics o de medul·la òssia, inscrit a l'Agència de Protecció de Dades amb el codi Nº 2060240260.

g) **FORUM**, de les dades de les persones inscrites en el fòrum de pacients i ex-pacients de la pàgina web de la Fundació Josep Carreras, inscrit a l'Agencia de Protecció de Dades amb el codi Nº 2101191373.

h) **NOMINA EXTERNO**, de les dades del personal assalariat de la Fundació que hi ha a Audi Consultores, inscrit a l'Agencia de Protecció de Dades amb el codi nº 2060240276.

i) **NEWSLETTER**, de les dades del personal de la Fundació Josep Carreras, Institut de Recerca contra la leucèmia Josep Carreras, i de persones que col·laboren estretament amb dos com son hospitals, facultats, Generalitat..., inscrit a l'Agencia de Protecció de Dades amb el codi nº 2141741633.

D'aquests fitxers, aquells als que cal aplicar mides de nivell alt de seguretat són els fitxers REDMO i DONANTES. Per a aquests fitxers caldrà efectuar una auditoria bianual que verifiqui el compliment de les Mides de Seguretat aplicables al fitxers i tractaments automatitzats

Realitzada l'actuació professional i vist:

1. Document de seguretat actualitzat a desembre 2015.

2. Documentació de la inscripció i modificació dels fitxers descrits en el document de seguretat.

3. Instal·lacions físiques de l'Entitat en relació a la protecció física de les dades de caràcter personal.

4. Equips i programes informàtics i arxiu de dades i suports.

5. Comunicats al personal sobre les mesures de seguretat que han d'acomplir d'acord a les normes implantades per l'Entitat.

6. Si existeix una relació actualitzada d'usuaris que tinguin accés autoritzat al sistema d'informació (Registre d'Usuaris) detallant l'accés autoritzat per a cadascun d'ells.

7. Si existeix un procediment d'identificació i autenticació per a l'accés al sistema d'informació. I si aquest procediment és a través de contrasenyes, si existeix un procediment d'assignació, distribució i emmagatzematge que garanteixi la seva confidencialitat i integritat.

8. Si els usuaris tenen accés autoritzat únicament a aquelles dades i recursos que necessiten per al desenvolupament de les seves tasques.

9. Si les contrasenyes es canvien amb la periodicitat que es determina en el document de seguretat.

10. Si el responsable del fitxer te establerts mecanismes per evitar que un usuari pugui accedir a dades o recursos amb drets diferents dels autoritzats.

11. Si els suports informàtics que contenen dades de caràcter personal permeten identificar el tipus d'informació que contenen, ser inventariats i s'emmagatzemen en un lloc amb accés restringit al personal autoritzat per això en el document de seguretat.

12. Si la sortida de suports informàtics que contenen dades de caràcter personal, fora dels locals en el que estan ubicats els fitxers, únicament està autoritzada pel responsable del fitxer.

13. Si els procediments establerts per a la realització de còpies de seguretat i per a la recuperació de dades garanteix la seva reconstrucció en l'estat en que es trobaven quan es va produir la pèrdua o destrucció.

14. Si es realitzen còpies de seguretat, al menys setmanalment.

15. Si en el Registre d'Incidències hi consta, el tipus d'incidència, moment en que s'ha produït, persona que realitza la notificació, a qui se li comunica, efectes derivats de la incidència, i addicionalment, en el cas del fitxer REDMO I RECEPTOR, si també hi consta els procediments realitzats de recuperació de les dades, persona que executa el procés, dades restaurades i dades gravades manualment en el procés de recuperació.

16. Si existeix autorització per escrit del responsable del fitxer REDMO I RECEPTOR per a l'execució dels procediments de recuperació de les dades.

17. Si el responsable del fitxer REDMO I RECEPTOR ha designat un responsable de seguretat encarregat de coordinar i controlar les mides definides en el document de seguretat. Designació del Responsable de seguretat.

18. Si existeix un mecanisme que permet la identificació de forma inequívoca i personalitzada de tot aquell usuari que intenta accedir al sistema de informació i la verificació de que està autoritzat per al fitxer REDMO I RECEPTOR.

19. Si per als fitxers REDMO I RECEPTOR existeix limitació d'intentar reiteradament l'accés no autoritzat al sistema d'informació.

20. Si exclusivament el personal autoritzat en el document de seguretat te accés als locals on es troben ubicats els sistemes d'informació que inclouen els fitxers REDMO I RECEPTOR.

21. Si el Registre d'entrada de suports informàtics dels fitxers REDMO I RECEPTOR permet conèixer el tipus de suport, la data i hora, l'emissor, el número de suports, el tipus d'informació que contenen, la forma d'enviament i si la persona responsable de la recepció està autoritzada per això.

22. Si el Registre de sortida de suports informàtics del fitxer REDMO I RECEPTOR permet conèixer el tipus de suport, la data i hora, el destinatari, el número de suports, el tipus d'informació que contenen, la forma d'enviament i si la persona responsable del lliurament està autoritzada per això.

23. Si existeixen mides per impedir qualsevol recuperació indeguda de la informació emmagatzemada dels fitxer REDMO I RECEPTOR en el suport informàtic quan aquest vagi a ser refusat o reutilitzat o be quan surt fora dels locals.

24. Si de cada accés al fitxer REDMO I RECEPTOR es guarda la identificació de l'usuari, la data i hora en que s'ha realitzat, el tipus d'accés i si ha estat autoritzat o denegat.

25. Si la informació guardada dels accessos autoritzats al fitxer REDMO I RECEPTOR permet identificar el registre accedit.

26. Si els mecanismes que permeten el registre de les dades detallades en els dos apartats anteriors es troben sota el control directe del responsable de seguretat i no es permet la seva desactivació.

27. Si les dades enregistrades a les que fa referència l'apartat anterior es guarden un període mínim de 2 anys.

28. Si el responsable de seguretat es revisa periòdicament la informació de control enregistrada del fitxer REDMO I RECEPTOR i elabora un informe de les revisions realitzades i els problemes detectats al menys un cop al mes.

29. Si del fitxer REDMO I RECEPTOR es conserva una còpia de seguretat i dels procediments de recuperació de les dades, en un lloc diferent en el que es troben els equips informàtics.

30. Si la transmissió de dades de caràcter personal del fitxer REDMO I RECEPTOR a traves de les xarxes de telecomunicacions es realitza xifrant aquestes dades.

31. Si les proves anteriors a la implantació o modificacions dels sistemes d'informació que tracten el fitxer REDMO I RECEPTOR no es realitzen amb dades reals, a no ser que s'asseguri el nivell de seguretat alt.

De la revisió realitzada es desprèn que les mides i controls de la Fundació Internacional Josep Carreras per a la Lluita contra la Leucèmia s'adeqüen al Reglament de mides de seguretat dels fitxers automatitzats que contenen dades de caràcter personal.

A la data d'aquest informe en la verificació del punts anteriors, no s'ha detectat anomalies significatives que requereixin les corresponents mesures correctores o complementaries necessàries.

A continuació exposem determinats aspectes a la Direcció per a la seva consideració, alguns d'ells representen un recordatori a títol informatiu d'aspectes mencionats en darreres revisions:

1. Descriure en el document de seguretat un resum de tots els contractes que l'Entitat ha subscrit amb tercers que fan referència a tractament de dades. Annexar al document de seguretat còpia d'aquests contractes.
   Completar la següent relació de contractes i característiques

| Contracte | Objecte |
|---|---|
| Mudanzas Casa Rojals | Contracte de guarda de documents |
| Estudis i Projectes Informàtics | Desenvolupament de noves aplicacions informàtiques |
| Ecologic | Destrucció documentació |
| Datem Groupe Spain, S.A | Serveis de Telemarketing |
| Wesser & Partner,S.L. | Captació de socis |
| ACDEM | Gestió devolució correo postal, comunicació a socis i interessats. |
| Axesor, conocer para decidir, SA | Normalització de la base de dades de donants econòmics |
| Institut Català d'Oncologia | Recerca de Donants |
| Hospital Sant Joan de Déu | Recerca de Donants |
| Hospital de la Santa Creu i sant Pau | Recerca de Donants |
| Hospital de la Vall d'Hebron | Recerca de Donants |
| Banco de Sangre y Tejidos de Cantabria. Centro de Referencia de Donantes | Recerca i gestió de Donants |
| Hospital San Pedro, Responsable del Centro de Referencia de Donantes designado por la Consejeria de Sanidad de la Comunidad Autónoma de La Rioja | Recerca i gestió de Donants |
| Banco Público de Sangre de Cordon Umbilical de Málaga | Banc de cordó umbilical |
| Banco de Sangre de Cordon Umbilical de la comunidad Valenciana | Banc de cordó umbilical |
| IVI Cordon SA – IVIDA | Banc de cordó umbilical |

2. Quan l'Entitat tracti dades de caràcter personal d'un fitxer sent el propietari de les dades un tercer, recomanem s'inclogui aquesta informació en el document de seguretat i s'apliquin les mides de seguretat adequades. Es aquest sentit, d'acord al conveni signat amb l'Hospital de San Joan de Déu l'1 de desembre de 2015, la Fundació Carreras hauria d'incloure dins el seu document de seguretat el tractament que efectua del fitxer Pacients per a la recerca i localització de donants propietat de l'esmentat Hospital.

3. Encriptar aquelles comunicacions que s'efectuïn amb tercers que així ho requereixin, tant sigui per la sensibilitat de les dades com per la seguretat de les comunicacions.

4. Actualment l'Entitat efectua una còpia de seguretat diària de les bústies de correu electrònic i documents i bases de dades, en el núvol de Microsoft (Azure i Office 365). Aquest model d'emmagatzematge fa que les dades emmagatzemades puguin estar ubicades a qualsevol lloc. Si les dades estan localitzades en països que no pertanyen a l'Espai Econòmic Europeu, es considera que hi ha una transferència internacional de dades. L'Agencia Española de Protección de datos, el 9 de maig de 2014 va emetre una resolució considerant adequades les garanties establertes en els models de contractes amb Microsoft quant a les transferències internacionals de dades.

   En tot cas, de cara a futures contractacions de serveis de cloud computing, recomanem a l'Entitat revisar les garanties de seguretat del proveïdor. Tanmateix, recomanem estar al corrent de les actualitzacions i canvis dels ja contractats.

5. Actualitzar la informació que l'entitat facilita "a tot el personal usuari de fitxers amb dades de caràcter personal" respecte les mides de seguretat per a protegir les dades. Comunicar al personal l'actualització i novetats per escrit, i guardar còpia signada pel treballador que acrediti la seva recepció. S'adjunta proposta d'actualització de carta (veure Annex 1), avaluar la incorporació de la següent recomanació al personal usuari de fitxers:

   a. Encriptar les comunicacions amb tercers quan les dades a transmetre són sensibles i/o les condicions ho requereixin.

6. Tenir clàusules de confidencialitat de tractament de dades amb els contractes formalitzats amb tercers (Models Annex 2).
   La realització del tractament de dades per tercers subcontractats, als que anomenarem encarregats del tractament, caldrà estar regulada per un contracte escrit o qualsevol altra forma que permeti acreditar la seva celebració i contingut que expressament indiqui les obligacions de l'encarregat del tractament

   Contingut del contracte:
   - Obligacions de l'encarregat
   - Serveis que seran objecte de subcontractació i dades de l'empresa subcontractada.
   - Prohibició d'accedir a les dades personals i l'obligació de secret respecte aquelles dades conegudes durant la prestació del servei.
   - Les dades només s'utilitzaran conforme les instruccions del responsable del fitxer.
   - Les dades no s'utilitzaran amb una finalitat diferent a l'establera en el contracte.
   - Les dades no es comunicaran, ni per a la seva conservació, a d'altres persones
   - Mides de seguretat a implementar
   - La destrucció o devolució de les dades un cop complert el contracte
   - En el cas de que l'encarregat del tractament destini les dades a altra finalitat, els comuniqui o els utilitzi incomplint les estipulacions del

contracte, respondrà de les infraccions en que hagués incorregut personalment.

7. Obtenir certificats periòdics per part de l'empresa encarregada de recollir el paper, en els que es deixi constància que es "destrueixen tots els documents", normalment es certifica que els papers han estat dipositats per a la seva destrucció. Com a mínim seria aconsellable disposar d'un certificat anual.

8. Fer alguna visita al magatzem logístic on es guarden els expedients clínics, amb la finalitat d'obtenir evidència que s'acompleixen les mides de seguretat per a la protecció de les dades.

9. Efectuar proves periòdiques de restaurar tota una còpia de seguretat, per a verificar la correcta restauració de tots els fitxers i dades. Aquesta prova s'hauria d'efectuar sempre que hi hagi canvis significatius en el sistema informàtic. Seria convenient efectuar la prova de restauració en un equip diferent del que s'han efectuat les còpies.

10. Respectar la normativa interna de l'Entitat de no comunicar ni deixar en lloc visibles les contrasenyes d'accés als ordinadors.

11. Quant a les mides de seguretat aplicables als fitxers i tractaments no automatitzats, caldrà aplicar les mateixes mides de seguretat que als fitxer automatitzats i d'acord amb el que estableixen els articles 106 i següents del R.D 1720/2007 de 11 de desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, s'hauran de seguir les següents mides:

    a. Els criteris d'arxiu hauran de garantir la correcta conservació dels documents, la localització i consulta de la informació i possibilitar l'exercici dels drets d'oposició al tractament, accés, rectificació i cancel·lació.

    b. Els dispositius d'emmagatzematge dels documents que continguin dades de caràcter personal hauran de disposar de mecanismes que obstaculitzin la seva obertura, o adoptar les mides necessàries que impedeixin l'accés de persones no autoritzades.

    c. Mentre la documentació amb dades de caràcter personal estigui en procés de revisió o tramitació i no es trobi arxivada en els dispositius d'emmagatzematge mencionats anteriorment, la persona al càrrec d'aquesta documentació haurà de custodiar-la i impedir que pugui ser accedida per persona no autoritzada.

12. Les mides de seguretat de **nivell alt** aplicables als fitxers i tractaments no automatitzats, addicionalment hauran de complir la següent normativa:

a. Els armaris, arxivadors o d'altres elements en els que s'emmagatzemin els fitxers no automatitzats amb dades de caràcter personal hauran d'estar en àrees en les que l'accés estigui protegit amb portes tancades en clau o dispositiu equivalent. Les àrees hauran d'estar tancades quan no sigui precís accedir als documents.

b. Utilitzar sistemes d'etiquetatge que permetin la identificació del contingut dels suports i documents a les persones autoritzades i dificultin la seva identificació a la resta.

c. La generació de còpies o la reproducció dels documents únicament podrà ser realitzada sota el control del personal autoritzat en el document de seguretat.

d. S'hauran de destruir les còpies o reproduccions que no serveixin de forma que s'eviti l'accés a la informació continguda en elles o la seva recuperació posterior.

e. L'accés a la documentació es limitarà exclusivament al personal autoritzat.

f. S'establiran mecanismes que permetin identificar els accessos realitzats en el cas de documents que puguin ser utilitzats per múltiples usuaris. L'accés per d'altres persones haurà de quedar adequadament enregistrat.

g. Sempre que es procedeixi al trasllat físic de la documentació continguda en un fitxer, s'hauran d'adoptar les mides dirigides a impedir l'accés o manipulació de la informació traslladada.

13. Quant als usuaris externs REDMO, caldria establir un protocol per garantir que aquests usuaris coneixen les mides de seguretat que han d'aplicar i es comprometen a aplicar-les. A títol orientatiu, es podria definir i aplicar el següent procés:

a. Quan és nou usuari:
   - que qui sol·licita i qui dóna tràmit per a nou usuari està autoritzat per aquest encàrrec. Guardar còpia de la sol·licitud i aprovació.
   - Crear l'usuari.
   - Impedir que l'usuari faci ús de les dades fins que no llegeixi i accepti les mides de seguretat (mateix model de carta que els usuaris personal de l'entitat). La lectura i acceptació de condicions podria aparèixer a la pantalla de l'ordinador quan l'usuari es connecti, impedir continuar fins que no es llegeix i accepta. Guardar còpia/registre de la lectura i acceptació per part de l'usuari.

b. Usuari ja existent
   - Fer aparèixer un missatge a l'ordinador quan es torni a connectar, donant un termini per a llegir i acceptar les mateixes condicions que

l'apartat anterior per nous usuaris. Si en el termini fixat (per exemple 1 mes) no ha llegit i acceptat les condicions, impedir que l'usuari accedeixi a les dades.

14. Quant a l'ús i a les dades penjades a les **xarxes socials**.

- Guardar la documentació necessària que justifiqui que es disposa d'autorització o consentiment per part del tercer per a publicar les seves fotos i/o altra informació. Si etiquetem a Internet una fotografia que pugui veure qualsevol sense permís de l'afectat, podríem incórrer en responsabilitat en matèria de protecció de dades personals. Podem ser responsables pels danys causats a la imatge, reputació o intimitat d'altres persones.

- En el cas de menors d'edat, per a recaptar, tractar i publicar les seves dades cal tenir en compte el que disposa el R.D.1720/2007, de 21 de desembre, pel que s'aprova el Reglament de desenvolupament de la llei orgànica de 15/1999, de 13 de desembre de protecció de dades

  *"Article 13. Consentiment per al tractament de dades de menors d'edat.*

  1. *Es pot procedir al tractament de les dades dels més grans de catorze anys amb el seu consentiment, excepte en els casos en què la Llei exigeixi per a la seva prestació l'assistència dels titulars de la pàtria potestat o tutela. En el cas dels menors de catorze anys es requereix el consentiment dels pares o tutors.*

  2. *En cap cas es poden sol·licitar dades del menor que permetin obtenir informació sobre els altres membres del grup familiar, o sobre les característiques del mateix grup, com ara les dades relatives a l'activitat professional dels progenitors, informació econòmica, dades sociològiques o qualssevol altres, sense el consentiment dels titulars d'aquestes dades. No obstant això, es poden sol·licitar les dades d'identitat i adreça del pare, mare o tutor amb l'única finalitat d'obtenir l'autorització que preveu l'apartat anterior.*

  3. *Quan el tractament es refereixi a dades de menors d'edat, la informació que s'hi adreci s'ha d'expressar en un llenguatge que els sigui fàcilment comprensible, amb la indicació expressa del que disposa aquest article.*

  4. *Correspon al responsable del fitxer o tractament articular els procediments que garanteixin que s'ha comprovat de manera efectiva l'edat del menor i l'autenticitat del consentiment prestat, si s'escau, pels pares, tutors o representants legals."*

  En tot cas, aconsellem obtenir el consentiment del pares per als menors d'edat i addicionalment el consentiment del menor quan aquest te una

edat compresa entre els 14 i 18 anys. Caldrà guardar còpia d'aquesta documentació.

- Un cop es penja una informació a Internet, esborrar-la del tot es converteix en una tasca pràcticament impossible. Per tant, caldrà tenir especial cura en la informació que es publica.

- En cadascuna de les xarxes socials en les que es participi, caldria revisar acuradament les condicions d'us i polítiques de privacitat.

Caldrà tenir en compte la informació i les recomanacions que publica l'Agencia Española de Protección de Datos al respecte.
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf

15. En el cas d'ús de cookies (per exemple en http://www.fcarreras.org), informar a l'usuari de la política d'ús i seguir les recomanacions de l'Agencia Española de Protección de Datos *"Guía sobre el uso de las cookies"* *http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf*

    A títol d'exemple, la guia editada per l'Agencia Española de Protección de Datos, manifesta:

    > *"El apartado segundo del artículo 22 de la LSSI establece que se debe facilitar a los usuarios información clara y completa sobre la utilización de los dispositivos de almacenamiento y recuperación de datos y, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.*
    >
    > *Por consiguiente, la información sobre las cookies facilitada en el momento de solicitar el consentimiento debe ser suficientemente completa para permitir a los usuarios entender la finalidad para las que se instalaron y conocer los usos que se les darán.*
    >
    > *En el caso de que un usuario preste su consentimiento para el uso de cookies, la información sobre cómo revocar el consentimiento y eliminar las cookies deberá de estar a su disposición de forma accesible y permanente.*
    >
    > *Además de facilitar la información necesaria para que los usuarios puedan prestar, en el momento requerido, un consentimiento valido, es aconsejable que la citada información, y en particular la relativa a la forma a través de la cual pueden gestionar las cookies, esté a su disposición de forma accesible y permanente en todo momento a través la página web desde la que se presta el servicio."*

*"EJEMPLO:*
*Utilizamos cookies propias y de terceros para mejorar nuestros servicios y mostrarle publicidad relacionada con sus preferencias mediante el análisis de sus hábitos de navegación. Si continua navegando, consideramos que acepta su uso. Puede cambiar la configuración u obtener más información aquí."*

16. L'Agencia Española de Protección de Datos, va publicant diferents guies i recomanacions d'acord a les innovacions i novetats que van apareixent respecte les dades de caràcter personal i les eines informàtiques. Recomanem consultar aquestes guies i anar implementant les recomanacions suggerides.

    Algunes de les guies d'interès publicades actualment són:

    - *Guía sobre el uso de las cookies*
    - *Guía para clientes que contraten servicios de Cloud Computing*
    - *Orientaciones para prestadores de servicios de Cloud Computing*
    - *El derecho fundamental a la protección de datos: guía para el ciudadano – 2011*
    - *Guía de Seguridad de Datos – 2010*
    - *Guía sobre seguridad y privacidad de las tecnologías RFID – 2010*
    - *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online – 2009*
    - *Guía de Videovigilancia – 2009*
    - *Recomendaciones a usuarios de Internet. 2009*
    - *Resoluciones y Documentos, que inclou Documents-Recomanacions de Grups de Treball del parlament europeu.*

17. Per la recollida de dades en la web, la Agencia Española de Protección de datos publica dins l'apartat de Documentos de Grupos de Trabajo, Grupo Europeo art 29 la "Recomendación 2/2001 sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea".
    http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/2001/common/pdfs/Recomendaci-oo-n-2-2001-sobre-determinados-requisitos-m-ii-nimos-para-la-recogida-en-l-ii-nea-de-datos-per.pdf

    Transcrivim part de les recomanacions:

    ***"Recomendaciones sobre la información que deberá facilitarse al recoger datos personales en el territorio de los Estados miembros de la Unión Europea***

    *4. Toda recogida de datos personales de un interesado a través de un sitio web implica facilitar previamente determinada información. Respecto al contenido, para cumplir esta obligación es necesario:*

*5. Declarar la identidad y las direcciones postal y electrónica del responsable del tratamiento y, cuando sea aplicable, la del representante designado en virtud del apartado 2 del artículo 4 de la Directiva*

*6.* ***Indicar claramente para qué fines de tratamiento*** *recoge los datos el responsable a través de un sitio. Por ejemplo, cuando los datos se recogen tanto para firmar un contrato (suscripción a Internet, pedido de un producto, etc.) como para márketing directo, el responsable del tratamiento debe indicar claramente ambos fines.*

*7.* ***Informar claramente sobre si la información solicitada es obligatoria u opcional.*** *La información obligatoria es aquella necesaria para prestar el servicio solicitado. La naturaleza obligatoria u opcional se podría indicar, por ejemplo, mediante un asterisco junto a los datos obligatorios o bien añadiendo la palabra «opcional» junto a la información no obligatoria. El hecho de que el interesado no facilite la información opcional no se utilizará en su contra de ninguna manera.*

*8.* ***Mencionar la existencia de los derechos de consentimiento u oposición****, según el caso, respecto al tratamiento de datos personales, y de las condiciones para ejercer tales derechos así como los derechos de acceso, rectificación y eliminación de datos. Deberá facilitarse información, en primer lugar, sobre la persona o el servicio al que acudir para ejercer estos derechos y, en segundo lugar, sobre la posibilidad de ejercerlos tanto en línea como en la dirección postal del responsable del tratamiento.*

*9. Enumerar los* ***destinatarios*** *o las categorías de destinatarios para la* ***información recopilada****. Al recoger cualquier tipo de datos, los sitios deberán indicar si los comunicarán o pondrán a disposición de terceros, en particular socios empresariales, filiales, etc., y por qué motivo (fines distintos de prestar el servicio solicitado y de márketing directo).*

*Si se da este caso, los usuarios de Internet tendrán la posibilidad real de oponerse a ello en línea marcando una casilla relativa a la comunicación de datos para fines distintos de la prestación del servicio solicitado. Puesto que el derecho de oposición se puede ejercer en cualquier momento, la posibilidad de ejercerlo en línea también debería indicarse en la información facilitada al interesado. El Grupo de trabajo, consciente del inconveniente que supone sobrecargar de información las pantallas, es de la opinión de que* ***no mencionar los destinatarios equivale a que el responsable de los datos se compromete a no comunicar ni transmitir la información*** *recogida a terceras partes cuya denominación y dirección no haya facilitado, a menos que la identidad de dicha tercera parte sea obvia y la comunicación de los datos sea estrictamente necesaria para prestar el servicio solicitado por el usuario de Internet y siempre que la comunicación se realice exclusivamente para ese fin. Si se prevé que el responsable de los datos transfiera dichos datos a países no miembros de la Unión Europea, indicar si estos países ofrecen una adecuada protección de los interesados en cuanto al tratamiento de sus*

*datos personales en el sentido que recoge el artículo 25 de la Directiva 95/46/CE. En este caso, se deberá facilitar información específica sobre la identidad y la dirección de los destinatarios (dirección postal y/o electrónica).*

*11. Proporcionar el nombre y la dirección (postal y electrónica) del servicio o la persona* ***responsable de responder*** *a las preguntas relacionadas con la protección de los datos personales.*

*12.* ***Mencionar con claridad la existencia de procedimientos automáticos de recogida de datos, antes de usar dichos métodos****. Cuando se utilicen tales procedimientos, el interesado deberá recibir la información indicada en este documento. Además, se le deberá informar del nombre de dominio del servidor de sitios que transmite los procedimientos automáticos de recogida, la finalidad de dichos procedimientos, su plazo de validez, si es necesaria o no la aceptación de dichos procedimientos para visitar el sitio y la opción de que dispone todo usuario de Internet de oponerse a su uso, además de las consecuencias de desactivar dichos procedimientos. En caso de que otros responsables del tratamiento de los datos participen en la recogida de datos personales, el interesado deberá recibir información sobre la identidad de los responsables del tratamiento y la finalidad del tratamiento en relación con cada controlador.*

*La información y la posibilidad de oponerse a la recogida deberán comunicarse antes de utilizar cualquier procedimiento automático que desencadene la conexión del ordenador del usuario con otro sitio web, por ejemplo, cuando un sitio web conecta automáticamente al usuario a otro sitio para mostrarle publicidad en forma de pancarta publicitaria, con el fin de evitar que este segundo sitio recopile datos sin que el usuario sea consciente de ello.*

*Por ejemplo,* ***si el servidor de un responsable del tratamiento coloca una cookie, la información deberá facilitarse antes de que ésta se envíe al disco duro del usuario de Internet****, además de la información facilitada por la tecnología actual, que se limita a dar el nombre del sitio transmisor y el periodo de validez de la cookie.*

*13.* ***Destacar las medidas de seguridad*** *que garantizan la autenticidad del sitio, la integridad y la confidencialidad de la información transmitida a través de la red y que se hayan tomado en aplicación de la legislación nacional en vigor.*

*14.* ***La información se proporcionará en todos los idiomas*** *utilizados en el sitio y, en particular, en los lugares donde vayan a recogerse datos personales.*

*15. Los responsables del tratamiento deberán verificar la coherencia de la información proporcionada en los diversos «documentos» que comprometen al sitio (encabezado «datos personales y protección de la intimidad», formularios electrónicos, texto relativo a las condiciones generales de venta y otras comunicaciones comerciales).*

*16. El Grupo de trabajo considera que la **información s**iguiente debe mostrarse directamente en la pantalla **antes de la recogida** para garantizar el tratamiento leal de los datos:*

- *la identidad del responsable del tratamiento*
- *la finalidad*
- *el carácter obligatorio o no de la información solicitada*
- *los destinatarios o las categorías de destinatarios de los datos recogidos*
- *la existencia de los derechos de acceso y rectificación*
- *la existencia del derecho de oposición a que los datos se comuniquen a terceros para fines distintos de la prestación del servicio solicitado y la manera de ejercerlo (por ejemplo, mediante una casilla que el usuario pueda marcar)*
- *la información que se deberá proporcionar al utilizar procedimientos automáticos de recogida*
- *el nivel de seguridad durante todas las fases del tratamiento incluida la transmisión, por ejemplo, entre redes. En estos casos, la información deberá proporcionarse de manera interactiva y en pantalla. Así, en el caso de los métodos automáticos de recogida de datos, si es necesario esta información podría facilitarse mediante la técnica de una ventana «emergente».*

*En lo que respecta al nivel de seguridad durante la transmisión de los datos desde el equipo del usuario hasta el sitio web, se podría emplear un encabezado del tipo: «Está iniciando una sesión segura» o los procedimientos de información automática de que disponen los navegadores, como la aparición de iconos específicos en forma de llave o de candado.*

*17. Además, el Grupo de trabajo considera que en la página inicial del sitio y en todos los lugares donde se recojan datos personales en línea deberá poderse acceder directamente a información completa sobre la política de protección de la intimidad (incluida la forma de ejercer el derecho de acceso). El título del encabezado que deba seleccionarse con el ratón deberá estar resaltado, ser explícito y específico, de manera que transmita al usuario de Internet una idea clara del contenido que se le va a mostrar. Por ejemplo, el encabezado podría indicar **«Esta página recoge y trata datos personales relacionados con usted. Si desea más información, pinche aquí» o bien «Protección de datos personales o de la intimidad».** También deberá ser lo bastante específico el contenido de la información a la que se dirige el usuario de Internet."*

18. Comunicacions comercials realitzades a través de correu electrònic.
    No efectuar cap enviament de comunicacions publicitària o promocional que prèviament no hagi estat sol·licitada o expressament autoritzada pel destinatari.
    Quan es faci, s'haurà d'oferir al destinatari una adreça de correu electrònic on poder exercir el dret d'oposició al tractament de les seves dades amb finalitats promocionals.

(art 21 Llei 34/2002 de 11 juliol de serveis de la societat de la informació i comerç electrònic)

El present document ha estat preparat a la seva sol·licitud, en relació a l'article 96 del R.D 1720/2007 de 11 de desembre, pel que s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, per tant no pot ser utilitzat per a cap altra finalitat.

**SERVEIS PROFESSIONALS D'AUDITORIA I CONSULTORIA, SLP**

Yolanda Soto Blasco
Barcelona, 30 de desembre de 2015

**Annex 1**

**Proposta d'actualització de carta per als usuaris de fitxers amb dades de caràcter personal**

**A tot el personal usuari de fitxers amb dades de caràcter personal.**

La Llei Orgànica 15/1999, de 13 de desembre, de Protecció de les Dades de Caràcter Personal (LOPD) estableix l'obligació de disposar d'unes mides d'índole tècnica i organitzativa necessàries que garanteixin la seguretat dels fitxers amb dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat.

L'Entitat ha elaborat un nou document de seguretat que està a la seva disposició, que detalla les mides d'índole tècnica i organitzatives, que han de reunir els fitxers, els centres de tractament, locals, equips, sistemes, programes i les persones que intervinguin en el tractament de les dades de caràcter personal subjectes al règim de la LOPD, es a dir, dades de caràcter personal enregistrades en suport físic que les faci susceptibles de tractament. Les mides establertes garanteixen la seguretat de les dades de caràcter personal i tracten d'evitar la seva alteració, pèrdua, tractament o accés no autoritzat. S'entén com a fitxer, tot conjunt organitzat de dades de caràcter personal, sigui quina sigui la forma o modalitat de la seva creació, emmagatzematge, organització i accés.

La Llei entén per dades de caràcter personal a qualsevol tipus d'informació, susceptible de recollida, tractament o transmissió referent a persones físiques identificades o identificables. Les dades que a la nostra entitat li afecten són les relatives als fitxers REDMO, Donantes, Nómina, FIJC (clients i proveïdors), Receptor, Posibles i Forum.
En particular, els usuaris d'aquests fitxers i dades han de seguir les següents recomanacions:

- Mantenir la confidencialitat del seu accés als fitxers (informàtics o no), evitant deixar una porta oberta a un accés no permès (despatxos i armaris tancats amb clau, contrasenya personal d'accés informàtic actualitzada periòdicament, evitar deixar l'ordinador i l'aplicació oberts en moments de risc d'utilització no autoritzada, evitar deixar documents a l'abast de tercers no autoritzats, etc.).

- En els llocs d'atenció al públic on hi hagi ordinadors i terminals, s'haurà de tenir especial cura en que les dades de caràcter personal no siguin fàcilment visibles pel públic. Així doncs, les pantalles d'entrades de dades no hauran de ser accessibles al públic i caldrà apagar l'ordinador en aquells moments en que no estigui atès per ningú. Com a mida de seguretat s'haurà d'activar un protector de pantalla per als casos d'absències no prolongades.

- D'acord amb el procediment establert per la societat amb les incidències, comunicar a la direcció en un termini màxim de 24 hores qualsevol incidència, accés al fitxer per tercers no autoritzats, o anomalia que pugui afectar a la seguretat dels fitxers i les seves dades.

- Conèixer les mides de seguretat dels fitxers dels que són usuaris

- Totes les persones hauran de guardar secret i confidencialitat sobre les dades personals que coneguin en el desenvolupament del seu treball. Aquest compromís de confidencialitat i secret professional serà vigent inclús després de finalitzar la relació laboral. L'inadequat compliment del secret i seguretat posa en risc el dret fonamental a la protecció de dades i causa habitualment un greu perjudici a l'entitat.

- S'haurà de guardar secret sobre les dades contingudes en els fitxers, tot seguint una màxima confidencialitat amb aquells fitxers que contenen dades a les que la llei obliga a aplicar unes mides de seguretat de nivell alt.

- Mantenir la confidencialitat en els processos de còpies i recuperació de dades i únicament realitzar aquelles que prèviament han estat autoritzades.

- Només es permetrà la sortida de fitxers fora dels locals si existeix autorització de la direcció, qui s'assegurarà del bon ús de les dades que comporti la sortida.

- No oblidar llistats i d'altres documents a la fotocopiadora i impressora.

- No deixar documents amb dades confidencials a les papereres

- Destruir aquells documents que així ho requereixin perquè ja no tinguin cap utilitat i continguin dades de caràcter personal crítiques.

- Guardar en lloc segur, per exemple armaris de seguretat, els documents que continguin dades de caràcter personal.

- No descarregar ni instal·lar programes en els ordinadors sense autorització del responsable de seguretat.

- Degut a que en els serveis prestats per la Fundació és fonamental la resposta immediata als usuaris utilitzant la xarxa informàtica, seria aconsellable no posar obstacles al bon rendiment informàtic. En aquest sentit, caldria intentar limitar l'accés a aquelles pàgines que no sent necessàries per al desenvolupament de la tasca laboral utilitzen molts recursos informàtics.

- Aplicar i recordar les mides de seguretat i ús informàtic. A títol d'exemple:

  * Les dades únicament s'han de tractar conforme les instruccions de la Fundació Carreras.
  * Les dades no s'utilitzaran amb finalitats diferents a les establertes en els contractes.
  * Les dades no es comunicaran, ni per a la seva conservació, a d'altres persones.
  * No instal·lar cap software sense el coneixement i consentiment dels responsables de seguretat informàtica.
  * Mantenir actualitzats els antivirus.
  * No proporcionar l'identificador de l'usuari a tercers ni claus d'accés.
  * Ser conscient que quan s'envien missatges de correu a una varietat de destinataris, s'estan revelant totes les adreces d'aquests destinataris, a no ser que s'enviïn a traves del camp *"Con Copia Oculta (CCO)"*
  * Procurar no utilitzar per a usos personals la direcció de correu electrònic que se li ha estat proporcionada per a us laboral.
  * No desatendre l'ordinador mentre s'està connectat o s'està realitzant una connexió segura en la que s'estiguin proporcionant dades.
  * Limitar l'ús de la xarxa informàtica. Minimitzar l'ús o consultes a pàgines d'internet per a usos particulars que fan alentir els processos i consultes laborals. Minimitzar l'emmagatzematge d'arxius voluminosos particulars als equips informàtics de la Fundació.
  * No desactivar els antivirus ni tallafocs.

- En el cas concret dels fitxers REDMO i RECEPTOR, els usuaris signaran una autorització per a que els companys del REDMO puguin accedir a la seva bústia de correu quan això sigui estrictament necessari per al bon funcionament de les recerques de REDMO.

Les obligacions dels usuaris es basaran en accedir únicament a aquelles dades i recursos que necessitin per al desenvolupament de les seves funcions i en la protecció d'aquestes dades, evitant accessos no autoritzats.

El personal que realitzi treballs que no impliquin el tractament de dades personals tindrà limitat l'accés a aquestes dades, als suports que les continguin, o als recursos del sistema d'informació.

Els usuaris han de conèixer que la societat podrà ser sancionada per l'incompliment de les mesures de seguretat descrites en la LOPD. La quantia de les sancions es graduarà atenent la naturalesa dels drets personals afectats, al volum dels tractaments efectuats, als beneficis obtinguts, al grau d'intencionalitat i a la reincidència.

Un cop llegida aquesta circular, els hi sol·licitem signar la llista de distribució que tenen a la seva disposició a Direcció per a deixar constància de la seva recepció i conformitat al seguiment de les recomanacions esmentades anteriorment que afecten a cadascun com a usuari.

Atentament,
Antoni Garcia i Prat

Annex 2

**Models de contractes o clàusules de confidencialitat en el cas de tractament de dades per tercers subcontractats**

**Model 1:**

MODEL DE CONTRACTE DE CONFIDENCIALITAT I APLICACIÓ DE LES MIDES DE SEGURETAT DE LA LOPD

Barcelona, __ de ___ de 201x

R E U N I T S

En_____, en representació de la Fundació_____, amb domicili a _____, nº ____, 08___ (Barcelona) i En ..... en representació de ....., amb domicili a C/ ....., convenen expressament en formalitzar el present contracte que tindrà per objecte la salvaguarda de la informació que ..... pugui rebre com a conseqüència dels diferents serveis prestats, i que comporten el tractament automatitzat de fitxers de dades de caràcter personals, obligant-se ..... a la necessària aplicació de la LOPD i normativa vigent respecte els fitxers propietat de la Fundació _____ amb subjecció al següents,

P A C T E S

.....es compromet a tractar les dades personals titularitat de la Fundació _____ per a l'estricta prestació dels serveis professionals encarregats, i a no aplicar o utilitzar les dades personals que provinguin dels fitxer automatitzats de la Fundació _____ amb diferent finalitat que per la prestació dels serveis encarregats, i a no comunicar-les ni cedir-les, ni per la seva conservació, a d'altres persones ni entitats.

Les dades personals que provinguin dels fitxers titularitat de la Fundació _____ subjectes a aquest contracte, quedaran durant tot el procés de l'operació en poder de ..... , qui a partir d'aquest moment serà responsable d'aquestes dades.

.....manifesta disposar d'un document de seguretat en el que es detallen les mesures d'índole tècnica i organitzatives, que han de reunir els fitxers, els centres de tractament, els equips, els sistemes, els programes i les persones que intervenen en el tractament de les dades de caràcter personal subjectes al règim de la LOPD, en particular les dades de caràcter personal enregistrades en suport informàtic o físic que les faci susceptibles de tractament titularitat de la Fundació _____. Les mesures establertes garanteixen la seguretat de les dades de caràcter personal i tracten d'evitar la seva alteració, pèrdua, tractament o accés no autoritzat tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a que estan exposades, ja provinguin de l'acció humana o del medi físic o natural.

..... i aquells que intervinguin en qualsevol fase del tractament de les dades de caràcter personal propietat de la Fundació _____, es comprometen a mantenir el secret professional i al deure de guardar-les

Un cop finalitzada la prestació contractual, les dades de caràcter personal hauran de ser retornades a la Fundació _____ a l'igual que qualsevol suport o documents en que consti alguna dada de caràcter personal objecte del tractament.

En el cas que ..... destini les dades a altra finalitat, les comuniqui o les utilitzi incomplint les estipulacions del contracte serà considerat, també, responsable del tractament, responent de les infraccions en que hagués incorregut personalment .

I, per a que consti firmen les parts el present document per duplicat i a un sol efecte en el lloc i data que al principi s'indiquen.

Per .....  Per Fundació _____

En  En

**Model 2**

Apartat x. Protecció de dades de caràcter personal

En relació amb el règim de protecció de dades de caràcter personal, s'entén que les dades facilitades per la Fundació Josep Carreras i pels interessats (Responsables dels Fitxers), com a conseqüència del procés de desenvolupament de les tasques que constitueixen l'objecte del present Conveni, seran incorporades en els fitxers _____ propietat de la Societat [---x---], mitjançant el qual la Societat [---x---] es reconeix com a Encarregat de tractament de les dades de la Fundació Josep Carreras i garantint que es mantenen i apliquen totes les mesures de seguretat i confidencialitat que la Llei i el Reglament en vigor exigeixen. Corresponen, per tant, a una i altra entitat, els drets i obligacions que en aquesta condició els atribueix la vigent Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, que per part de la Societat [---x---] es manifesta i declara complir en la seva totalitat, mitjançant aquesta declaració.

En aquest sentit, la Societat [---X---] manifesta que:

1. No utilitzarà les dades de caràcter personal a què accedeixi per una altra finalitat que la que constitueix l'objecte d'aquest contracte.
2. No comunicarà les dades a tercers, excepte en els casos legalment previstos i amb el consentiment del Responsable del Fitxer.
3. No subcontractarà els serveis a tercers, sense el previ consentiment del Responsable del Fitxer
4. Comunicarà al Responsable del Fitxer els casos de sol·licitud dels drets d'accés, rectificació, cancel·lació i oposició que li sol·liciti un titular de dades.
5. La Societat [---X---] disposa de mesures tècniques i organitzatives de seguretat de les dades, tant automatitzades com no automatitzades, per tal d'evitar-ne la seva pèrdua, alteració i/o accés no autoritzat, definides en el seu Document de Seguretat.
6. Tot el personal de la Societat [---X---] manté un acord de confidencialitat signat i assumit en relació amb el deure de secret sobre les dades personals a què puguin accedir, a través de qualsevol mitjà. Incloent-ne fins i tot després de finalitzar la relació contractual entre les parts.
7. Per les empreses subcontractades, que poguessin intervenir, la Societat [---x---] estableix igualment Contractes de confidencialitat i compromís signats.

8. La Societat [---x---] es compromet a tornar, destruir o gestionar les dades de caràcter personal segons indiqui el Responsable dels Fitxers, un cop acabada la relació contractual del servei de referència. Sols en cas de previsió legal exigible, en conservarà una còpia degudament bloquejada i custodiada.
9. La Societat [---x---] es reconeix responsable de la correcta custòdia i confidencialitat de les dades de caràcter personal a què hagi tingut accés el seu personal o persones en el seu nom.
10. Els potencials litigis que es poguessin produir com a conseqüència d'aquesta relació, es regiran per la legislació espanyola (Llei 15/1999 i Reial decret 1720/2007 de 21 de desembre) i es dirimiran als tribunals de Barcelona.

**Model 3**

Protección de datos

En relación con la prestación de servicios objeto de esta carta de encargo, les informamos que la sociedad [---x---] tratará los datos de carácter personal a los que pudiera acceder durante la misma de conformidad con lo dispuesto en el artículo 12 de la LOPD: que únicamente tratará los datos con arreglo a las instrucciones de la Fundació Josep Carreras; que no los aplicará o utilizará con una finalidad diferente a la prevista en los servicios pactados ni los comunicará a otras personas, a excepción de lo dispuesto en el párrafo siguiente, y que implantará y mantendrá en los ficheros que contengan datos de carácter personal, propiedad de la Fundació a los que tenga acceso, las medidas de índole técnica y organizativa oportunas para alcanzar el nivel de seguridad exigible conforme a lo establecido en el artículo 9 de la LOPD i en el Real Decreto 1720/2007, de 21 de diciembre, y en cualquier otra norma que lo complemente, modifique o derogue en el futuro.

Por la presente, la Fundació autoriza expresamente a la sociedad [---x---] para que subcontrate en su nombre con terceros la custodia de las copias de seguridad de los datos y el mantenimiento de los servidores donde se mantiene la información, los cuales están sujetos a cumplir les mismas medidas de seguridad mencionadas en el párrafo anterior.

Una vez finalizados los servicios pactados, la sociedad [---x---] procederá a destruir o devolver los datos personales obtenidos durante la ejecución de los servicios, con independencia del soporte o documento en que éstos consten, sin perjuicio de lo dispuesto en el artículo 10 de la LOPD. No obstante, la sociedad [---x---] queda autorizada a conservar aquellos datos estrictamente necesarios para poder justificar la prestación de servicios profesionales para el caso de que la misma fuera cuestionada y por el tiempo legalmente establecido para la prescripción.

**Model 4**

**CONTRATO PARA EL TRATAMIENTO DE DATOS PERSONALES POR CUENTA DE TERCERO**

En ....., a ..... de ..... de.....

**REUNIDOS**

De una parte, D. ..... con DNI núm. ..... y domicilio a estos efectos en ..... calle ..... núm. .....,

De otra parte, D. ....., con DNI núm. ..... y domicilio en ....., calle ..... núm. .....,

**INTERVIENEN**

El primero, en nombre y representación de XXXX (en adelante, X), constituida en fecha ..... ante el Notario de ..... D. ....., e inscrita bajo el núm. ..... de su protocolo.

El segundo, en nombre y representación de YYYY (en adelante, Y), constituida en fecha ..... ante el Notario de ..... D. ....., e inscrita bajo el núm. ..... de su protocolo.

Y, reconociéndose ambas partes, mutua y recíprocamente con capacidad legal suficiente para el presente acto,

**EXPONEN**

A) Que X ha subcontratado las actividades consistentes en *[añadir descripción de los servicios que realiza el encargado del tratamiento]* de su sociedad en la empresa Y.

B) Que, en cumplimiento con lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de protección de datos de carácter personal (en adelante LOPD), el tratamiento de datos de carácter personal por cuenta de tercero requiere la celebración de un contrato privado con los requisitos legales correspondientes.

De acuerdo con lo anterior, las partes suscriben el presente contrato, que se regirá de conformidad con las siguientes

**CLÁUSULAS**

**PRIMERA.- Definiciones**

Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Según la terminología anterior, X es el responsable de los ficheros y Y es el encargado del tratamiento de los mismos.

**SEGUNDA.- Objeto**

El objeto del presente contrato es el tratamiento por parte de Y de los datos personales relativos a *[incluir colectivo de personas físicas afectadas]* de X, con la finalidad de poder realizar *[añadir descripción de los servicios que realiza el encargado del tratamiento]*, para lo cual previamente deberá ésta poner a disposición del encargado del tratamiento dichos datos personales.

Dicho tratamiento se realizará de conformidad con lo establecido en la LOPD y en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, o normativa que los sustituya.

**TERCERA.- Precio**

La remuneración por los servicios concertados en virtud del presente contrato se entiende incluida en la cantidad que percibe Y por las actividades indicadas en el expositivo primero que realiza por cuenta de X.

**CUARTA.- Datos a los que se da acceso y nivel de seguridad**

Los datos personales que forman parte de los ficheros de X, a los que tendrá acceso el encargado del tratamiento son los siguientes:

- *[incluir relación de ficheros y datos afectados por el tratamiento de Y y su nivel de seguridad]*

**QUINTA.- Obligaciones del Encargado del Tratamiento**

1. El encargado del tratamiento solamente tratará los datos que se le han encomendado conforme a las instrucciones del responsable del fichero.
2. Los datos facilitados no se aplicarán ni utilizarán con una finalidad diferente a la que figura en este documento, ni el encargado del tratamiento los comunicará, ni siquiera a efectos de su conservación, a terceros.
3. El encargado del tratamiento y el personal a su cargo están obligados a guardar secreto y absoluta confidencialidad respecto de los datos que les han sido confiados para su tratamiento.
4. El encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, sustracción, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
5. En caso de resolución del presente contrato, los datos serán destruidos en su totalidad o devueltos al responsable del fichero, teniendo en cuenta los distintos soportes o

documentos donde estos puedan constar: bases de datos en discos, ficheros temporales, copias de seguridad, soportes en papel, etc.
6. Una vez se haya realizado la operación mencionada en el punto anterior, el encargado del tratamiento se compromete a entregar una declaración por escrito al responsable del fichero donde conste que así se ha realizado.
7. Será de aplicación en todo caso, en lo no previsto en este contrato, la normativa vigente en materia de protección de datos personales.

**SEXTA.- Duración y resolución del contrato**

El presente contrato se considera accesorio del contrato de arrendamiento de servicios, consistente en *[añadir descripción de los servicios que realiza el encargado del tratamiento]* de X existente entre las partes, por lo que su duración y extinción queda supeditada al mismo.

**SÉPTIMA.- Ley aplicable y foro**

El presente contrato se regirá e interpretará conforme a la legislación española en aquello que no esté expresamente regulado, sometiéndose las partes, para las controversias que pudieran surgir en relación con el mismo, a la competencia de los Juzgados y Tribunales de la ciudad de ....., con renuncia a cualquier otro foro que les pudiera corresponder.

Y en prueba de su conformidad, firman las partes el presente contrato en duplicado ejemplar y a un sólo efecto, en lugar y fecha señalados en el encabezamiento.

D. .....
por X

D.....
por Y