TFG:Estudi del nou reglament general de protecció de dades en sistemes informàtics

Àrea : Administració de xarxes i sistemes operatius

Autor: Ismael del Rosal Hernández
Data: 03 / 01 / 2018

Consultor: Miquel Colobran Huguet
Titulació: Grau de Tecnologies de la Telecomunicació, 4º curs, UOC

Dedicatòria i agraïments

Dedico aquest projecte a totes les persones que han cregut en mi, i m'han recolzat en tot moment:
Als meus pares que, des que era un nen, van posar tots els seus esforços per a que fos una persona amb arraigats valors ètics i morals, a més de sempre intentar donar-me la millor educació que van poder, i que tingués uns estudis superiors per a poder afrontar la vida amb les millors condicions possibles.

Als meus germans i a la meva neboda, que, sempre que m'han faltat les "forces", en aquells moments en què sentia que ja no podia més, he rebut la seva estima i recolzament.

Als meus amics que m'han fet sentit que puc ser una mena d'inspiració per a ells. I que han tingut sempre paraules que m'han omplert d'orgull per tot l'esforç d'aquests anys.

I, per últim, a totes les persones que no han pogut finalitzar els seus estudis, siguin quines siguin les raons; dir-los que també ho poden aconseguir. Només fa falta que creguin en ells mateixos, i, sobretot, que siguin persistents. TFG: Estudi del nou reglament general de protecció de dades en sistemes informàtics.

Resum

On May 25, 2018, the implementation period of the new data privacy law will finish for all member countries of the European Economic Community (EEC). This new regulation affects users, workers, and companies among others. It is known as the General Data Protection Regulation (GDPR) of the European Parliament and of the Council of 27 April 2016 (EU) 2016/679.

The present work is motivated by the relevance of this law, which will involve consequences for a large part of the world population. Therefore, this study will be carried out on how to apply it within a private organization, focusing on the necessary modifications of the information system in any company.

This migration of the computer information system to the regulation involves the analysis of the present system. After that, the process of modification will be done in a step-by-step way: evaluating each article of the new legislation and trying to find the most effective solution at the IT level.

The work have to reach its objectives by detailing the changes to be implemented at the hardware and software level, and at the same time arguing the reason why such changes are performed according to the corresponding section of the law. Moreover, the steps to follow must be developed with a clear and concise language, using whatever. tools are necessary in order to specify the main ideas.

One hopes that the work will be a useful reference for anyone who intends to get an overview of the relevance of this law, as well as to those who need to know what his or her responsibilities are depending on his or her role, whether it is worker, company owner or user. More specifically, one of the main objectives of this work is that any user becomes able to solve many of his or her doubts regarding the new law, as well as acquire the knowledge of how to face a migration. The work can also be used to simply get an overall idea of everything the new law can involve.

Índex de continguts

Índex de figures

1.Introducció

1.1 Justificació del TFG

El present document correspon al treball de fi de grau (TFG) del Grau de Tecnologies de la Telecomunicació desenvolupat a la Universitat Oberta de Catalunya (UOC) i està emmarcat dins de l'àrea d'administració de xarxes i sistemes operatius. S'ha escollit la temàtica d'aquest projecte a través de dos criteris:

- Es considera aquesta iniciativa molt interessant, ja que representa tot un desafiament.
- La transcendència a nivell global que aquesta tindrà entre els membres i entitats involucrades.

1.2 Objectius

Identificar, analitzar i finalment exposar en un treball escrit fins a on arriba el marc legal de la implantació de la nova llei de privacitat de dades. Es tindrà en compte tant la part legal com la d'ètica civil. Es posarà èmfasi en els passos en línies generals que cal seguir per la seva implementació amb atenció a les repercussions pels sistemes informàtics existents.

- Elaborar un estudi de recerca provinent de diferents fonts d'informació d'àmbit governamental per obtenir la informació jurídica necessària.

- Determinar quins són els aspectes més rellevants a desenvolupar i com plantejar-los per aconseguir que siguin el més entenedors possibles. S'inclourà una guia general d'adaptació dels sistemes informàtics als canvis de la reforma legal.

- Analitzar la informació de manera eficient i objectiva.

- Organitzar la informació fent servir gestors de documents, bibliografia, etc.

- Analitzar les modificacions dels nous punts respecte a la legislació anterior i com repercutiran. I com afecta a l'administració dels sistemes informàtics.

1.3 Enfocament i mètode seguit

El context el treball es basa en una empresa fictícia (consultori psicològic online) on es necessita implantar el nou Reglament de Protecció de Dades. En primer lloc, s'ha descrit a nivell general a què es dedica l'empresa així com els sistemes de xarxa que requereix. A partir d'aquí s'han seguit els diferents punts de la guia d'implantació del nou reglament sempre posant exemples específics d'aplicació d'aquest.

1.4 Planificació del projecte

Estudi del nou reglament general de protecció de dades en sistemes informàtics.			
	Setmana	**Activitat**	**Memòria**
1	20-24 setembre	Elecció del tema a desenvolupar.	
2	25-1 octubre	Determinar quines són les pautes a complimentar en general. Recerca d'una part fonamental del projecte a desenvolupar, elemental per a complimentar la planificació del treball.	
3	**2-8 octubre**	**PAC1 - Proposta de pla de treball del TFG.**	**PAC 1**

Estudi del nou reglament general de protecció de dades en sistemes informàtics.			
	Setmana	**Activitat**	**Memòria**
4	9-15 octubre	Elaboració de la portada, dedicatòria i resum del treball.	

5	16-22 octubre	Establir l'índex dels continguts més el cos de la memòria.	
6	23-29 octubre	Desenvolupament de l'índex i dels primers capítols.	
7	30-5 novembre	Desenvolupar els apartats des del punt 5.1.1 fins al 5.1.6.	
8	**6-12 novembre**	**Lliurament PAC2: eines triades + disseny.**	**PAC 2**
9	13-19 novembre	Afegir altres capítols en referència al tema que he escollit.	
10	20-26 novembre	Penúltim capítol amb la llista de verificació.	
11	27-3 desembre	Últim capítol amb la mesura del nivell d'implantació.	
12	4-10 desembre	Glossari, Bibliografia i Annexos.	
13	**11-17 desembre**	**Lliurament PAC3: resultats.**	**PAC 3**
14	18-24 desembre	Lliurament Memòria.	
15	25-31 desembre	Presentació.	
16	1-7 gener	**Entrega FINAL. Memòria i presentació.**	**Entrega Final**

El diagrama de Gantt corresponent es mostra a continuació:

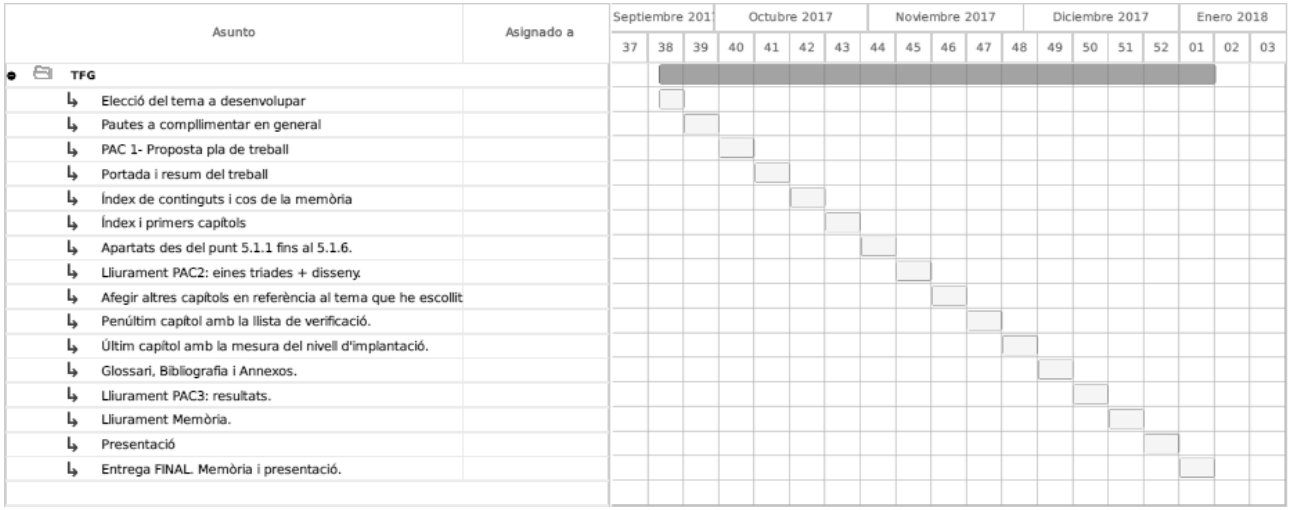

Figura 1: Diagrama de Gantt.

1.5 Breu descripció dels altres capítols de la memòria

Capítol 1: Introducció. En aquest capítol es realitza la justificació de la temàtica escollida pel TFG, els objectius que es desitgen assolir en el desenvolupament d'aquest i l'enfocament i la metodologia seguida.

Capítol 2: Anàlisi del Nou Reglament de Protecció de Dades. En aquest capítol es presenta un visió general del Nou Reglament de Protecció de Dades i es fa un petit resum dels diferents aspectes que cal tractar i tenir en compte quan es vol implantar aquest reglament en una organització.

Capítol 3: Descripció de l'empresa. En aquest capítol es presenta una empresa fictícia sobre la que es pretén implantar el reglament de protecció de dades. Es realitza una visió general de l'empresa incidint sobre la seva estructura organitzativa. També es descriuen els equips informàtics i la xarxa que s'utilitza.

Capítol 4: Bases de la legitimació del tractament de dades. En aquest capítol es presenta una descripció de la base legal per l'empresa analitzada i la documentació associada .

Capítol 5: Transparència i informació. En aquest capítol es presenta una descripció de com es presenta la informació sobre com es tracten les dades personals dels clients de forma clara i transparent.

Capítol 6: Drets. En aquest capítol es presenta una descripció de com els usuaris dels serveis que ofereix l'empresa poden exercir els seus drets tal i com estableix el RGPD.

Capítol 7: Mesures de responsabilitat activa. En aquest capítol es presenta una descripció de les mesures de seguretat que cal que l'empresa tingui en compte per protegir la privacitat dels usuaris. Això inclou un anàlisi previ de les dades que es tracten i un detall de les mesures adoptades.

Capítol 8: Llista de verificació I. En aquest capítol es presenten unes qüestions que pretenen verificar el grau d'implantació del RGPD en l'empresa estudiada.

Capítol 9: Llista de verificació II. En aquest capítol es presenten la segona part de qüestions referent al capítol 8.

Capítol 10: Mesura del nivell d'implantació. El capítol va íntimament lligat amb els dos capítols anteriors i pretén verificar el nivell d'implantació del RGPD.

Capítol 11: Guia de bones pràctiques per la implantació del RGPD. En aquest capítol es presenta una guia bàsica general dels aspectes més rellevant a tenir en compte per realitzar la implantació del RGPD en una empresa genèrica.

Capítol 12: Conclusions. En aquest capítol es detalla les conclusions finals.

Capítol 13: Bibliografia. En aquest capítol es detalla les fonts utilitzades.

Capítol 14: Apèndix. En aquest capítol es detalla els apèndixs.

2.Analisi del Nou Reglament de Protecció de Dades

2.1 Visió general

La progressiva integració econòmica i social de la Unió Europea ha comportat un augment substancial dels fluxos de dades personals en i entre tots els estats membres. Aquest increment d'intercanvi de dades personals involucra tant a operadors públics com privats, persones físiques, associacions i empreses. Aquest fet és inevitable i necessari pel progrés del conjunt de la societat europea però implica un sistema de regulació i protecció de dades personals a nivell europeu. Aquesta protecció de dades és un dret fonamental tal com estableix la Carta dels Drets Fonamentals de la Unió Europea involucrant a totes les persones residents a la Unió Europea i assegurant el respecte a la vida privada i familiar, la llibertat de personal i a la diversitat cultural, religiosa i lingüística. Cal destacar però, que el dret a la protecció de dades personals no és un dret absolut sinó que s'ha de considerar en relació amb la seva funció a la societat i mantenir l'equilibri amb els altres drets fonamentals tot fent ús del principi de proporcionalitat [1].

Per altra banda, la ràpida evolució tecnològica i la globalització han plantejat nous reptes per a la protecció de dades personals ja que la magnitud de la recollida i l'intercanvi de dades personals ha augmentat de manera significativa. Aquest intercanvi de dades, que molts cops pot implicar tercers països, ha d'estar recolzada amb sistemes tecnològics prou robustos a fi de garantir un nivell de protecció de dades personals suficientment elevat.

És per aquest motiu que el nou Reglament General de Protecció de Dades (RGPD), (UE) 2016/679, va entrar en vigor al maig de 2016 i serà aplicable a partir de maig de 2018. Aquest nou reglament substitueix les disposicions de la Directiva 95/46. El nou reglament permet adaptar-se a l'entorn sòcio-econòmic actual evitant que el reglament de protecció de dades suposi un obstacle en l'exercici de les activitats econòmiques i permetre que els autoritzats compleixin les seves funcions. En aquest període de transició entre la Directiva 95/46 i el nou RGPD, els responsables i encarregats del tractament de dades han d'adoptar les mesures necessàries pel compliment del RGPD en el moment de l'aplicació.

Cal destacar que la nova RGPD conté molts dels conceptes, principis i mecanismes establerts en la Directiva 95/46 amb la qual cosa, les empreses que l'apliquen actualment ja tenen una bona base de partida per la correcta aplicació d'aquest nou Reglament.

Dos dels elements que suposen la major innovació del RGPD respecte la Directiva 95/46 són els que es mencionen a continuació:

- **Principi de responsabilitat proactiva:** Aquest principi estableix que el responsable del tractament de dades personals, analitzi quines dades tracta l'organització, amb quina finalitat ho fan i quin tipus de tractament es porta a terme amb elles. A partir d'aquest anàlisi, cal explicitar les mesures adequades per complir amb el RGPD i que aquestes puguin ser demostrades davant dels interessats i els autoritats de supervisió. D'aquí es dedueix el nom del principi, on es demana pro activitat per part de les organitzacions davant del tractament de dades personals que es portin a terme.

- **L'enfocament de risc:** En aquest enfocament es ressalta que les mesures establertes pel RGPD s'han d'aplicar necessàriament quan les dades suposin un alt risc pels drets i llibertats mentre que les altres s'han de modular en funció del tipus de riscs que els tractaments presenten. Això implica un enfocament de risc en el tractament de dades específic per cada organització i que unes mesures aplicables en una empresa no tenen perquè ser necessàries en una empresa de característiques diferents.

Cal destacar que el passat 24 de Novembre de 2017 es va presentar davant del Congrés de Diputats el Projecte de Llei Orgànica de Protecció de Dades de Caràcter Personal. El projecte de Llei té per objectiu adaptar l'ordenament jurídic espanyol al reglament 2016/679 del Parlament Europeu relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals de les persones físiques i la lliure circulació d'aquestes dades. Tot i així, en aquest document s'ha seguit el que queda establert en el reglament 2016/679 ja que aquesta Llei Orgànica pot patir esmenes i en el moment de la redacció del document encara no havia estat presentada davant del Congrés.

2.2 Bases de la legitimació pel tractament de dades

Tal i com s'ha exposat en el punt anterior, el RGPD manté molts dels principis exposats en la Directiva 95/46, entre ells, una base jurídica que la legitimi. Aquesta base jurídica està basada en els següents punts:

- Consentiment.
- Relació contractual.
- Interessos vitals de l'interessat o d'altres persones.
- Obligació legal pel responsables.
- Interès públic o exercció de poders públics.
- Interessos legítims prevalent del responsable o de tercers als que es comuniquen les dades.

En aquest sentit, cal documentar i identificar clarament les bases legals sobre les que s'articula el tractament de dades personals. Això fa necessari que s'inclogui la base legal en el moment de la recollida de dades dels interessats. A més a més, cal especificar i documentar els interessos legítims en el que es fonamenten les operacions de tractament de dades.

La identificació de la base legal és per tant indispensable per estar en condicions de demostrar que es compleix amb les previsions dels RGPD.

Cal destacar, a més a més, que tant la identificació com la documentació s'ha d'adaptar al tipus de tractament de dades que fa l'organització i per tant és responsabilitat d'elles adaptar-la a les seves característiques.

Per altra banda, el consentiment de la persona que cedeix les seves dades personals ha de ser inequívoc a través d'una acció clara i afirmativa. En el marc d'aquest nou reglament, queda descartat el consentiment per omissió o inacció.

Segons la sensibilitat de les dades personals i de les operacions a realitzar es poden distingir diferents matisos en el consentiment. D'aquesta manera, el consentiment cal que sigui **inequívoc i explícit** en els següents casos:

- Tractament de dades sensibles.
- Adopció de decisions automatitzades.
- Transferències internacionals.

En altres casos, el consentiment ha de seguir sent inequívoc però es pot realitzar de forma implícita. En el cas de tractaments de dades iniciats anteriorment al RGPD, seguiran sent legítims sempre que la forma de consentiment s'adapti al tractament inequívoc (i explícit si és el cas) que s'ha mencionat anteriorment.

És per aquest motiu que es recomana que no s'obtingui el consentiment per omissió. En el cas que sigui necessari l'adaptació al nou RGPD es pot procedir obtenint el consentiment directe de l'interessat o bé informant a l'interessat donant-li el dret a l'oposició basant-se amb altres bases legals.

2.3 Transparència i informació als interessats

Tota la informació que es proporcioni als interessats s'haurà de presentar de forma concisa i transparent amb un llenguatge senzill i clar.

Això implica evitar utilitzar expressions excessivament complexes així com referències a textos legals. Això afecta també a tota clàusula informativa, que a més a més hauran de ser fàcilment accessibles i entenedores per tota persona, independentment del seu domini del tema. A més a més tota informació que es proporcioni als interessats s'ha de facilitar per escrit.

2.4 Drets establerts al RGPD

En el RGPD s'estableixen els drets ARCO (Accés, Rectificació, Cancel·lació i Oposició) a part d'alguns drets nous. Els usuaris poden exercir els seus drets en qualsevol moment i el responsable de tractament de dades de l'organització n'ha de facilitar l'accés i assegurar-se que aquest sigui fàcil de realitzar. A més a més, aquest servei cal que sigui gratuït, només amb l'excepció de que els usuaris vulguin exercir els seus drets de forma molt reiterada. En aquest cas, l'organització pot cobrar-li un cànon de gestió a l'usuari o bé negar-se a formular la seva sol·licitud sempre i quan escrigui a l'usuari el motiu de forma clara.

El termini màxim establert per la resposta a les sol·licituds d'exerció de drets dels usuaris és d'un mes i es pot ampliar a dos mesos per sol·licituds especialment complexes si s'informa a l'usuari dins del període del primer mes. Un punt interessant a tenir en compte, és que es pot disposar d'un sistema remot segur i amb prou garanties per facilitar a l'usuari l'accés directe amb a les seves dades personals.

Cal fer menció explícita a l'anomenat **dret a l'oblit**, el qual no està contemplat de forma directa, perquè és conseqüència de dos drets ARCO, en concret el dret a la cancel·lació i el dret a l'oposició. A efectes pràctics, per tant, s'ha de garantir també el dret a l'oblit tot assegurant la correcta eliminació de qualsevol possible traça d'informació atribuïble a l'organització. A més a més, si la informació s'ha de compartir amb una altre organització, s'ha de comunicar a aquesta la sol·licitud de l'usuari que vol exercir dret a l'oblit.

Així mateix, l'usuari pot sol·licitar la limitació del tractament de les seves dades. Aquest fet implica que l'empresa no podrà fer servir les dades de l'usuari fins a nova ordre de l'usuari.

En el RGPD, s'estableix també el dret a la portabilitat on s'ha de crear una còpia estructurada de les dades personals del sol·licitant transmetent-les directament al responsable de tractament de dades de l'organització on es vol fer la portabilitat.

2.5 Relacions responsable-encarregat

En el RGPD s'estableixen les obligacions específiques de l'encarregat del tractament de dades personals. Els responsables hauran d'escollir únicament encarregats que ofereixin garanties suficients per aplicar mesures tècniques i organitzatives apropiades, de manera que el tractament sigui conforme amb el RGPD. La relació entre el responsable i l'encarregat s'ha de formalitzar amb un contracte o bé amb un acte jurídic.

2.6 Mesures de responsabilitat activa

Tots els responsables hauran de realitzar una valoració del risc de tots els tractaments de dades que realitzin a fi d'establir les mesures que s'han d'aplicar. Les grans organitzacions cal que utilitzin alguna de les metodologies d'anàlisis existents. Pel que fa a les organitzacions de menor complexitat es pot realitzar un reflexió a partir de determinades qüestions com les que es mostren a continuació:

- Es tracten dades sensibles?
- S'inclouen dades d'una gran quantitat de persones?
- S'inclou l'elaboració de perfils en el tractament de dades?
- Es creuen les dades obtingudes amb els disponibles en altres fonts?
- Es poden utilitzar les dades obtingudes per altres finalitats?
- Es tracten grans quantitats de dades?
- S'utilitzen tecnologies invasives com ara la GEO localització o la videovigilància a gran escala?

Quantes més respostes afirmatives hi hagi, més risc pot derivar-se del tractament de dades. Els responsables del tractament de dades han d'assegurar que només es tractin les dades necessàries. Aquests hauran d'adoptar les mesures tècniques i organitzatives tot buscant un compromís entre el

cost de la tècnica, el cost de l'aplicació i els riscos pels drets i llibertats de les persones.

Quan es produeixi una violació de la seguretat de les dades, el responsable ha de notificar-la a l'autoritat de protecció de dades competent. Aquesta notificació ha de ser el més immediata possible i dins de les primeres 72 hores de que hi hagi constància de la violació de seguretat. A més a més, pot ser necessària una notificació a l'usuari si aquesta pot atemptar contra els seus drets i llibertats.

Per altra banda, els responsables del tractament de dades hauran de realitzar una avaluació d'Impacte sobre la Protecció de Dades (EIPD) si el tractament pot comportar un alt risc pels drets i les llibertats. El contingut mínim d'aquest EIPD no està estipulat però existeix una guia de referència[3]. En el cas que es detecti alt risc que no es pugui abordar amb la tecnologia actual caldrà posar-se en contacte amb l'autoritat competent.

2.7 Transferències internacionals

Les dades podran ser comunicades fora de l'Espai Econòmic Europeu en els següents casos:

- Països, territoris o sectors on s'hagi adoptat un decisió reconeixent el nivell de protecció adequat.
- Quan es tinguin garanties suficients del destí d'aquestes.
- Es poden aplicar excepcions per interès del propi usuari o per interessos generals.

2.8 Tractaments de dades de menors

El RGPD estableix que el consentiment de l'usuari només serà vàlid a partir dels 16 anys. Altrament s'haurà de comptar amb l'autorització dels pares o tutors legals. Tot i així, cada estat membre pot reduir aquest llindar d'edat sempre i quan no sigui inferior als 13 anys. En el cas d'Espanya es preveu que aquesta sigui de 14 anys.

Es requereix que els responsables de tractament de dades facin tots els esforços que la tecnologia permeti a fi de verificar que els menors de l'edat límit tinguin el consentiment per part dels pares o tutors legals.

2.9 Llista de verificació

A fi de fer una valoració ordenada de la situació de l'organització enfront de les principals obligacions del RGPD s'utilitza l'anomenada llista de verificació que estableix un seguit de qüestions emmarcades dins dels següents apartats:

- Legitimació.
- Informació i drets.
- Relacions responsable-encarregat.
- Mesures de responsabilitat proactiva.

Aquesta llista es pot simplificar quan el volum de dades tractades és menor o quan el risc de les dades personals és baix. En aquest cas es pot simplificar la llista en els següents punts:

- Identificació de la base jurídica.
- Verificació de la informació que es proporciona als interessats.
- Establiment d'un registre d'activitats de tractament.
- Exercici de drets dels interessats.
- Identificació de les mesures de seguretat.
- Verificació de les relacions amb els encarregats del tractament de dades.

3.Descripció de l'empresa

Fins aquí s'ha revisat la nova legislació i els canvis que comporta. En aquest capítol es descriu una empresa genèrica de mida mitjana on es farà l'estudi i aplicació perquè s'ajusti a la nova normativa.

3.1 Visió general de l'empresa

L'empresa genèrica que es presenta per implantar el nou reglament de protecció de dades (RGPD) és un consultori psicològic online. L'empresa disposa d´una plataforma online accessible per mitjà d'ordinadors connectats a internet o des d'aplicacions mòbils que permetin que els usuaris comparteixin per aquesta via les seves preocupacions i interessos a psicòlegs amb titulació oficial. La plataforma permet que s'estableixi un contacte virtual entre els clients i els psicòlegs titulats i permet gestionar la seva activitat professional. L'empresa és una empresa inventada pel present Treball de Fi de Grau i serà anomenada Psico online.SL

Figura 2: Logotip de l'empresa Psico Online.SL.

3.2 Característiques del servei

Les característiques del servei que ofereix l'empresa són les següents:

- **Servei d'alta qualitat:** Psico Online ajuda a millorar la felicitat del client. Es posen a la disposició del client fins a 100 psicòlegs especialistes en el suport al client.
- **Accessible:** És un servei que de manera accessible, privada i còmode permet mantenir video-trucades i xat amb un psicòleg titulat en dies laborables.
- **Garantia de devolució:** La prioritat de l'empresa es fonamenta en una relació de confiança amb el client. Per aquest motiu, si no es queda satisfet amb el servei durant la primera setmana, es retornen els diners sense compromís.

Quan un client accedeix al servei, és atès personalment per un dels assessors, i aquest al seu torn procedeix a assignar un especialista segons les necessitats requerides. El servei inclou la realització de tests psicològics que permeten assignar l'especialista més adequat pel client. Un cop assignat l'especialista en qüestió, aquest realitzarà una exhaustiva avaluació a fi de poder comprendre millor la situació del client a través d'una videoconferència o xat segons el que es cregui oportú. Un cop realitzat el contacte, el psicòleg explicarà l'origen del problema i junt amb el client es definiran els objectius i el tractament a seguir per part del client.

Arribat a aquest punt, es definirà el tractament que intentarà incidir de forma positiva sobre les emocions, les conductes, els pensaments i les relacions afectives o socials del client amb l'objectiu de millorar l'estat actual. Aquestes eines s'oferiran al client mitjançant sessions totalment interactives.
Un cop acabat el servei, el client tindrà la possibilitat de valorar al psicòleg que l'ha atès i podrà opinar sobre el servei rebut. A més a més, el client té a la seva disposició gràfics indicatius sobre la seva evolució.

3.3 Organigrama de l'empresa

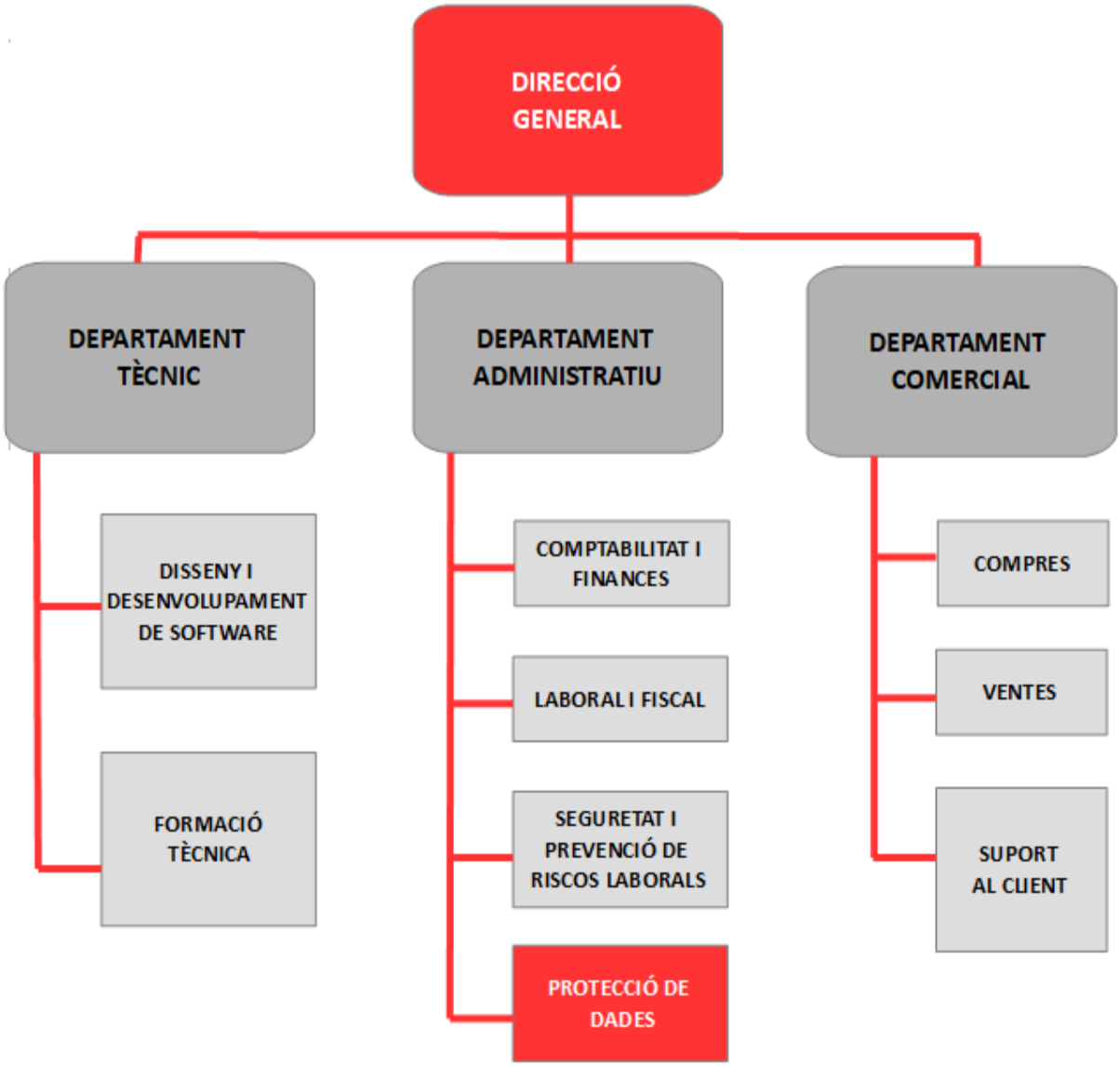

Figura 3: Organigrama de l'empresa Psico Online.SL.

El departament tècnic de l'empresa ocuparà el gruix més important d'aquesta ja que es tracta d'una companyia que ofereix un servei online. Aquest departament s'encarregarà del desenvolupament i manteniment del software i les bases de dades relacionades, així com la instal·lació d'equips informàtics (ordinadors, servidors, impressores...) i el seu manteniment. L'objectiu principal és desenvolupar un programari eficient, amb un interfase per l'usuari que sigui el més simplificada i intuïtiva possible a part de que l'experiència per part del client sigui la més satisfactòria possible.

El software ha de tenir cura que el client se senti guiat en tot moment durant el servei ofert amb una interfase atractiva visualment i ben estructurada. Tots els menús i botons d'accés han de quedar ben destacats. A més a més, el departament tècnic de l'empresa s'ocuparà de que el software sigui tecnològicament prou robust a fi d'evitar possibles atacs al servidor per part de tercers amb el fi de garantir en tot moment la confidencialitat i la protecció de dades dels usuaris del servei.

Una altra de les funcions importants del departament tècnic serà la correcta documentació del software i les bases de dades a fi de facilitar i millorar la productivitat dels programadors. En aquesta línia, el departament tècnic oferirà formació tècnica als treballadors de nova incorporació o als becaris que facin pràctiques d'universitats procurant que es sentin el més acompanyats possible en tot moment i que comencin a ser productius el més aviat possible.

El departament d'administració s'encarregarà de la part de la comptabilitat i finances així com tot el tema laboral i fiscal. En l'àmbit laboral es portarà tot el tema de les nòmines dels treballadors i la selecció i incorporació de nous treballadors per l'Empresa. En aquest departament també hi haurà l'encarregat de riscos laborals i el responsable de protecció de dades personals, el qual tindrà un paper molt important ja que en aquesta empresa es tracten dades molt confidencials de clients.

El departament comercial de l'empresa ocupa un lloc destacat dins de l'organització de l'empresa amb l'objectiu principal de potenciar la venta del servei que ofereix l'empresa, el màrqueting i el suport al client. Com que es tracta d'una empresa que ofereix un servei digital online, el tema del suport al client cal que estigui molt cuidat i potenciat ja que es vol que qualsevol client es senti recolzat en tot moment davant de qualsevol dubte que li pugui sorgir abans, durant o després del servei ofert per l'empresa

3.4 Implementació dels serveis TIC de l'empresa

Els elements bàsics dels quals disposarà la xarxa de l'empresa Psico Online amb la finalitat de cobrir totes les necessitats de l'empresa són els següents:

- Estacions de treball.
- Servidor.
- Switch.
- Router.
- Servidor d'impressió.
- Impressora.
- Fax.

Aquests elements queden interconnectats tal i com s'indica a la figura que es mostra a continuació:

Figura 4: Esquema de la xarxa de Psico Online.

3.4.1. Infraestructura de la xarxa

La infraestructura de la xarxa estarà basada en un switch que permet la creació d'una xarxa local i que a diferència dels Hub, permet enviar informació directament a l'ordinació destí sense replicar-se a la resta d'equips que estiguin connectats a la xarxa. D'aquesta manera es pot obtenir una comunicació fluida tot disminuint els errors de transmissió.

La xarxa LAN implementada (backbone) serà de 1 Gb Base-TX (bits transmesos a 1000 Mbit/s). Cal dir que aquesta és una velocitat de transmissió teòrica a la qual no s'arribarà realment degut a la capçalera i la cua pel direccionalment i la detecció d'errors en els paquets. A més a més, és possible que es produeixin errors a la transmissió que obliguin a retransmetre el paquet i també hi pot haver temps d'espera si hi ha la xarxa ocupada.

Aquesta xarxa s'implementarà físicament amb cable de parell trenat. Aquest tipus de cablejat presenta dos conductors elèctrics aïllats i entrellaçats amb l'objectiu d'anular interferències externes i la diafonia del cablejat adjacent. Segons els tipus de xarxa implementada, existeixen diferents categories de cables a utilitzar. En el cas de Psico Online, al tractar-se d'una xarxa 100 Base-Tx serà necessari un cable de Categoria 6.

Figura 5: Cable de categoria 6.

Com que l'empresa tracta i guarda dades confidencials de clients, serà necessari utilitzar una xarxa privada i confiable que permeti preservar tota aquesta informació en un servidor de base de dades. Per al nostre cas, el router ja incorpora la DMZ integrada. D'aquesta manera, en cas de que entri algun malware al servidor públic, la xarxa privada que conté el servidor de base dades queda protegit.

L'enllaç a internet es farà a través d'un router proveït d'un firewall que donarà un primer nivell de protecció, però hi haurà un segon firewall entre servidor i la xarxa privada.

A més a més, degut a que l'empresa tractarà amb dades molt importants, s'utilitzarà el protocol HTPPS el qual es basa en SSL/TLS a fi de crear un canal xifrat de comunicació. Aquest protocol per tant, garanteix la seguretat en la informació ja que evita atacs de tercer que es poden fer amb informació confidencial com pot ser l'atac man-in-the-middle i el eavesdropping.

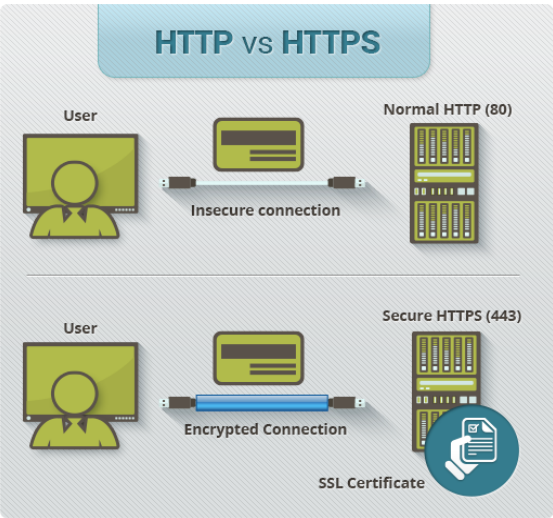

Figura 6: Diagrama que contrasta el protocol HTTP amb HTTPS.

3.4.2. Servidor

El primer element clau per la xarxa és el **servidor,** el qual té com a finalitat principal l'oferiment de serveis, i és per aquest motiu que ha d'estar composat per elements que permetin oferir seguretat,

estabilitat i eficiència, no només a nivell de hardware sinó també a nivell de software.

En l'empresa Psico Online serà necessari implementar dos servidors, tal i com s'ha explicat en l'apartat anterior. El primer serà un servidor públic en la zona desmilitaritzada i el segon estarà dins de la xarxa segura i contindrà tota la informació crítica a protegir.

- **Servidor de la zona desmilitaritzada:** Es tracta d'un servidor d'accés públic que es troba en la zona desmilitaritzada. Aquest servidor gestionarà l'accés dels clients a la plataforma de Psico-Online i no contindrà cap base de dades amb informació privada dels clients.
- **Servidor dins de la xarxa segura:** Es tracta d'un servidor d'accés restringit que es troba en la zona privada. Aquest servidor és el que contindrà les bases de dades amb la informació personals dels clients de la plataforma.

El sistema operatiu seleccionat pels servidors de forma que puguin administrar de forma ràpida i segura l'entorn de treball és Ubuntu Server 16.04.3 LTS, el qual és específicament dissenyat per servidors i pertany al grup de software lliure. Aquest sistema operatiu és compatible amb la majoria de perifèrics i a més a més es pot obtenir una imatge del sistema operatiu de forma ràpida i totalment gratuïta.

3.4.3. Estacions de treball

Les estacions de treball són equips d'altes prestacions destinades al treball tècnic. Els equips han de permetre treballar de forma fluida i eficient als treballadors de l'empresa. Han de ser fiables, compatibles entre ells i han d'oferir escalabilitat. Han de tenir, per tant, unes bones característiques bàsiques com per exemple el processador, la memòria RAM i la connexió a la xarxa. Les estacions de treball estaran equipades amb el sistema operatiu Ubuntu 17.10.

Serà necessari crear un sistema d'identificació d'usuaris amb diferents perfils de forma que cada usuari tindrà un nivell de privilegis diferent en funció de les tasques que ha de desenvolupar. D'aquesta manera, els treballadors tècnics que s'encarreguen de desenvolupar i mantenir el software tindran més privilegis que treballadors d'altres departaments.

3.4.4. Servei d'intercanvi d'informació

Pel que es refereix al **servei d'intercanvi d'informació**, aquest està dissenyat per emmagatzemar, publicar i administrar la informació generada pels usuaris de la xarxa. Tot i que existeixen solucions a Internet com Dropbox o Google Drive que permeten fer l'intercanvi de forma ràpida i gratuïta, el fet de tractar amb informació confidencial dels clients, fa que sigui preferible comptar amb una solució pròpia que permeti administrar i compartir informació dins de la institució. Un dels beneficis d'haver escollit Linux com a plataforma de treball és que incorpora un servei d'intercanvi anomenat Samba, la qual és compatible amb equips Linux i Windows, permetent l'intercanvi d'informació de forma clara i transparent. El servei permet compartir documents, unitats de disc, impressores i estableix un procés d'autentificació per restringir l'accés als recursos.

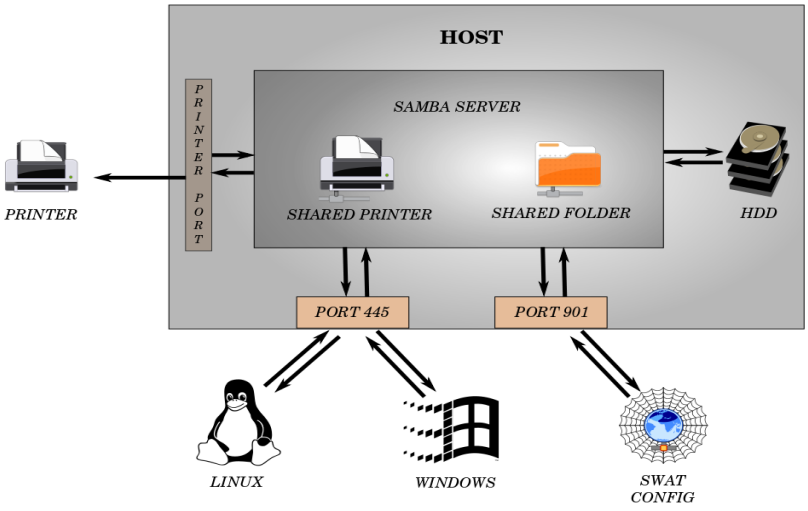

Figura 7: Esquema d'intercanvi d'informació a través del servei Samba.

3.4.5. Servei d'impressió

Pel que es refereix al **servei d'impressió en xarxa**, es pot utilitzar un altre dels serveis que ofereix

Linux anomenat CUPS (Common Unix Printing System). Aquest software permet configurar tot el que està relacionat amb els equips d'impressió com pot ser:

- Donar d'alta impressores.
- Administració centralitzada de recursos d'impressió.
- Balanç de càrregues de treball.
- Restricció d'accés al recurs (per usuari i per hora).
- Restricció d'impressions.
- Política de seguretat (configuració del recurs i modificacions al servidor).

3.4.6. Servei de base de dades

Pel que es refereix al **servei de bases de dades** s'utilitza el Postgre SQL perquè és una solució confiable, segura i estable pel tipus d'informació que tracta l'empresa. El Postgre SQL està dissenyat per treballar amb qualsevol tipus de càrrega de treball o volum d'accés, compta amb els controladors necessaris per intercanviar informació amb altres serveis de bases de dades. És una solució de software lliure que té suport a nivell mundial per millorar el servei dia a dia. A més a més, està dissenyat per treballar amb la majoria de llenguatges de programació actuals i permet emmagatzemar per a cada taula 32 Tb. Ha estat premiada en varies ocasions com el millor servei de bases de dades per "The Linux Journal Editor's Choice Awards"

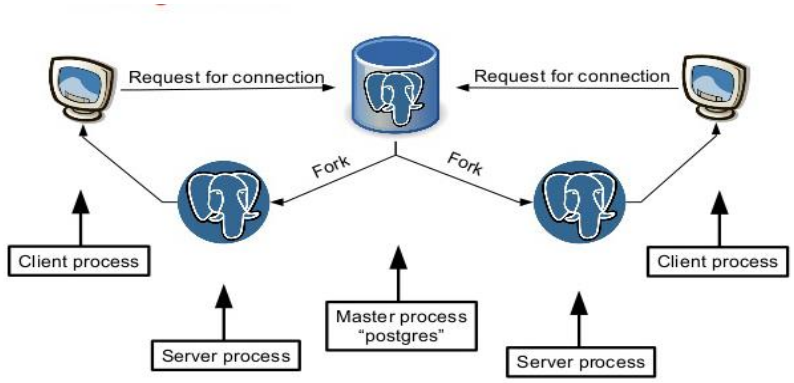

Figura 8: Interacció Client/Servidor amb PosgreSQL.

4.Bases de la legitimació pel tractament de dades

4.1 Documentació i identificació de la base legal sobre la que es desenvolupen els tractaments de dades

En primer lloc cal definir la base legal sobre el que es desenvoluparà el tractament de dades. Aquesta informació cal que sigui llegida per l'usuari i a més a més estigui reflectida de forma clara i entenedora. D'aquesta manera, i a través del mateix sistema informàtic, s'ha d'obligar a l'usuari que vol contractar el servei a llegir la base legal sobre la que es desenvolupen els tractaments de dades. Les condicions legals proposades per l'empresa Psico Online es poden consultar a l'apèndix 1.

Un cop definides les bases legals de l'empresa Psico Online, s'especificarà la política de protecció de dades que de fet complementen les condicions legals anteriors. L'objectiu és que quedin especificats i documentats els interessos legítims en els que es fonamenten les operacions de tractament de dades. El document de política de privacitat es pot consultar a l'apèndix 2.

4.2 Consentiment inequívoc

Tal com s'estableix en el RGPD cal que el consentiment que proporcioni l'usuari sigui clarament afirmatiu i ja no pot ser per omissió. En el cas de l'empresa Psico Online, a més a més, cal que sigui un consentiment explícit ja que treballa amb dades sensibles de l'usuari. D'aquesta manera, i aprofitant que el servei proporcionat és online, serà possible registrar-se a la plataforma de Psico Online complint els següents requisits en el moment d'emplenar les dades.

Caldrà que totes les dades que es demanen en el formulari de registre estiguin completes. Es pot fer la comprovació per codi a més a més que els caràcters que emplenen els diferents camps siguin lògics.

Figura 9: Camps demanats a l'usuari de caràcter obligatori.

S'obligarà a llegir a l'usuari que es vol registrar les condicions legals amb un sistema d'scroll que fins que no arribi a la part més baixa no habiliti la possibilitat d'habilitar la casella d'acceptació de les condicions legals esmentades. Si aquesta casella d'acceptació no està habilitada no es podrà enviar el formulari.

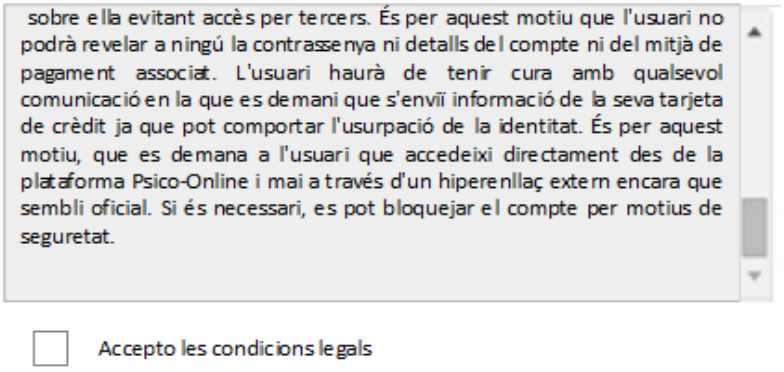

Figura 10: Scroll i acceptació de les condicions legals.

De la mateixa manera que en el punt anterior, s'obligarà a l'usuari a llegir la política de protecció de dades mitjançant un sistema d'scroll que quan arribi a la part inferior habilitarà la casella d'acceptació de la política de protecció de dades. Si aquesta casella no està habilitada no es podrà enviar el formulari.

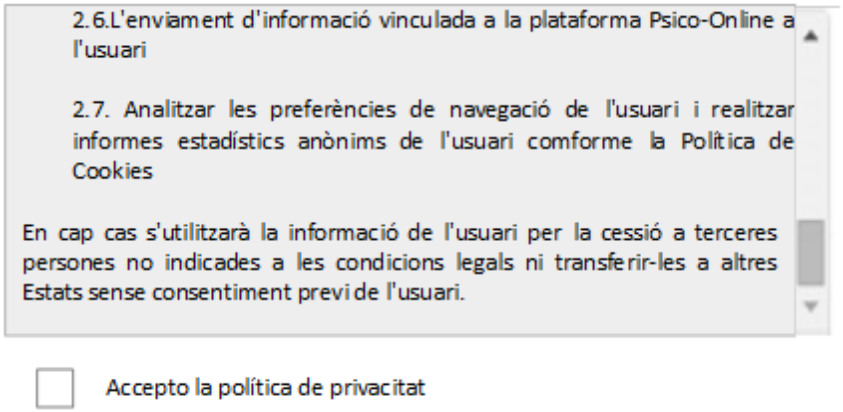

Figura 11: Scroll i acceptació de la política de privacitat.

5.Transparència i informació

5.1 Aspectes generals

Actualment la LOPD estableix les següents informacions que s'han de facilitar a les persones interessades:

- La existència del fitxer o tractament, la seva finalitat i destinataris.
- El caràcter obligatori o no de la resposta, així com les seves conseqüències.
- La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició
- La identitat i dades de contacte del responsable del tractament.

A més a més, segons el RGPD caldrà afegir els següents punts:

- Les dades de contacte del Delegat de Protecció de Dades.
- La base jurídica o legitimació pel tractament.
- El termini o criteris de conservació de la informació.
- La existència de decisions automatitzades o elaboració de perfils.
- La previsió de transferències a tercers països.
- El dret a presentar una reclamació davant les Autoritats de Control.

5.2 Qui i quan cal informar

La responsabilitat d'informar recau sobre el Responsable de Tractament de Dades. La informació s'ha de proporcionar de forma immediata i en cas de que no s'obtinguin del propi interessat es facilitaran abans d'un mes. A més a més, cal que quedi constància que s'ha facilitat aquesta informació. En cas que l'usuari ja disposi de la informació, no serà necessari proporcionar la informació, o bé quan resulti un esforç desproporcionat. En qualsevol cas caldrà donar una resposta a l'usuari que ha fet la petició d'informació.

5.2 On i com informar

El mitjà de transmissió d'informació que s'utilitzarà per defecte serà la pròpia plataforma web Psico Online donat que aquest és un servei web. Per aquesta raó, dins de l'espai personal de l'usuari s'inclourà una pestanya que permeti la gestió de la informació de l'usuari. En aquesta pestanya es detallarà tota la informació necessària de forma clara i detallada tal i com estableix el RGPD. Quan l'usuari cliqui la pestanya del seu perfil es desplegarà la següent informació:

- **Responsable del tractament de dades:** En aquest apartat s'inclourà la informació del responsable del tractament. Concretament, cal incloure de forma clara com contactar amb el responsable, així com la identitat i les dades de contacte del representant.

- **Finalitat del tractament:** S'inclourà una breu descripció senzilla de la finalitat del tractament de dades. A més a més, hi haurà els terminis i criteris de conservació d'aquestes dades i si cal la lògica amb la qual s'automatitza aquesta informació.

- **Legitimitat del tractament de dades:** En aquesta secció la base jurídica sobre la que es sustenta el tractament de dades, així com l'obligació o no de facilitar dades.

- **Destinataris del tractament de dades:** En aquest apartat s'especificaran els destinataris d'aquesta informació així com les decisions corporatives aplicables.

- **Drets de les persones interessades:** Caldrà detallar clarament com exercir els drets d'accés, rectificació, supressió, i portabilitat de dades. A més a més, s'ha de poder retirar el consentiment donat així, com la possibilitat de reclamar davant l'Autoritat de Control.

5.3 Clàusula Informativa de Psico Online

Dins del seu perfil personal de la plataforma Psico Online l'usuari tindrà accés a la clàusula informativa. Aquesta clàusula especificarà de forma clara i entenedora el nom del contacte i el seu correu de contacte. En aquesta clàusula informativa, quedarà clara la finalitat del tractament de les dades de l'usuari i es justificarà perquè es demana cada una d'elles. Es deixarà clar també, que s'està complint el Reglament General de Protecció de Dades aplicable a partir del maig de 2018. A més a més, caldrà que quedi clar qui rebrà i tractarà aquesta informació així com els protocols interns i codis de conducta que s'estableix en la corporació. Finalment, es deixarà clar a l'usuari la possibilitat d'exercir els seus drets i es facilitarà que ho pugui fer de forma clara i fàcil.

La clàusula informativa de Psico Online es pot consultar a l'apèndix 3.

6.Drets

6.1 Aspectes generals

El responsable de tractament de dades de l'organització cal que faciliti als clients l'exercici dels seus drets i per tant, els procediments han de ser senzills, visibles i fàcilment accessibles. Com que Psico Online es tracta d'una empresa que ofereix un servei on-line, caldrà que aquests drets es puguin exercir per mitjans electrònics. A més a més, caldrà que l'exerció d'aquests drets sigui gratuïta pels usuaris exceptuant el cas en que les sol·licituds siguin molt reiteratives o excessives on l'empresa es podrà negar a actuar o bé cobrar un cànon per compensar els costos administratius.

6.2 Procediment per l'exercici dels drets

El sistema informàtic de Psico Online proporcionarà dins de l'espai personal de cada client l'opció d'exercir els seus drets. La pestanya dins de l'espai personal s'anomenarà Drets de l'usuari, i quan es cliqui es mostraran els drets que es permeten exercir a l'usuari. Aquests drets són els següents:

- Accés a les dades personals.
- Rectificació de les dades personals.
- Cancel·lació de les dades personals.
- Oposició de les dades personals.

Abans d'accedir a qualsevol de les opcions que es despleguen en la pestanya de Drets de l'usuari, es realitzarà un procés de validació d'identitat de l'usuari tal i com estableix el RGPD. Aquesta validació es realitzarà enviant o bé un correu electrònic o bé un SMS al mòbil de l'usuari que contindrà una clau de verificació d'identitat. L'aspecte visual d'aquest sistema de validació d'identitat és tal i com es mostra a continuació:

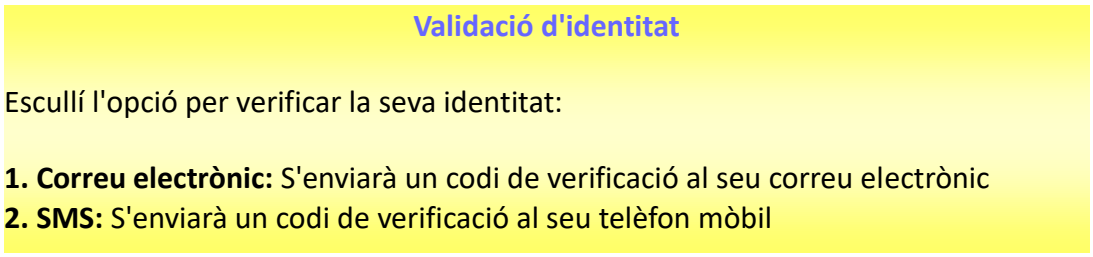

Figura 12: Mètode de validació d'identitat de l'usuari.

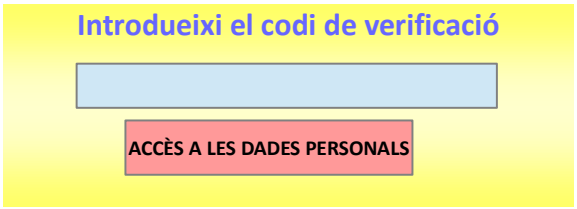

Figura 13: Codi de verificació de l'usuari.

Un cop es validi la identitat de l'usuari es podrà accedir a la part privada que permet exercir els drets a l'usuari. En el cas de **l'accés a les dades personals** es desplegarà un finestra emergent amb les dades de l'usuari que consten al registre de Psico Online actualment. En aquesta finestra emergent es desplegaran els següents camps de l'usuari:

- Nom i cognoms.
- DNI.
- Contrasenya.
- Correu electrònic.
- Telèfon Mòbil.

A més a més, el sistema permetrà descarregar-se aquestes dades al dispositiu de l'usuari en format .PDF. L'usuari també tindrà accés als resultats dels tests psicològics que hagi realitzat utilitzant la plataforma.

6.3 Dret d'accés

El nou reglament de protecció de dades (RGPD) contempla l'obligació de l'organització a proporcionar una còpia de les dades personals a l'usuari si així ho sol·licita. Tal i com es contempla en el punt anterior, l'usuari podrà descarregar-se en format .PDF les seves dades personals des de la seva àrea d'usuari. Aquest accés es realitzarà mitjançant una connexió segura amb el procés de validació previ descrit en el punt anterior.

6.4 Dret a l'oblit

El dret a l'oblit no és un dret que es contempli de forma directa en el RGPD, però si que es pot considerar un dret derivat d'altres drets ARCO que si que estan contemplats. Per tant no deixa de ser una manifestació dels drets de cancel·lació i oposició. La combinació d'aquests dos drets fa que l'usuari pugui exercir el dret a esborrar les seves dades personals si així ho sol·licita.

Psico Online permetrà l'esborrament de les dades personals de l'usuari dins de l'àrea d'usuari. Aquest fet comportarà que es donarà de baixa l'usuari de la plataforma i per tant no podrà tornar a accedir al servei a no ser que es torni a registrar de nou. Aquest fet s'informarà de forma clara en el moment de que es realitzi la sol·licitud d'esborrament de dades personals.

Aquest apartat es trobarà dins de l'àrea privada d'usuari i s'anomenarà **Baixa del servei i esborrat de dades personals.** Quan l'usuari cliqui aquest apartat es desplegarà un finestra emergent amb el següent aspecte:

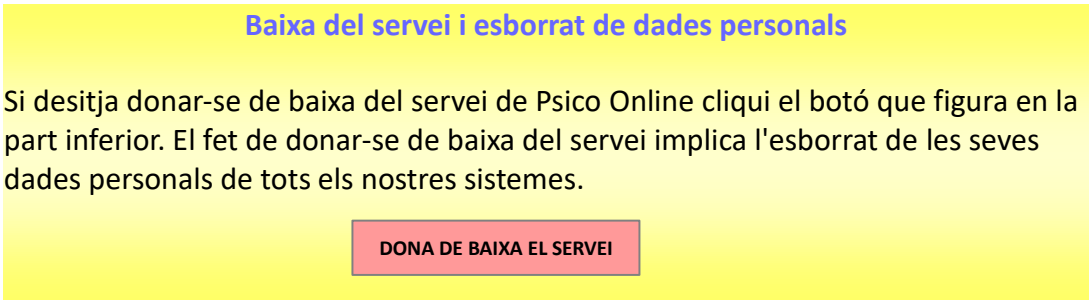

Figura 14: Baixa de servei i esborrat de dades personals.

6.5 Limitació del tractament de dades

El nou RGPD permet que l'usuari sol·liciti a l'organització que realitza el tractament de dades personals la limitació del tractament d'aquestes. Aquest fet comportarà que les dades de l'usuari no es pugin tractar fins a nou avís i la única funció de l'empresa serà la de conservar aquestes dades llevat de certes excepcions. L'organització podrà tractar les dades d'un usuari que ha sol·licitat la limitació de les seves dades personals en els següents casos:

- Quan es compti amb el consentiment de l'usuari.
- Per l'exercici de reclamacions.
- Per protegir els drets d'una tercera persona.
- Per raons d'interès públic important dins de la UE.

D'aquesta manera, l'empresa Psico Online disposarà també d'un apartat dins de l'espai personal de l'usuari que permetrà sol·licitar la limitació d'ús de les seves dades personals. Aquest apartat dins de l'àrea privada d'usuari s'anomenarà **Sol·licitud de la limitació de dades personals**. L'aspecte que presentaria aquest apartat seria el següent:

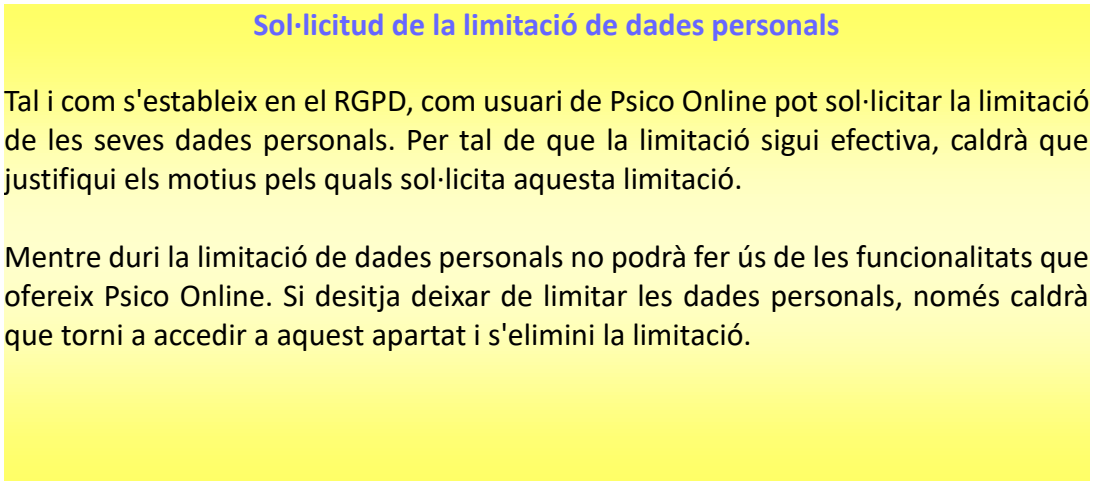

Figura 15: Sol·licitud de la limitació de dades personals.

No es podrà limitar les dades personals si no s'especifica el motiu.

En el cas de que l'usuari ja tingui limitat l'ús de dades personals, quan aquest torni a accedir al seu espai personal dins de l'apartat **Sol·licitud de la limitació de dades personals,** veurà la següent finestra**:**

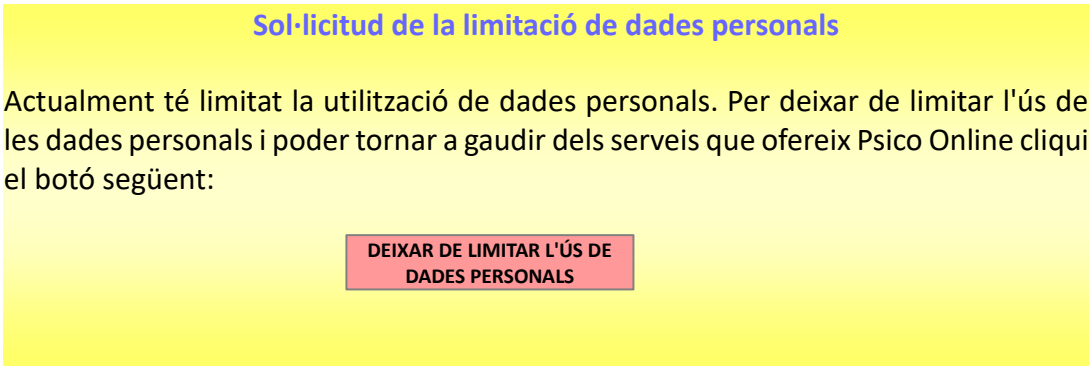

Figura 16: Deixar de limitar de dades personals.

6.6 Portabilitat

El dret a la portabilitat consisteix en un forma avançada del dret d'accés. El RGPD estableix que l'organització ha de facilitar la portabilitat de les dades personals d'un usuari si així es sol·licita. A més a més, cal que aquestes dades es proporcionin de forma que es puguin llegir de forma automatitzada.

En el cas de Psico Online, s'establirà un format de portabilitat de dades personals basat en un full de càlcul ja que es considera que la majoria de sistemes informàtics són capaços de llegir-ho de forma fàcil i el seu tractament de forma automatitzada també resulta fàcil i còmode.

7.Mesures de responsabilitat activa

7.1 Aspectes generals

El nou RGPD estableix obligacions expressament dirigides als encarregats tot i que la responsabilitat última segueix residint en el responsable de protecció de dades personals. Les obligacions específiques que caldrà que exerceixin els encarregats de protecció de dades són les següents:

- Manteniment de les dades personals.
- Determinar mesures de seguretat aplicables al tractament que realitzen.
- Designar un Delegat de Protecció de Dades.

7.2 Elecció de l'encarregat del tractament de dades

Tal i com estableix el RGPD cal que l'encarregat del tractament de dades personals tingui les garanties suficients en el referit a l'aplicació de mesures tècniques i organitzatives. Per aquest motiu, l'empresa Psico Online establirà que si es vol disposar d'un encarregat de dades caldrà que aquest certifiqui les seves competències a través d'un certificat expedit per un empresa externa.

7.3 Contingut del contracte entre responsable i encarregat

El RGPD estableix que tota relació entre el responsable del tractament de dades i l'encarregat corresponent s'ha de formalitzar a través d'un contracte. Aquest contracte haurà de contenir els següents aspectes:

- Objecte, duració i naturalesa dels tractaments.
- Tipus de dades personals i categories d'interessats.
- Obligació de l'encarregat de tractar les dades personals seguint les instruccions del responsable.

- Condicions per que el responsable pugui donar l'autorització prèvia a las subcontractacions.
- Assistència al responsable per l'exercici de drets dels interessats.

El model de contracte entre el responsable de protecció de dades i l'encarregat de protecció de dades s'estableix en l'annex 4 del present document.

8.Llista de verificació I

8.1 Aspectes generals

El nou RGPD estableix que els responsables del tractament de la informació han de seguir un conjunt de mesures per tal de garantir que tots els tractaments de dades que realitza una organització són conformes amb el Reglament General de Protecció de Dades.

8.2 Anàlisi de risc

Tots els responsables del tractament de dades hauran de realitzar una valoració de risc dels tractaments que realitzen. Caldrà tenir en compte aspectes com el tipus de tractament realitzat, la naturalesa de les dades, el nombre d'interessats afectats i la quantitat de tractaments que es realitzen.

Com que Psico Online és una empresa relativament petita es realitzarà una reflexió documentada sobre la implicació dels tractaments realitzats en els drets i llibertats dels usuaris. Aspectes plantejats:

1. Es tracten dades sensibles? **SÍ.**
2. S'inclouen dades d'una gran quantitat de persones? **SÍ.**
3. Inclou el tractament la elaboració de perfils? **SÍ.**
4. Es creuen les dades obtingudes dels interessats amb altres disponibles en altres fonts? **NO.**
5. Es pretén utilitzar les dades obtingudes per una altra tipus de finalitat? **NO.**
6. Es tracten grans quantitats de dades. Incloses tècniques d'analisi massiu tipus big data? **NO.**
7. S'utilitzen tecnologies especialment invasives per la privacitat, com les relatives a GEO localització, videovigilància a gran escala? **NO.**

En el cas de Psico Online per tant, es respon afirmativament 3 de les 7 qüestions plantejades i per tant cal posar en marxa mesures per la protecció de les dades tractades per l'organització.

8.3 Registre de les activitats de tractament

En les empreses de més de 250 treballadors, els responsables del tractament de dades i si és el cas l'encarregat del tractament de dades cal que mantinguin un registre del tractament que es realitza en la corporació:

- Nom i dades de contacte del responsable del tractament de dades.
- Finalitats del tractament de dades.
- Descripció de les categories del interessats i categories de dades personals tractats.
- Transferències internacionals de dades.

Psico Online, tot i tenir menys de 250 treballadors, treballa amb dades personals rellevants. A més a més, es recullen dades sobre el seu comportament i es realitzen perfils psicològics. Tot això implica que caldrà mantenir un registre de les activitats que realitzi del tractament de dades.

Psico Online per tant posarà a la disposició de qualsevol organisme de control el nom i les dades de contacte del responsable de tractament de dades, en concret el correu electrònic de domini psico-online.com

Per justificar la finalitat del tractament de dades s'exposaran els següents punts:

- Es demana el nom ,cognoms i document nacional d'identitat per tal de poder tenir identificat l'usuari donat que hi ha pagaments on-line. A més a més, serà necessari el correu electrònic i el telèfon mòbil de l'usuari com a mitjà de comunicació entre l'empresa i l'usuari. El correu electrònic també servirà per accedir a l'espai personal online i per gestionar la contrasenya d'accés a la plataforma. El telèfon mòbil i el correu electrònic també s'utilitzen com a mitjà de validació de la identitat de l'usuari quan aquest vulgui accedir a les seves dades personals tal i com estableix el RGPD.

- Es recolliran dades de caràcter psicològic mitjançant tests psicològics amb la finalitat

d'elaborar un perfil psicològic de l'usuari que puguin ajudar a seleccionar el professional que encaixi millor amb el client.

- Es mantindrà un registre amb les conversacions establertes en els xats entre els pacients i els professionals per tal de vetllar per l'ús adequat i ètic de la plataforma per les dues parts.

8.4 Protecció de dades des del disseny i per defecte

El nou RGPD demana que es pensi en la protecció de dades el mateix moment en que es dissenya un tractament de dades determinat.

El responsable de tractament de dades de Psico Online prendrà totes les mesures organitzatives i tècniques per integrar en els tractaments les garanties que permetin aplicar de forma efectiva tots els elements exposats en el RGPD. És per aquest motiu que Psico Online garanteix que només es tracten les dades estrictament necessàries pel correcte funcionament de la plataforma.

A més a més, Psico Online garanteix que els treballadors només podran accedir a les dades personals que siguin estrictament necessàries. La plataforma que brinda Psico Online serà prou robusta per tal d'evitar intrusions de tercers que puguin accedir sense permís a les dades personals de clients.

8.5 Mesures de seguretat

En el nou RGPD, els responsables estabiran les mesures tècniques i organitzatives per tal de garantir un nivell de seguretat adequat en funció dels riscs detectats prèviament.

En el cas de l'empresa Psico Online es treballa amb dades classificades amb nivell de risc ALT ja que estan relacionats amb aspectes psicològics dels usuaris. Psico Online presentarà les següents mesures de seguretat:

- **Emmagatzemant de la informació:** Els documents amb dades personals estaran emmagatzemats en armaris i arxivadors amb protecció d'accés i es trobaran en un lloc tancat.
- **Accés a dades a través de xarxes de comunicacions:** Les dades personals corresponents als fitxers dels pacients de Psico Online es realitzarà mitjançant xifrat de dades utilitzant el protocol HTTPS basa en SSL/TLS. D'aquesta manera es garanteix que la informació no serà intel·ligible ni manipulable per tercers.

- **Fitxers temporals o còpies de treball de documents:** Els fitxers temporals o còpies de documents creats exclusivament per treballs temporals o auxiliars seran esborrats o destruïts un cop hagin deixat de ser necessaris per la finalitat que van motivar la seva creació.

- **Còpia o reproducció:** La realització de còpies o reproducció dels documents amb dades personals només es podrà realitzar sota el control del responsable o l'encarregat del tractament de dades. Les còpies hauran de ser destruïdes impossibilitant el posterior accés a la informació continguda en elles.

- **Periodicitat de còpies:** Es realitzaran còpies de recuperació de dades amb una periodicitat setmanal llevat de que no s'hagués produït cap actualització de dades en aquest període. Les proves anteriors a la implantació o modificació de sistemes d'informació es realitzarà amb dades reals prèvia còpia de seguretat.

8.6 Notificació de violacions de seguretat de dades

Davant de qualsevol destrucció, pèrdua o alteració (accidental o il·lícita) de dades personals o bé un accés no autoritzat a aquestes dades serà considerada una violació de seguretat de dades. Davant d'aquesta situació, caldrà una notificació en menys de 72 hores a l'autoritat de protecció de dades.

En el cas de Psico Online, si es detecta un cas de violació de seguretat de dades personals, el

responsable de tractament de dades personals es posarà en contacte de forma immediata amb l'Autoritat Catalana de Protecció de dades. En aquesta notificació s'explicitarà la naturalesa de la violació, la categoria de les dades personals afectades i les mesures adoptades per solucionar la situació. A més a més, com que les dades que tracta Psico Online són molt sensibles caldrà realitzar també una notificació als usuaris que hagin quedat afectats.

Cal destacar però, que la mera sospita de que ha existit una violació de seguretat sense que es coneguin mínimament les circumstàncies no hauria de donar lloc a una notificació donat que no seria possible determinar fins a quin punt pot existir risc pels drets i llibertats dels interessats. Tot i així, Psico Online intensificaria en els esforços dels seus tècnics informàtics per tal d'esbrinar el més aviat possible de si es tracta realment d'un cas de violació de seguretat de dades.

9.Llista de verificació II

La llista de verificació pretén ajudar a les organitzacions a dur a terme de forma ordenada una valoració de la situació davant de les principals obligacions del RGPD. És per tant un excel·lent indicador sobre el grau d'implantació de les mesures explicitades en el RGPD. Aquesta llista de verificació està composta de diverses preguntes aglutinades per àmbits d'aplicació.

LEGITIMACIÓ	
Té establerta clarament quina és la base legal dels tractaments que realitza i ha documentat d'alguna forma la manera en què l'ha establert?	**SÍ**
Si algun dels tractaments que realitza està basat en el consentiment dels interessats, ; Ha verificat que aquest consentiment reuneix els requisits que exigeix el RGDP? en cas contrari, s'ha previst com demanar el consentiment de forma adaptada a l'RGPD o ha trobat una altra base legal adequada per a aquests tractaments?	**SÍ**

INFORMACIÓ I DRETS	
La informació que es proporciona als interessats, està presentada de forma clara, concisa, transparent i de fàcil accés?	**SÍ**
Conté aquesta informació tots els elements que preveu el RGPD?	**SÍ**
Disposa de mecanismes per l'exercici dels drets visibles, accessibles i senzills? Poden exercir-se els drets per via electrònica?	**SÍ**
Té establerts procediments o mecanismes que li permetin verificar la identitat de qui sol·licita accés o exerceixin els altres drets ARCO?	**SÍ**
Té establerts procediments que li permetin respondre als exercicis de drets en els terminis previstos pel RGPD? Ha valorat si seria necessària la col·laboració dels encarregats per respondre a les sol·licituds dels interessats i, si és així, té previst incloure aquesta col·laboració en eles contractes d'encàrrec?	**SÍ**
En particular, té previstos mecanismes per atendre possibles exercicis de drets a la limitació del tractament de dades, de forma que les dades dels afectats puguin ser conservats sense ser objecte de les operacions de tractament que correspondria?	**SÍ**
Ha valorat si els tractaments de les dades que realitza poden ser objecte del dret a la portabilitat? En cas afirmatiu, ha previst el procediment o mecanismes per poder atendre aquest dret i proporcionar les dades a l'interessat (o a un responsable) en un format estructurat, d'ús comú i de lectura mecànica?	**SÍ**

RELACIONS RESPONSABLE-ENCARREGAT	
Ha previst com valorar si els encarregats amb els quals hagi contractat o vagi a contractar operacions de tractament ofereixen garanties de compliment del RGPD quan sigui de aplicació?	**SÍ**
Contenen els contractes d'encàrrec que actualment tingui subscrits tots els elements que preveu el RGPD? En cas contrari, està fent passos per adaptar-los abans de l'aplicació del RGPD?	**SÍ**

MESURES DE RESPONSABILITAT PROACTIVA	
Ha fet una valoració dels riscos que els tractaments que desenvolupa impliquen per els drets i llibertats dels ciutadans? Ha determinat quines mesures de responsabilitat activa corresponen a la seva situació de risc i com ha de aplicar-les?	**SÍ**
Ha previst com establir el registre d'activitats de tractament en la seva organització?	**SÍ**
Ha valorat si li és d'aplicació alguna de les excepcions a aquesta obligació? Ha previst qui s'encarregarà de mantenir actualitzat el registre?	**SÍ**
Ha revisat les mesures de seguretat que aplica als seus tractaments a la llum dels resultats de l'anàlisi de risc dels mateixos? Considera que pot seguir aplicant les mesures de seguretat previstes en el Reglament de la LOPD? Ha valorat prou la possibilitat d'introduir mesures addicionals en funció del tipus de tractament o del context en què es realitza?	**SÍ**
Atenent al tipus de tractaments que realitza, ha establert mecanismes per identificar amb rapidesa l'existència de violacions de seguretat de les dades?	**SÍ**
Té previstes mesures de reacció davant els diferents tipus de fallides de seguretat, inclosos els procediments per avaluar el risc que puguin suposar per als drets i llibertats dels afectats? Ha establert procediments per notificar les violacions de seguretat a les autoritats de protecció de dades i, si cal, als interessats? Disposa d'un registre o eina similar en què pugui documentar els incidents de seguretat que es produeixin, encara que no siguin notificats a les autoritats de protecció de dades?	**SÍ**
Ha valorat si els tractaments que realitza requereixen una Avaluació d'Impacte sobre la Protecció de Dades perquè suposen un alt risc per als drets i llibertats dels interessats?	**SÍ**
Disposa d'una metodologia per a la realització de l'Avaluació d'Impacte?	**SÍ**
Segons el tipus de tractament que realitza i els resultats de l'anàlisi de riscos previ, ¿té de nomenar un Delegat de Protecció de Dades?	**NO**
	NO

Ha establert els criteris per seleccionar al Delegat de Protecció de Dades i, en particular, per valorar les seves qualificacions professionals i els seus coneixements?	
El lloc de DPD tal com està configurat en la seva organització, respecta els requisits d'independència en l'exercici de les funcions, posició en l'organigrama, absència de conflicte d'interessos i disponibilitat dels recursos necessaris establerts pel RGPD?	**NO**
Ha fet pública la designació del DPD i les seves dades de contacte i els ha comunicat a la autoritat de protecció de dades?	**NO**
Ha establert procediments perquè els interessats contactin amb el DPD?	**NO**

10.Mesura del nivell d'implantació

Tal i com s'ha pogut constatar en el punt anterior del present document, el nivell d'implantació de les mesures exposades en el RGPD es pot considerar alt.

S'ha aconseguit identificar la base jurídica dels tractaments de dades que es realitzen a Psico Online. S'ha establert una relació contractual entre el client i l'empresa que el mateix client ha d'acceptar si es vol registrar en la plataforma conforme amb les especificacions del RGPD.

Psico online informa clarament i de forma transparent sobre els tractaments que es realitzen. A més a més, s'explica a l'usuari la finalitat i la justificació de cada una de les dades personals que es demanen als usuaris. També es proporciona el contacte amb el responsable de tractament de dades. Tota aquesta informació es proporciona a través de la plataforma virtual i es troba dins d'una aparença clara i entenedora.

Psico Online preveu els mecanismes per facilitar l'exercici dels drets i la resposta a les sol·licituds. L'empresa ofereix una plataforma online on l'usuari pot accedir al seu espai personal amb un sistema d'identificació previ que li permeten exercir tots els drets contemplats en el RGPD. Psico Online proposa un sistema d'exerció de drets d'usuaris molt intuïtiu i fàcil d'utilitzar per part de l'usuari. A més a més, es disposa d'una servei d'atenció personalitzat en cas de qualsevol dubte per part de l'usuari.

Pel que es refereix a les mesures de seguretat, Psico Online ha establert mesures en tot el que es refereix a l'emmagatzemat de documents digitals i físics, política de còpies de seguretat i recuperació i xifratge de dades.

Psico Online ha establert la relació entre el responsable de tractament de dades i l'encarregat de tractament de dades a través d'un document contractual tal i com s'estableix en el RGPD.

11. Guia de bones pràctiques per la implantació del RGPD en una organització.

Per tal d'implantar el RGPD el primer que cal considerar és que cada organització és diferent. Una de les premisses del RGPD és que cal particularitzar i analitzar en detall l'empresa i les dades que s'utilitzen en ella per tal d'establir els protocols de forma adequada. De totes maneres, es poden establir un seguit de passos comuns que poden servir per la majoria de les organitzacions.

1 LEGITIMACIÓ

El primer pas a seguir per tal d'implantar el RGPD en una organització és establir una base legal pel tractament de dades. Cal establir una verificació del consentiment de l'usuari. Tota la informació que es proporcioni a l'usuari ha de ser clara i concisa, tot tenint en compte que l'usuari no ha de ser expert en temes legals.

2 INFORMACIÓ I DRETS

En segon lloc cal assegurar-se de que es transmet a l'usuari informació a l'usuari de com es tracten les seves dades i perquè l'empresa les necessita. S'ha de propiciar a l'usuari una forma fàcil per tal que pugui exercir els seus drets. Per tant, preferiblement es recomana utilitzar una plataforma on-line fàcil i intuïtiva. És recomanable a més a més, que l'empresa despongui de suport telefònic per l'usuari. Cal establir un mecanisme d'identificació de l'usuari que vol exercir els seus drets. Es recomana utilitzar sistemes com el telèfon mòbil o el correu electrònic com a mitjà de verificació d'identitat. Cal establir també mecanismes que permetin realitzar la portabilitat de les dades personals dels usuaris en format llegible de forma automàtica. Es recomana utilitzar la creació d'arxius en formats àmpliament utilitzats com poden ser .txt o .xls

3 RELACIONS RESPONSABLE-ENCARREGAT

Cal realitzar un contracte entre el responsable del tractament de dades de l'empresa i l'encarregat del tractament de dades. En el contracte cal que consti l'objecte de l'encàrrec, la identificació, la duració i les obligacions de l'encarregat i del responsable del tractament de dades.

4 MESURES DE RESPONSABILITAT PROACTIVA

Cal que el responsable del tractament de dades faci una valoració dels riscs que entranya el tractament de dades de l'empresa.

A més a més, cal explicitar les mesures de seguretat que es tenen en compte per garantir la privacitat dels usuaris. En concret, cal incidir en temes com l'emmagatzemament de les dades, el xifratge de les dades i els protocols de creació de còpies de seguretat i recuperació. En el cas d'empreses multinacionals i que transmetin dades sensibles a gran escala caldrà que designin un Delegat de Protecció de Dades.

12.Conclusions

Un cop realitzat el present treball escrit s'ha pogut analitzar en detall el marc legal de la implantació de la nova llei de privacitat de dades. Després de realitzar un estudi de recerca contrastant diferents fonts d'informació s'han pogut determinar els punts més rellevant que cal desenvolupar per tal d'implantar la nova llei. S'ha pogut constatar que l'aplicació de la llei requereix fer un estudi previ profund de les característiques de l'empresa a la qual es vol implantar aquesta nova llei. És per aquest motiu que s'ha plantejat l'estudi a través d'una empresa fictícia on s'ha definit la seva organització principal i l'estructura de la seva xarxa i dels equips informàtics que la conformen. Cal destacar que les mesures implementades poder variar sensiblement en funció de les característiques de l'empresa escollida. Tot i així, s'ha procurat escollir un model d'empresa habitual en el nostre territori, amb dades sensibles i amb servei on-line.

S'ha pogut constatar que els aspectes per implantar el RGPD en una empresa es poden agrupar en quatre blocs bàsics. En primer lloc, cal establir un base legal que ha de quedar clara a l'usuari. En segon lloc, cal que l'usuari estigui informat de com es tracten les seves dades i cal assegurar-se de que pugui exercir els seus drets de forma fàcil. En tercer lloc, cal que s'estableixi una relació contractual entre els responsables i els encarregats del tractament de dades. Finalment, cal que l'empresa adopti mesures de seguretat per protegir les dades dels clients tenint en compte aspectes com l'emmagatzematge, el xifrat o les còpies de seguretat.

Finalment, cal destacar que actualment hi ha un projecte de Llei Orgànica de Protecció de Dades de Caràcter Personal presentada el 24 de Novembre davant del Congrés de Diputats. Aquesta llei encara pot patir esmenes, però en el moment en el qual sigui aplicable, caldria revisar el present document per assegurar que els protocol establerts s'adapten a la Llei Orgànica de Protecció de Dades.

13.Bibliografia

[1] Carta de los drets fonamentals de la Unión Europea [en línia]. Article 8
Disponible en*: http://www.europarl.europa.eu/charter/pdf/text_es.pdf*

[2] Agencia Espanyola de protecció de dades [en línia]. Guia d'avaluació d'Impacte sobre la protecció de Dades.[Madrid.2014]. Disponible en*: https://www.boe.es/doue/2016/119/L00001-00088.pdf*

[3] Agencia Espanyola de protecció de dades [en línia]. Guia d'avaluació d'Impacte sobre la protecció de Dades.[Madrid.2014]. Disponible en*: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/index-ides-idphp.php*

[4] Projecte de llei. [Madrid.2017]. Disponible en:
http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF

14.Apèndix

14.1 Apèndix 1

Condicions legals

1. Informació sobre Psico Online.SL

Psico Online.SL es una societat de responsabilitat limitada de nacionalitat espanyola que disposa de NIF número XXXXXX. La societat està inscrita en el Registre mercantil de Barcelona. Les dades de contacte de Psico Online.SL són les següents: XXXX, Barcelona. Direcció de correu electrònic: suport@psico-online.com

2. Descripció de la plataforma

Psico-Online és una plataforma online accessible per mitjà d'ordinadors o dispositius digitals amb connexió a internet que posa a la disposició dels usuaris la possibilitat de poder compartir interessos de caire psicològic amb psicòlegs que tenen titulació oficial.

3. Advertències importants sobre l'ús de la plataforma

Els clients del servei han de diferenciar els serveis que presten els terapeutes als clients dels serveis que ofereix Psico Online. Les comunicacions són oferires exclusivament pels psicòlegs pel seu compte i no en nom de l'empresa Psico Online. L'empresa Psico Online, únicament ofereix els mitjans tècnics necessaris per fer possible la comunicació entre els clients i els psicòlegs, així com el cobrament del servei prestat. D'aquesta manera, només els terapeutes són responsables de qualsevol reclamació de clients o terceres persones en relació als serveis prestats pels terapeutes o de la seva actuació durant les comunicacions.

4. Finalitat de la utilització del servei

Les comunicacions entre els clients i els psicòlegs és perquè els primers puguin compartir interessos de caire psicològic amb els segons. En cap cas però, les comunicacions es poden utilitzar per realitzar cap activitat mèdica ni un seguiment de patologies que requereixin una teràpia presencial. En aquests casos, els clientes i psicòlegs cal que s'abstinguin d'utilitzar la plataforma Psico Online.

En el cas de que vostè cregui que necessita atenció psicològica immediata (perill per la salut mental, està pensant en el suïcidi o que es pot posar en risc la salut de tercers) cal que es dirigeixi a un servei d'emergència mèdica de forma immediata.

5. Compromisos per part del client i psicòlegs

La utilització d'aquesta plataforma implica que s'ha de ser major d'edat. Cal utilitzar la plataforma Psico Online en el seu propi nom i per conta pròpia sota la seva pròpia responsabilitat i per fins personals. No es pot utilitzar la plataforma per fins promocionals o comercials i no perjudicar a tercers. Tampoc es pot utilitzar la plataforma per arxivar, descarregar, reproduir o crear treballs utilitzant la informació continguda en la plataforma Psico Online. En cap cas es pot fer difusió de continguts delictius, violents, pornogràfics, racistes o ofensius contraris a la llei i a l'ordre públic. Tampoc es pot utilitzar la plataforma per introduir virus informàtics o elements que danyin els sistemes informàtics de l'empresa o de terceres persones. De la mateixa manera, cal que els usuaris es comprometin a no intentar accedir a les comptes de terceres persones amb la finalitat d'extreure informació. En cas que es detecti que un usuari intenta infringir alguna d'aquestes condicions, Psico Online es reserva el dret de restringir l'accés al compte de l'usuari en qüestió.

14.2 Apèndix 2

Política de privacitat

1. Introducció

La present política de protecció de dades personals forma part de les Condicions Legals de l'empresa Psico Online. Aquesta Política de Protecció de Dades regula la recollida i el tractament per part de l'empresa Psico Online les dades personals dels usuaris que resulta del seu accés i la utilització de la plataforma Psico Online.

2. Informació i consentiment

Les dades personal que l'usuari voluntàriament faciliti per registrar-se a Psico Online, o els que es generen posteriorment com a conseqüència de la relació de Psico Online amb l'usuari, seran objecte de tractament, i en el seu cas, incorporats a fitxers, dels quals Psico Online és responsable.

Les dades que es sol·liciten a l'usuari en els formularis de recollida tindran caràcter obligatori llevat que s'indiqui el contrari i en el cas de que no es facilitin les dades no es podrà tramitar el formulari. A més a més, l'usuari garantida que les seves dades són correctes i no es refereixen a terceres persones. La finalitat de la recollida d'informació és la següent:

2.1.La gestió, desenvolupament i compliment de la relació contractual derivada de l'acceptació d'aquesta Política de Protecció de Dades, les Condicions Legals i la Política de Cookies amb motiu d'utilització de Psico Online.
2.2. Gestionar el registre de l'usuari a la plataforma Psico Online.
2.3. Assignar un psicòleg al client per les qüestions que preocupen al client.
2.4. Verificar la qualitat dels serveis prestats pels psicòlegs a través de Psico Online.
2.5. Atendre les sol·licituds, consultes i suggereixes de l'usuari.
2.6.L'enviament d'informació vinculada a la plataforma Psico Online a l'usuari.
2.7. Analitzar les preferències de navegació de l'usuari i realitzar informes estadístics anònims de l'usuari conforme la Política de Cookies.

En cap cas s'utilitzarà la informació de l'usuari per la cessió a terceres persones no indicades a les condicions legals ni transferir-les a altres Estats sense consentiment previ de l'usuari.

14.3 Apèndix 3

Clàusula informativa

Responsable del tractament de dades

NOM i COGNOMS RESPONSABLE
contacte: rtd@psico-online.com

Finalitat del tractament

Psico Online garanteix que el tractament de dades serà a nivell intern. El nom d'usuari i contrasenya són necessaris per poder gestionar l'accés a la plataforma i s'emmagatzema a una base de dades amb el nivell de seguretat adequat per tal d'evitar que aquesta sigui profanada. A més a més, quedaran enregistrats tots els xats entre l'usuari i els psicòlegs, però aquesta informació serà únicament accessible per part de l'usuari o pel psicòleg corresponent, però en cap cas es cedirà a tercers aquesta informació. A més a més, es demanarà el DNI de l'usuari per tal de poder identificar l'usuari en cas de mal ús de la plataforma.

Per altra banda, la informació que s'extregui de tests psicològics online, seran utilitzats de forma interna nivell corporatiu i mai es transferiran a tercers. A més a més, aquesta acció es farà de forma automatitzada i serà per la recomanació del professional o psicòleg més adequat per cada cas.

Legitimitat del tractament

Psico online garanteix que està complint amb el Reglament General de Protecció de Dades que va entrar en vigor a partir del maig de 2016 i serà aplicable a partir de maig de 2018. La base legal pel tractament de dades és l'execució del contracte de subscripció a la plataforma que va ser signat en el moment d'alta a la plataforma.

Destinataris de la informació

Els destinataris de part de la informació de l'usuari seran els psicòlegs amb els quals contacti l'usuari en les seves consultes. Aquests rebran informació purament professional quan estiguin en comunicació amb l'usuari. Els treballadors del departament informàtic tenen accés a la base de dades amb la informació, però en cap cas en poden fer ús forma de l'àmbit tècnic i molt menys transmetre-la a terceres persones. Per aquest motiu, els treballadors que tracten aquestes dades firmen clàusules de protecció de dades i la corporació estableix codis de conducta als seus treballadors amb l'objectiu de preservar la privacitat dels clients en tot moment.

Drets de l'usuari

L'usuari té dret a exercir els drets d'accés, rectificació, supressió i portabilitat de dades i la limitació del tractament de les seves dades en la pestanya Drets de l'usuari del perfil personal. En la mateixa pestanya, es podrà retirar el consentiment del tractament de dades donat en el moment de registrar-se. Aquest fet implicarà que l'usuari no podrà accedir a la plataforma fins que no torni a donar el consentiment. De la mateixa manera, l'usuari podrà demanar la limitació del tractament de dades, de manera que només els conservarem per l'exercici o defensa de possibles reclamacions per part de l'usuari.

14.4 Apèndix 4

Clàusula contractual per l'encarregat de protecció de dades personals

1.Objecte de l'encàrrec del tractament de dades

Mitjançant les presents clàusules s'habilita a l'entitat Psico Online S.L, encarregada del tractament, per tractar a càrrec de …....., responsable de tractament de dades, les dades de caràcter personal necessàries per prestar el servei d'encarregat de tractament de dades de l'empresa Psico Online S.L.

El tractament consistirà en la conservació ,consulta, limitació i destrucció de les dades personals dels clients dins de la plataforma que ofereix Psico Online.

2.Identificació de la informació afectada

Per l'execució de les prestacions derivades del compliment de l'objecte d'aquest encàrrec, el responsable del tractament de dades posa a la disposició de l'encarregat del tractament de dades l'accés sense limitacions a la base de dades amb el registre de les dades personals del clients de Psico Online.

3.Duració

El present acord té una duració de dos anys. Un cop finalitzi el present contracte, l'encarregat del tractament de dades haurà de retronar al responsable les dades personals tractades i suprimir qualsevol còpia que estigui al seu poder.

4.Obligació de l'encarregat del tractament de dades

L'encarregat del tractament de dades està obligat a:

a. No utilitzar les dades dels clients de Psico Online S.L per fins propis.

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

c. Portar per escrit un registre de totes les categories d'activitats de tractament efectuades.

d. No comunicar les dades a terceres persones, llevat que es consti amb l'autorització expressa del responsable del tractament de dades personals, en els supòsits legalment admissibles.

e. No subcontractar cap de les prestacions que formin part de l'objecte d'aquest contracte que comportin el tractament de dades personals.

f. Mantenir el deure de secret respecte les dades de caràcter personal a les que hagi tingut accés inclús després de que finalitzi el present contracte.

g. Garanteix que els persones autoritzades per tractar les dades personals es comprometen, de forma expressa i per escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents, de les que cal informar-les convenientment.

h. Mantenir a disposició del responsable de tractament de dades la documentació acreditativa del compliment de l'obligació establerta a l'apartat anterior.

i. Garanteix la formació necessària en la matèria de protecció de dades personals de les persones autoritzades per tractar dades personals.

j. Assistir al responsable del tractament de dades en el que es refereix a l'exerció dels drets d'accés, rectificació, supressió i oposició.

k. Correspon al responsable facilitar el dret d'informació en el moment de la recollida de dades.

l. En el moment en que es detecti una violació en la seguretat caldrà realitzar una descripció de la naturalesa de la violació, el nom i les dades de contacte del delegat de protecció de dades i la descripció de les possibles conseqüències de la violació.

m. Donar suport al responsable del tractament de dades en la realització de les avaluacions d'impacte relatives a la protecció de dades.

n. Donar suport al responsable del tractament de dades en la realització de consultes prèvies a l'autoritat de control.

o. Posar a disposició del responsable tota la informació necessària per demostrar el compliment de les obligacions.

p. La implantació de les mesures de seguretat que permetin:

Garantir la confidencialitat, integritat, disponibilitat i resiliència dels sistemes i serveis de tractament.

Restaurar la disponibilitat i l'accés a les dades personals de forma ràpida. Verificar, avaluar i valorar, de forma regular, la eficàcia de les mesures organitzatives implantades per la seguretat del tractament de dades. Xifrar les dades personals.

5. Obligacions del responsable del tractament de dades

El responsable del tractament de dades entregarà les dades que es refereix la clàusula 2 del present document. També realitzarà un avaluació de l'impacte en la protecció de dades personals de les operacions de tractament realitzades per l'encarregat. Per altra banda, també vetllarà del compliment del RGPD per part de l'encarregat. Finalment, supervisarà el tractament de dades, inclosa les inspeccions i les auditories.