Avaluació impacte en protecció de dades del tractament de SIGNATURA BIOMÈTRICA de les sol·licituds per part de la ciutadania

AJUNTAMENT DE FIGUEROLA DEL CAMP

Data: Gener 2025 RAT E.02 – V.28

INDEX

1. INTRODUCCIÓ

La Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPAC), regula les relacions entre els ciutadans i l'Administració amb l'objectiu d'assolir una administració electrònica, millorant l'eficiència i eficàcia de la prestació de serveis públics.

La identitat digital, la signatura electrònica, les evidències són elements imprescindibles per a la seguretat jurídica del procediment administratiu electrònic. L'article 10 (LPAC) estableix que els interessats podran signar a través de qualsevol mitjà que permeti acreditar l'autenticitat de l'expressió de la seva voluntat i consentiment, així com la integritat i inalterabilitat del document.

L'article 12 (LPAC) reconeix el dret dels interessats a ser atesos en l'ús del mitjans electrònics especialment en referència amb la identificació i la signatura electrònica. L'article 13 (LPAC) reconeix el dret de les persones a ser assistides el l'ús de mitjans electrònics en les seves relacions amb les Administracions Públiques, a l'obtenció i utilització de mitjans d'identificació i signatura electrònica i la protecció de dades de caràcter personal.

Per tot això, l'ús d'un sistema de digitalització de signatura biomètrica pot ser admès com un mitjà de signatura electrònica segons l'article 10 (LPAC) de sistemes de signatura admesos per les Administracions Públiques, amb l'especificitat que aquest sistema ha de garantir que les dades personals que tractin s'ajustin al disposat a la legislació vigent en matèria de protecció de dades de caràcter personal.

L'ús de la signatura electrònica biomètrica permet signar electrònicament les sol·licituds per part dels interessats, sense necessitat de disposar d'una identitat digital amb registre previ vinculada a un mecanisme de signatura electrònica.

La Diputació de Tarragona, en el marc dels fons Next Generation ha adquirit tauletes digitals i les llicències de programari necessari per disposar de punts de signatura biomètrica que permeten signar documents i realitzar tràmits per la ciutadania davant les administracions, sense disposar de mecanismes d'identificació i/o signatura digital. Un d'aquests dispositius i la corresponent llicència s'ha facilitat a aquest Ajuntament per tal d'utilitzar-lo en l'atenció a la ciutadania, que davant l'Ajuntament presenti algun tràmit dirigit a qualsevol administració pública.

L'article 35 del REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (endavant RGPD) disposa que quan sigui probable que un tipus tractament, pot comportar **un alt risc per als drets i les llibertats de les persones físiques**, abans del tractament el responsable ha d'avaluar l'impacte de les operacions de tractament en la protecció de dades personals.

En cas que de la valoració resulti que el risc pels drets i llibertats de les persones físiques és elevat, caldrà portat a terme una Avaluació d'impacte relativa a la protecció de dades (endavant AIPD). La AIPD s'haurà de realitzar ABANS del tractament corresponent.

2. BREU DESCRIPCIÓ DEL TRACTAMENT

2.1.- Responsable del tractament.-Aquest Ajuntament

2.2.- Descripció del tractament: Emmagatzematge de documents signats, dades de les persones signants i dades biomètriques de les signatures manuscrites sobre tauletes digitals.

La recaptació de les característiques biomètriques de la signatura manuscrita del signant d'un document es realitza mitjançant el servei VIDsigner BIO utilitzant una tauleta. Les dades biomètriques tractades són la posició, el temps i la pressió de la signatura.

2.3.- Finalitat del tractament.

L'ús de la signatura electrònica biomètrica permet signar electrònica i presencialment les sol·licituds per part dels interessats, sense necessitat de disposar d'una identitat digital en un entorn digital d'expedients electrònics.

La finalitat concreta és garantir la validesa, dels documents signats de forma manuscrita en un entorn digital d'expedients electrònics.

2.4.-Licitud del tractament i compliment normatiu (es a dir quina és la base jurídica que legitima realitzar el tractament):

Article 6 del RGPD	**SI**	**NO**
Art.6.1.a) **Consentiment** Excepció regulada a l'article 9.2.a) del RGPD. Per tal que el consentiment sigui vàlid, s'ha d'informar prèviament a la persona afectada dels aspectes regulats a l'article 13 del RGPD i el consentiment ha de ser voluntari, es a dir, que la falta de consentiment no impedeix a l'afectat fer el tràmit. ***Justificació**: Una vegada omplerta la sol·licitud aquesta es mostra a la persona afectada i es demana el consentiment. Si l'usuari no dona el consentiment té altres alternatives per efectuar la sol·licitud; amb certificat digital, utilitzant l'IDCATmòbil o en format paper (en el cas de persones físiques. El sistema permetrà imprimir la sol·licitud i la persona que no hagi donat el consentiment podrà signar-la manualment), per la qual cosa cal considerar que el consentiment , en el cas que es doni, es dona de forma voluntària*	X	
Art.6.1.c) Obligació legal *Norma amb rang de Llei que legitima el tractament:* art 10,12 i 13 de la Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPAC) Primer tractament: En el moment de la signatura) Article 9.2.f) RGPD. "*el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial*;". Si hi ha una reclamació en la qual la persona nega que hagi signat el document	X	

3. VALORACIÓ SI EL TRACTAMENT REQUEREIX AIPD

Per determinar si el risc és prou significatiu primer hem de **valorar la necessitat de fer una AIPD** mitjançant els recursos que ens proporciona el RGPD:

3.1. Aplica alguns dels supòsits que ens eximeix de fer l'AIPD? (llistat emès per l'AEPD d'acord amb l'article 35.5 RGPD).

Supòsits de l'article 35.5 del RGPD	SI	NO
El tractament té natura, abast context i finalitat semblant a un altre tractament pel qual ja s'ha fet una AIPD		X
El tractament té una base jurídica en el Dret de la UE o d'un estat membre, i s'ha realitzat una AIPD en l'adopció d'aquesta base jurídica.		X
S'inclou en llista orientativa dels tipus de tractament que no requereixen una AIPD de l'article 35.5 del RGPD.		X
El tractament no compleix amb aquests supòsits i per tant **NO EXIMEIX DE FER AIPD**		

3.2. El tractament és troba en algun dels supòsits de **l'article 35.3 RGPD** que sí requereixen una AIPD?:

Supòsits de **l'article 35.3 RGPD**	SI	NO
La finalitat és **l'avaluació "sistemàtica i exhaustiva",** de caràcter **automatitzat**, de diversos aspectes de la persona. **Justificació:** Els dispositius capturen la imatge de la signatura d'una persona, que la identifica de forma inequívoca, així com el traç i totes les característiques que la identifiquen tant a la persona signant i les dades signades	X	
Es pretenen tractar a **gran escala** categories especials de dades o dades personals relatives a condemnes i infraccions penals **Justificació**: Es tractarà dades biomètriques de tots els ciutadans que utilitzin el sistema	X	
Es realitza **l'observació sistemàtica**, a gran escala, de **zones d'accés públic**		X
Si el tractament compleix algun dels supòsits anteriors, **SÍ REQUEREIX AIPD**		

3.4. CONCLUSIONS

3.4.1. Comporta alt risc pels drets i llibertats de les persones físiques?

SI ☒	**NO** ☐

3.4.2. Opinió del DPD respecte a la necessitat de fer l'AIPD:

Per a la implementació d'aquest servei de signatura biomètrica s'observa que compleix amb dos dels supòsits concrets de l'article 35.3 del RGPD i per tant, suposa un alt risc pels drets i llibertats fonamentals dels interessats en matèria de protecció de dades, en aquest sentit, es considera necessari efectuar una AIPD.
Es necessari fer una **AVALUACIÓ D'IMPACTE EN PROTECCIÓ DE DADES?**

SI ☒	**NO** ☐

4. DESCRIPCIÓ SISTEMÀTICA DE LES OPERACIONS DEL TRACTAMENT I DE LES FINALITATS PERSEGUIDES

A) Naturalesa (com es dur a terme el processament)

A.1) Com es recopilen i s'utilitzen les dades

La recaptació de les dades es realitza als punts d'atenció ciutadana de l'Ajuntament (les oficines de registre). Les dades es recapten utilitzant un dispositiu electrònic tipus tauleta, facilitat per la Diputació de Tarragona, que el va adquirir en un Next Generation.

El programari necessari que permeti signar electrònicament documents o realitzar tràmits amb l'administració a la ciutadania també va ser facilitat per la Diputació de Tarragona en el mateix programa Next Generation.

La persona que signa s'identifica davant del treballador municipal, mitjançant la presentació del Document Nacional d'Identitat o document identificació equivalent.

L'aplicació del registre d'entrada es comunica amb el servei VIDsigner BIO (programari facilitat per la Diputació de Tarragona). La captura de les dades es realitza a través d'aquesta eina mitjançant la recollida de les característiques biomètriques de la signatura manuscrita del signant d'un document utilitzant una tauleta (també facilitada per la Diputació de Tarragona).

Es garanteix que el document que es mostra al dispositiu coincideix amb el document que es signa.

En el tractament de dades intervenen diferents serveis al núvol certificats que permeten a l'interessat vincular de forma prèvia el document i recollir la signatura garantint a l'Ajuntament l'autenticitat de la documentació que es signa.

Totes les comunicacions entre la tauleta i els serveis al núvol estan assegurades sota SSL amb certificat SSL de host per a que tota la informació sigui xifrada. Això implica que totes les dades intercanviades de l'usuari es mantenen confidencials.

El procés de signatura es basa en la utilització de tecnologia de signatura electrònica manuscrita i s'empren elements de gran valor com l'obtenció d'elements biomètrics de signatura. Aquests elements estan codificats segons estàndard ISO, certificats digitals i segells de temps i xifrat de les dades biomètriques amb claus custodiades en seu notarial.

Durant el termini temporal que les dades són conservades pel prestador de l'Eina als seus sistemes d'informació aquest aplica mesures de seguretat adients per mantenir les dades xifrades/encriptades i, per tant, inaccessibles inclús per ell mateix.

La documentació es manté emmagatzemada al núvol de Microsoft Azure, que compta amb certificació de nivell alt segons l'Esquema Nacional de Seguretat (ENS) i està adequada al Reglament General de Protecció de Dades.

Un cop signat el document, l'Eina entrega a l'Ajuntament el fitxer amb les dades biomètriques per la seva conservació únicament en els seus sistemes d'informació. Per tant, les dades biomètriques captades de l'Interessat en cap cas són utilitzades per fins d'identificació en grans bases de dades centralitzades, sinó que es conserven xifrades/encriptades i signades electrònicament en els sistemes d'informació de l'Ajuntament. D' acord amb el que hem indicat anteriorment, es fa ús de sistemes de custòdia de les claus de xifrat en seus notarials o similars.

El Servei ofert i els dispositius dels Usuaris estan connectats mitjançant línies de telecomunicacions xifrades.

Un cop l' Ajuntament ha descarregat el document signat, el prestador de l' Eina elimina qualsevol còpia del document i la informació de l' Interessat dels seus sistemes.

Les Dades són objecte de conservació per l'Ajuntament durant el temps necessari segons la finalitat per la qual s'ha recollit la signatura, així com per garantir el dret de l'Ajuntament a demostrar, davant l'autoritat judicial o administrativa competent, l'autoria i autenticitat de la signatura realitzada per l'Interessat respecte al document en qüestió.

Com annex s'adjunta document detallat facilitat per l'empresa proveïdora sobre el funcionament del sistema.

A.2.Encarregats del tractament

La Diputació de Tarragona en tant que ha contractat el servei de manteniment durant 4 anys:

- ✓ Subencarregat del tractament: VID.
- ✓ Altres Subencarregats dels tractaments contractats per VID per prestar-li diversos serveis:
    - FIRMAPROFESIONAL, per la prestació a VID de serveis de emissió de certificats digitals.
    - MICROSOFT IRELAND OPERATIONS LIMITED, per la prestació a VID de serveis de infraestructura tecnològica (AZURE).

A.3.S'utilitzen noves tecnologies

La solució tecnològica emparada és de VIDsigner BIO

B) Àmbit (quines dades es veuen afectades)

B.1.Tipus de dades tractades

S'identifiquen tres categories de dades personals en la fase d'entrada de dades:

● Dades personals bàsiques d'identificació dels signants:

- Nom i cognoms (obligatori)
- NIF (obligatori)
- Correu electrònic (opcional)

● Dades personals especials d'identificació dels signants:

Dades Biomètriques dels trets de comportament de la signatura manuscrita (obligatori): posició, temps i pressió dels trets de la signatura.

● Dades personals de qualsevol naturalesa, bàsics i especials, inclosos en els documents signats

B.2. Persones usuàries?

Qualsevol persona interessada que realitzi tràmits a les oficines del registre municipal i que no disposi de mecanismes d'identificació i/ o signatura digital. Per tal de poder realitzar els tràmits un mitjà alternatiu.

B.3. Durada del tractament

Durant el termini temporal que les dades biomètriques són conservats en el sistema d'informació de VID, aquesta aplica les mesures de seguretat que s'estableixen el document de "VIDsignersecurity". Cal destacar que en tot moment les dades es mantenen xifratges i inaccessible fins i tot per al prestador.

Una vegada signat el document l'eina VIDsigner BIO lliura a l'Ajuntament el fitxer amb les dades biomètriques xifrades per a la seva conservació en el seu sistema d'informació. L'Ajuntament conservarà les dades aplicant el termini definit a les TAAD corresponent a cada tràmit i a l'expedient administratiu.

C. Context:

C.1. Entorn normatiu

✓ El Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica y els serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE, en endavant Reglament eIDAS

✓ REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (endavant RGPD)

✓ Directriu 5/2020 sobre el consentiment en el sentit del Reglament (UE) 2016/679 del Comitè Europeu de Protecció de Dades (CEPD)

✓ La Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPAC)

✓ Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals

✓ RD 311/2022 de 3 de maig pel que es regula l'Esquema Nacional de Seguretat (ENS)

C.2. Cessió de les dades

Les dades no es comuniquen a tercers excepte a l'autoritat administrativa o judicial que els sol·liciti i en els casos en què s'hagi de complir amb una obligació legal.

C.3. Transferències internacionals

Les dades es conserven en la UE.

D. Finalitat

D.1. Finalitat principal. La finalitat perseguida pel sistema de signatura manuscrita sobre un suport electrònic és garantir la validesa dels documents signats de forma manuscrita en un entorn digital d'expedients electrònics.

D.2. **Efectes previstos per a les persones**

Els **principals riscos identificats** són l'accés a les dades biomètriques xifrades i emmagatzemades en el document signat.

Utilització, per part de tercers, de les dades biomètriques amb altres finalitats.

D.3. **Beneficis per l'usuari i per a la societat en el seu conjunt**

Els usuaris que no disposin de certificat electrònic o clau concertada podran presentar i signar electrònicament els documents presentats a les oficines de registre municipals.

Assolir una administració electrònica, millorant l'eficiència i eficàcia de la prestació de serveis públics de tal manera que hi pugui accedir qualsevol persona.

5. NECESSITAT, IDONEITAT I PROPORCIONALITAT DEL TRACTAMENT

5.1 Judici d'idoneïtat

Es considera que el tractament és idoni per a la signatura de documents electrònics, en tant que el mateix és un mitjà útil i de confiança per a permetre identificar a l'autor de la signatura d'un document electrònic i poder demostrar fefaentment, si cal, en un futur davant l'autoritat judicial corresponent, l'autoria de la mateixa (autenticitat) així com la integritat del document signat (integritat).

Per tant, la finalitat perseguida pel sistema de signatura manuscrita sobre un suport electrònic, ofereix a l'Ajuntament i als usuaris dels seus serveis, una seguretat jurídica en el món digital que, des de la perspectiva del dret de protecció de dades, fa que sigui idònia, legítima i justificada.

5.2 Judici de necessitat

La utilització de documents electrònics i en conseqüència de la signatura electrònica és, avui dia una necessitat, sent l'ús de sistemes de signatura biomètrica l'única opció de signatura electrònica possible per als casos en els quals el signant no compta amb els mitjans tecnològics necessaris per a emprar altres tecnologies de signatura (com el certificat digital).

La finalitat del tractament no es pot aconseguir raonablement per altres mitjans, és a dir, no es disposa d'una alternativa a la signatura biomètrica en el marc del procediment administratiu que garanteixi amb igual eficàcia, en seu judicial, l'obtenció d'una prova robusta i segura d'una signatura, com els serveis de signatura electrònica manuscrita .

5.3 Judici de proporcionalitat

Sobre aquest tema entenem que la ingerència produïda en la privacitat de l'usuari és la mínima possible, atès que el sistema capta els mínims trets biomètrics (principi de minimització de dades per defecte i des del disseny del sistema) exclusivament per demostrar a l'autor de la signatura.

5.4 Opinió dels interessats

El RGPD estableix que, si és possible, cal recollir l'opinió dels interessats sobre la necessitat i la proporcionalitat del tractament. Aquesta opinió no s'ha recollit perquè la identificació dels interessats és una obligació legal en els tràmits administratius i a més l'ús d'aquest sistema serà totalment voluntària, tenint l'usuari altres alternatives.

6. CONTROLS PER GARANTIR EL COMPLIMENT DELS PRINCIPIS I DELS DRETS

6.1.Controls dels principis

L'article 5 del RGPD regula tota una sèrie de principis que l'Ajuntament ha d'aplicar als tractaments de dades personals que porti a terme.

6.1.1 Limitació de la finalitat

6.1.2 Licitud i lleialtat

6.1.3. Minimització

6.1.4. Limitació del termini de conservació

6.1.5. Exactitud de les dades

6.1.6. Seguretat (ENS)

6.1.1. Finalitat del tractament:

D'acord amb la legislació vigent, les dades recollides s'han d'utilitzar per a assolir la finalitat del tractament que va motivar la recollida, és a dir, les dades s'han de recollir amb fins determinats, explícits i legítims, i no hauran de ser tractats ulteriorment de manera incompatible amb aquests fins.
El tractament de la signatura biomètrica objecte d'aquest anàlisi **solament serà utilitzat per la finalitat per la qual es recapta**: garantir la validesa legal del document signat de forma manuscrita en un entorn digital d'expedients electrònics. La signatura biomètrica solament s'utilitzarà en les oficines de registre per tal que les persones que no disposin de signatura electrònica puguin presentar escrits a l'administració de forma electrònica

6.1.2. Principis de licitud i lleialtat

Les dades s'han de tractar de manera lícita, lleial i transparent en relació amb l'interessat. Per tal que el tractament sigui **lícit** cal d**isposar d'una base jurídica sobre la qual es sustenten els tractaments realitzats sobre les dades.** Un tractament **és lleial** si fa un ús de les dades previsible per part dels interessats, i del tractament no se'n deriven conseqüències adverses pels interessats que no siguin justificables.
Cal entendre que el tractament gaudeix de suficient legitimació, tal i com es detalla al punt 3.4 d'aquest document. Art.6.1.a) **Consentiment** Excepció regulada a l'article 9.2.a) del RGPD. Per tal que el consentiment sigui vàlid, s'ha d'informar prèviament a la persona afectada dels aspectes regulats a l'article 13 del RGPD i el consentiment ha de ser voluntari, es a dir, que la falta de consentiment no impedeix a l'afectat fer el tràmit. ***Justificació**: Una vegada omplerta la sol·licitud aquesta es mostra a la persona afectada i es demana el consentiment. Si l'usuari no dona el consentiment té altres alternatives per efectuar la sol·licitud; amb certificat digital, utilitzant l'IDCATmòbil o en format paper (en el cas de persones físiques. El sistema permetrà imprimir la sol·licitud i la persona que no hagi donat el consentiment podrà signar-la manualment), per la qual cosa cal considerar que el consentiment , en el cas que es doni, es dona de forma voluntària.* Art.6.1.c) Obligació legal *Norma amb rang de Llei que legitima el tractament:* art 10,12 i 13 de la Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques (LPAC) I pel que fa a les excepcions de l'article 9.2 del RGPD, cal entendre que la persona interessada donarà el consentiment de forma voluntària ja que en altre cas podrà presentar la sol·licitud per altres mitjans. També cal considerar que el tractament **és lleial** donat que es recull com a identificació de la persona en el tràmit en que aquesta participa, no fent-se cap ús diferent del derivat de la seva associació – voluntària o per imperatiu legal – al procediment administratiu on signa la documentació

6.1.3. Principi de minimització

Les dades han de ser adequades, rellevants i limitades a l'estrictament necessari per acomplir la finalitat del tractament
Les dades tractades són: Nom i cognoms, DNI , e-mail (voluntari) i signatura manuscrita
Es recull la informació mínima per identificar de forma inequívoca a les persones, deslligant la seva gestió del contingut dels procediments administratius i evitant accés no autoritzat ni necessari per part dels proveïdors del sistema

6.1.4. Principi de limitació de conservació

Les dades personals no s'han de conservar més temps de l'estrictament necessari per complir amb la finalitat del tractament.
Una vegada signat el document l'eina VIDsigner BIO lliura a l'Ajuntament el fitxer amb les dades biomètriques xifrades per a la seva conservació en el seu sistema d'informació. El temps de conservació de les dades està vinculat als tràmits on s'utilitza per a la identificació de les persones signants. El temps de conservació bé definit per la TAAD corresponent a cada tràmit i expedient administratiu o al Registre d'Activitats de Tractament Les dades de la signatura biomètrica NO es conservaran amb finalitat d'arxiu en interès públic, amb finalitat d'investigació científica o històrica, o amb finalitat estadística

6.1.5. Principi d'exactitud

El principi d'exactitud estableix que les dades han de ser exactes i que el responsable de les dades ha de prendre mesures raonables per garantir que les dades siguin exactes i s'actualitzin, rectifiquin o s'esborrin sense dilació.
El procediment administratiu pel qual es recull la signatura associada al document es realitza pel personal municipal encarregat del Registre d'entrada, a les oficines municipals, davant el qual la persona sol·licitant s'identifica

6.1.6.Principi de seguretat

Segons la Disposició Addicional Primera de la Llei Orgànica 3/2018 de Protecció de dades i garanties dels drets digitals, l'Ajuntament en els tractaments de dades personals que porti a terme com a responsable ha d'adoptar les mesures de seguretat que corresponguin de les previstes a l'ENS. L'article 3.3. del RD 311/2022 disposa que en tot cas prevaldran les mesures a implantar com a conseqüència de l'anàlisi de riscos en el cas de resultar agreujades de les previstes al RD 311/2022
Les tauletes i les llicències han sigut adquirides i facilitades per la Diputació de Tarragona, per la qual cosa es considera que s'han adquirir un equipament i un sistema que reuneix els requisits de seguretat adients, que disposen de les mesures de seguretat adients. A més a més solament es faran servir per la signatura de documents i tràmits presentats al registre municipal. El procés de signatura es basa en la utilització de tecnologia de signatura electrònica manuscrita i s'empren elements de gran valor com l'obtenció d'elements biomètrics de signatura. Aquests elements estan codificats segons estàndard ISO, certificats digitals i segells de temps i xifrat de les dades biomètriques amb claus custodiades en seu notarial.

Durant el termini temporal que les dades són conservades pel prestador de l'Eina als seus sistemes d'informació aquest aplica mesures de seguretat adients per mantenir les dades xifrades/encriptades i, per tant, inaccessibles inclús per ell mateix. La documentació es manté emmagatzemada al núvol de Microsoft Azure, que compta amb certificació de nivell alt segons l'Esquema Nacional de Seguretat (ENS) i està adequada al Reglament General de Protecció de Dades

6.2.Controls dels drets

Als articles 12 i següents del RGPD es regulen els drets de les persones interessades en protecció de dades. Per a garantir el compliment d'aquest drets tot seguit s'enumeren una sèrie de mesures o controls a aplicar:

6.2.1. Dret d'informació

Facilitar la informació en matèria de protecció de dades i redactar-la de forma accessible i fàcil d'entendre
L'interessat abans de signar cal que doni el consentiment per al tractament de les seves dades personals. En el moment de donar el consentiment pot desplegar la informació relativa al tractament.

6.2.2. Drets d'autodeterminació informativa

Garantir l'exercici dels drets de les persones afectades, d'acord amb l'article 15 i següents del RGPD
A l'espai catàleg de tràmits l'Ajuntament té habilitat els tràmits per l'exercici dels drets en protecció de dades i disposa d'unes instruccions internes per a tramitar el procediment de l'exercici dels drets

7. AVALUACIÓ DELS RISCOS PER ALS DRETS DELS INTERESSATS

A continuació s'avalua i identifiquen els possibles efectes negatius sobre les persones derivats del tractament de dades motiu de l'avaluació.

L'anàlisi de riscos s'ha portat a terme considerant el tractament i el cicle de vida de les dades.

El risc s'ha determinat considerant dos factors:

- Impacte sobre la intimitat i la privacitat de les persones
- Probabilitat que succeeixi

El risc es determina com a resultat directe de l'impacte i de la probabilitat

7.1 Impacte

L'impacte del tractament s'avalua analitzant en la pèrdua de la confidencialitat, de la integritat i de la disponibilitat de les dades personal sobre els interessats en determinats escenaris.

Amb el següent criteri:

IMPACTE	DESCRIPCIÓ
Menyspreable (baix)	Poc o cap efecte
Limitat (mig)	Els efectes se senten però no són crítics
Significatiu (alt)	Impacte seriós en el curs d'acció i el resultat
Màxim (Molt alt)	Podria resultar un desastre

Per a cadascuna de les dimensions de seguretat:

Confidencialitat: accés no autoritzat o difusió pública

Els escenaris contemplats atès el tractament i sistema empleat són:

- ✓ Pèrdua o robatori d'una tableta amb la informació dels usuaris.
- ✓ Vulneració del canal de comunicació.
- ✓ Enviament per error de dades personals a sistemes diferents del definit.
- ✓ Possibilitat d'accedir de forma no autoritzada al servidor vCloud.
- ✓ Difusió no autoritzada de la informació en servidor vCloud.
- ✓ Robatori d'informació (lògica o física) dels servidors de l'encarregat del tractament.
- ✓ Accés per perfils no autoritzats per error de configuració o permisos.

Impacte: Limitat (mig)

Justificació:

Les dades es delimiten a dades identificatives i dades biomètriques però aquestes es delimiten a la signatura manuscrita que la seva difusió no suposaria un impacte significatiu en la privacitat i intimitat de les persones.

Integritat: modificació no autoritzat de les dades

Els escenaris contemplats atès el tractament i sistema empleat són:

- ✓ Modificació errònia accidental o intencionada de les dades per part de personal autoritzat.
- ✓ Error en les comunicacions impliquen alteració de les dades entre la tableta i el servidor vCloud o bé en les consultes des de l'Ajuntament.
- ✓ Modificació per un atac cibernètic.

Impacte: Limitat (mig)

Justificació:

L'afectació de la integritat de les dades podria afectar a la identificació correcta de l'usuari associat a l'inici d'un expedient administratiu. Això pot causar problemes principalment en l'àmbit del dret administratiu i puntualment molèsties a la ciutadania, però no afectació sobre la intimitat i privacitat d'aquests

Disponibilitat: impossibilitat d'accés a les dades

Els escenaris contemplats atès el tractament i sistema empleat són:

- ✓ El servei deixa d'estar disponible (caiguda del hosting per diverses causes: problema de comunicacions, programari, maquinari, alimentació elèctrica, etc.)
- ✓ La informació es va malbé i no hi ha possibilitat de recuperació.

Impacte: Baix

Justificació:

La no disponibilitat de la informació no suposa un impacte significatiu per a les persones atès que el servei que es lliura és d'emmagatzematge de validació de procediments i expedients iniciats i/o finalitzats.

Aquesta indisponiblitat no afecta al funcionament organitzatiu ni als procediments administratius del ciutadà. Si es requereix aquesta identificació prèvia hi han mecanismes legals que ho poden suplir.

L'impacte resultant és el major dels tres:

Limitat (mig)

7.2 Probabilitat inicial

La probabilitat es determina de l'exposició, tecnologia empleada i l'organització:

Paràmetre	Valor
TECNOLOGIA	
El sistema de tractament està connectat a sistemes externs a l'organització?	**SI**
Alguna part del tractament es fa a través d'internet?	**SI**
Manca de seguiment d'un document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?	**SI**
Manca de seguiment d'un document de bones pràctiques rellevant en el manteniment, la monitorització i la resposta a incidents del sistema de tractament?	NO
Hi ha una manca de seguretat física a les instal·lacions on té lloc el tractament?	NO
ÚS DEL SISTEMA DE TRACTAMENT	
Hi ha una manca de claredat en la definició dels rols i les responsabilitats dels treballadors?	**SI**
Hi ha manca de claredat en la definició dels usos acceptables dels sistemes de tractament?	NO
Pot el personal connectar dispositius externs al sistema?	NO
Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?	**SI**
PERSONES QUE INTERVENEN EN EL TRACTAMENT	
El personal rep permisos que no són necessaris per complir les tasques que té encomanades?	**SI**
S'ha externalitzat alguna part del tractament a un encarregat?	**SI**
Hi la una manca de coneixement del personal respecte de l'ús adequat del sistema d'aspectes de seguretat de les dades o de les limitacions d'ús que imposa el RGPD?	NO
ALTRES CARACTERÍSTIQUES	
Ha patit l'empresa o altres empreses del sector atacs darrerament?	NO
S'han rebut queixes d'alguna persona respecte de l'establiment o la seguretat del sistema de tractament darrerament?	NO
Es tracten dades especials o dades d'un nombre molt gran d'usuaris?	NO

Es calcula la probabilitat en funció del nombre de respostes afirmatives i d'acord el següent criteri:

TIPUS DE PROBABILITAT	DESCRIPCIÓ	Respostes Afirmatives
Menyspreable (molt remota)	És improbable que tingui lloc el risc	0-3
Limitada (Poc probable)	És possible que tingui lloc el risc.	4-8
Significativa (Possible)	Risc molt probable en la comissió d'Infracció	8-12
Màxim (Molt Alta)	**Alta probabilitat que succeeixi**	**Més de 12**

Probabilitat resultant de 7 respostes afirmatives és:

Limitada (poc probable)

7.3 Risc inicial

El risc potencial es determina com a resultat directe de l'impacte i de la probabilitat

RISC = IMPACTE X PROBABILITAT

D'acord la següent taula:

		IMPACTE			
		Menyspreable	Limitat	Significatiu	Màxim
PROBALITAT	Màxim	Mig	Alt	Molt alt	Molt alt
	Significatiu	Mig	Mig	Alt	Molt alt
	Limitat	Baix	Mig	Mig	Alt
	Menyspreable	Baix	Baix	Mig	Mig

El tractament de digitalització de signatura manuscrita el risc detectat és **MIG**

8. MESURES TÈCNIQUES, ORGANITZATIVES I DE SEGURETAT

A fi de mitigar els riscos derivats de les amenaces detectades es determinen les següents mesures per tal de mitigar els riscos detectats

Aquestes mesures s'han d'implantar i valorar la seva eficàcia per detectar desviacions. Es recomana revisar-les en una periodicitat mínima d'un any, i en tot cas, sempre que es produeixi alguna violació de seguretat que afecti a dades personals. Tanmateix s'hauria de tornar a valorar els riscos en casos modificacions substancials del tractament

8.1. Mesures tècniques i organitzatives

Permisos i control d'accessos:

- Les tauletes **únicament** s'utilitzaran en les oficines d'atenció al ciutadà per la signatura de documents o tràmits que els dirigeixin a alguna administració pública.

- Les taules no sortiran de l'edifici municipal i estaran sota la custodia del funcionari encarregat del registre.

- El treballador responsable de la custodia dels dispositius signarà l'acord de confidencialitat

- Atribució responsabilitats i rols als treballadors que hagin de fer servir el sistema

- Es realitzarà formació capacitació personal i càrrecs electes

- Supervisió dels encarregats

- Canals habilitats i accessibles per a l'exercici dels drets d'autodeterminació informativa

- Registre de queixes i suggeriments

- El ciutadà s'identificarà davant el funcionari que l'atengui en les oficines d'atenció ciutadana. El treballador municipal li oferirà signar el tràmit amb certificat digital (si en disposa), o en el cas de no disposar també serà possible imprimir la sol·licitud i signar-la manualment.

8.2.Mesures de seguretat

Les mesures de seguretat seran les derivades de l'ENS. El sistema és el seleccionat i facilitat per la Diputació de Tarragona i es connectarà amb el gestor documental .

9. RISC RESIDUAL

L'aplicació de les mesures definides sobre el tractament impliquen una reducció del rics. L'impacte no variaria, que ja es troba minimitzat per tipus de tractament i dades, garantint les mesures l'increment de la confidencialitat, integritat i disponibilitat.

En canvi la Probabilitat, en els punts sensibles detectats resultaria

PARÀMETRE	**VALOR**
TECNOLOGIA	
El sistema de tractament està connectat a sistemes externs a l'organització?	**SI**
Mesures correctives: - La connexió es realitza mitjançant comunicacions segures. - Els sistemes estan allotjats a un hosting dins de l'UE que compta amb certificacions de seguretat ISO 27000 i ENS	
Alguna part del tractament es fa a través d'internet?	**SI**
Mesura correctiva: - La connexió es realitza mitjançant comunicacions segures, creant una xarxa privada virtual (VPN)	
ÚS DEL SISTEMA DE TRACTAMENT	
Manca de seguiment d'un document de bones pràctiques rellevant en el disseny o la configuració del sistema de tractament?	**SI**
Mesures correctives: -El sistema (tables i app) van ser adquirides per la Diputació de Tarragona dintre d'una subvenció next generation i ha sigut la Diputació qui es va encarregar de la seva configuració	
Manca un procediment adequat de registre i supervisió de les activitats relacionades amb el tractament?	**SI**
Mesures correctives: - Implantació de gestió d'usuaris a l'Ajuntament -Regulació els usos de les tauletes: al tractar-se d'una subvenció de la Diputació les condicions de l'ús ja ven imposables que solament s'ha de destinar a la signatura de documents presentats al registre municipal -Les taules no sortiran de l'edifici municipal	
PERSONES QUE INTERVENE EN EL TRACTAMENT	
El personal rep permisos que no són necessaris per complir les tasques que té encomanades? S'ha externalitat alguna part del tractament a un encarregat?	**SI**
Mesura correctiva: --Atribució de rols i responsabilitats -Formació i capacitació	

S'ha externalitzat alguna part del tractament a un encarregat?	**SI**
Mesura correctiva: - Regulació del tractament mitjançant acord de confidencialitat. - Acord de nivell de serveis per garantir la seguretat i disponibilitat	

Finalment el risc residual final, aplicant les mesures definides seria:

Impacte Residual	Limitat
Probabilitat Residual	Menyspreable
Risc residual	Baix

Atès el risc residual existent amb les pròpies mesures aplicades pel sistema no és necessària la comunicació i consulta a l'Autoritat Catalana de Protecció de Dades

Figuerola del Camp a, 31 de gener de 2025

L'Alcalde

10. ANNEX: Detall sobre el funcionament del sistema facilitat per l'empresa proveïdora

INFORME-GUIA PARA LA REALIZACIÓN DE LA EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS (EIPD) POR PARTE DE LOS CLIENTES DE VALIDATED ID, SL RESPECTO AL TRATAMIENTO DE DATOS BIOMÉTRICOS MEDIANTE EL USO DEL SERVICIO VIDSIGNER BIO

SA-MAN-R-2019-0001 v.1.1

Validated ID
Always be yourself

Document Control

Change Record

DATE	AUTHOR	VERSION	CHANGE REFERENCE
30-ene-20	David Gracia (DPO), Xavier Vila (CISO) Ramón Bernabeu (Legal Manager)	1.0	Versión inicial
14-dic-20	Ramón Bernabéu (DPO)	1.1	Cambio DPO y correcciones

Distribution

DISTRIBUTION	
Owner:	Validated ID, S.L.
Distribution:	Internal, Clients
Permission:	Confidencial

Signatures

AUTHOR	
Name:	David Gracia
Title:	DPO
Signature:	

REVIEW	
Name:	Xavier Vila
Title:	CISO
Signature:	

APROVAL	
Name:	Fernando Pino Sola
Title:	CLO
Signature:	

Contenido

1 Introducción

El presente informe es una guía para ayudar a la realización, por parte de los clientes de Validated ID, SL (en adelante, VID), de una Evaluación de Impacto en la Protección de Datos del tratamiento de los datos biométricos derivado del uso del servicio VIDsigner suministrado por VID, el cual está basado en el "Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para Administraciones Públicas" publicado por la AEPD (versión de 9 de julio de 2019), el cual se orientó a cumplir con las previsiones del Reglamento General de Protección de Datos (RGPD), y que incluye, entre las obligaciones del responsable del tratamiento, la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de datos personales cuando resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas.

Así, el RGPD regula dicha evaluación de impacto relativa a la protección de datos (EIPD), la cual tiene por finalidad valorar la particular gravedad y probabilidad de un alto riesgo de los derechos y libertades de las personas físicas debido al tratamiento de datos personales que se lleve a cabo en una entidad.

VID no está obligada a realizar la EIPD pues sus actividades de tratamiento de datos, en calidad de responsable de los tratamientos, no están expuestas a riesgos relevantes que motiven la necesidad de realizarla, es decir, son tratamientos de bajo riesgo. Sin embargo, hay que observar, que según el considerando 95 del RGPD *"El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control"*, y, conforme al artículo 28 del RGPD, entre las obligaciones de dicho encargado, se señala que *"ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado".*

Y como ya se ha dicho, en tanto que VID también realiza tratamientos de datos personales derivados de los servicios prestados a clientes (servicios de firma electrónica), gestiona datos por cuenta del responsable en su calidad de encargado del tratamiento. Uno de dichos tratamientos es el basado en el uso de datos biométricos mediante la herramienta "VIDsigner BIO", que es considerado un tratamiento que puede implicar un alto riesgo de los derechos y libertades de personas físicas.

Aunque VID, conforme al art. 35.1[1] RGPD, no está obligada a la realización de una EIPD en relación a dicho tratamiento (pues no es la responsable de dicho tratamiento, sino que lo son sus clientes) llevar a cabo la ayuda y soporte al responsable es una medida de responsabilidad proactiva en su calidad de encargado, con el objeto de ayudar a estudiar en profundidad dichos tratamientos y sus procesos asociados necesarios para la consecución de los objetivos de sus clientes, siempre teniendo en cuenta que estos son los que determinan los fines y medios de los mismos, y por ello, son responsables del tratamiento.

[1] "1.Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares."

Por ello, el presente informe es el resultado de dicho trabajo de ayuda para la realización de un análisis de riesgos del tratamiento que deben llevar a cabo los responsables, el cual es necesario para la utilización del servicio VIDsigner BIO, con el objeto de analizar los riesgos de protección de datos y seguridad del tratamiento de datos, que deberá abordar los riesgos normativos del tratamiento en cuanto a los fines legítimos del mismo y al juicio de necesidad y proporcionalidad del tratamiento, evaluación que es competencia y responsabilidad de los responsables del tratamiento, en virtud del referido art. 35.1 del RGPD.

2 Resumen ejecutivo

Este resumen debe tratar de forma condensada los aspectos más significativos de los capítulos que se desarrollan a lo largo del documento

Contendrá la identificación del responsable-RGPD del tratamiento, de la unidad responsable en la organización, unidades gestoras de los datos que intervienen en alguna de las fases del tratamiento, encargados del tratamiento y subencargados del tratamiento.

A su vez, incluirá una breve descripción del tratamiento, su finalidad, las principales categorías de datos y su planeada implementación.

También destacará los factores de riesgo que motivan la realización de la EIPD y, en caso de no ser necesaria la EIPD, una exposición de los motivos por los que el responsable decide llevar a cabo la EIPD.

Finalmente, incluirá una breve descripción sobre el contexto de la EIPD como la metodología utilizada, la extensión y límites de la EIPD, los principales riesgos de privacidad identificados, los beneficios del tratamiento, las soluciones de gestión y técnicas planeadas, el análisis coste-beneficio y las conclusiones derivadas del riesgo residual y, en particular, la necesidad de realizar o no realizar una consulta previa a la AEPD.

Así, esta información puede resumirse del modo siguiente:

2.1 Aspectos más significativos de los capítulos que se desarrollan a lo largo del informe EIPD

Los aspectos más significativos de los capítulos que se desarrollan a lo largo del informe EIPD son los siguientes:

- Descripción (desde la recogida hasta la destrucción de los datos) y contexto del tratamiento (licitud, necesidad y proporcionalidad);
- Identificación, valoración y gestión de riesgos;
- Conclusión (plan de acción) y validación (conclusión favorable o no favorable).

2.2 Identificación de los Roles en el tratamiento de datos

- Responsable del tratamiento: los clientes de VID que contratan los servicios VIDsigner BIO.

- Unidad responsable dentro de los clientes (responsables del tratamiento): pueden ser, en la mayoría de los casos, las unidades de datos, seguridad, asesoría jurídica.

- Unidades gestoras de los datos que intervienen en alguna de las fases del tratamiento: unidades ventas y atención al cliente.

- Encargados del tratamiento: VID, en la mayoría de los casos, aunque VID puede ser identificada también como subencargado del tratamiento en aquellos supuestos que una empresa externa de servicios del responsable del tratamiento es la que subcontrate a VID los servicios VIDsigner BIO.

- Subencargados del tratamiento contratados por VID para prestarle diversos servicios:

- FIRMAPROFESIONAL, para la prestación a VID de servicios de emisión de certificados digitales.
- MICROSOFT IRELAND OPERATIONS LIMITED, para la prestación a VID de servicios de infraestructura tecnológica (AZURE).

2.3 Breve descripción del tratamiento, su finalidad, las principales categorías de datos y su planeada implementación

El responsable deberá indicar la siguiente información:

Descripción del tratamiento: recogida de los rasgos biométricos de la firma manuscrita del firmante de un documento mediante el servicio VIDsigner BIO utilizando un dispositivo electrónico tipo "tablet". Dichos datos son la posición, tiempo y presión de los rasgos de la firma.

Finalidad del tratamiento: que el responsable o el interesado puedan identificar, con las máximas garantías de seguridad jurídica, al autor de la firma y demostrar, en caso de litigio, la autoría y autenticidad de la firma. En el servicio VIDsigner Bio el proceso de firma se basa en la utilización de tecnología de firma electrónica manuscrita y emplea elementos de gran valor como la obtención de elementos biométricos de la firma codificados según estándar ISO, certificados digitales y sellos de tiempo, cifrado de los datos biométricos con claves custodiadas en sede notarial, entre otros.

Categorías de datos que se obtienen mediante VIDsigner Bio: Datos especiales de tipo biométricos

Implementación del tratamiento: se encuentra implementado en la actualidad por el responsable/no se encuentra implementado en la actualidad por el responsable.

2.4 Factores de riesgo que motivan la realización de la EIPD

Conforme al art. 35 RGPD, el responsable del tratamiento está obligado a la realización de una EIPD en relación a los tratamientos que realiza, dado que existen factores de riesgo, como es el recabo de datos biométricos de personas físicas, considerados como categorías especiales de datos por el art. 9 del RGPD.

2.5 Breve descripción sobre el contexto de la EIPD

Metodología utilizada

El responsable debe escoger una metodología para llevar adelante la EIPD, por ejemplo las basadas en las siguientes guías:

- "Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD" (Agencia de Protección de Datos Española).
- "Guía práctica para la Evaluación de impacto relativa a la Protección de datos" (Autoridad Catalana de Protección de Datos)

Extensión y límites de la EIPD

La EIPD se extiende a todo el proceso del tratamiento de los datos biométricos.

Principales riesgos de privacidad identificados

Acceso a los rasgos biométricos cifrados y almacenados en el documento firmado.

Beneficios del tratamiento

El beneficio del tratamiento lo constituye la obtención de las máximas garantías de seguridad jurídica de la autenticidad de la autoría de las firmas realizadas por los interesados en los documentos firmados que presentan al responsable del tratamiento.

Soluciones de gestión y técnicas planeadas

El responsable recaba los datos mediante la herramienta VIDsigner BIO.

Una vez firmado el documento dicha herramienta VIDsigner BIO entrega al responsable el fichero con los datos biométricos cifrados para su conservación en su sistema de información.

Durante el plazo temporal que los datos biométricos son conservados en el sistema de información de VID, esta aplica las medidas de seguridad que se establecen el documento de "VIDsigner security" (Anexo II). Hay que destacar que en todo momento los datos se mantienen cifrados e inaccesible incluso para el prestador.

Análisis coste-beneficio y las conclusiones derivadas del riesgo residual y, en particular, la necesidad de realizar o no realizar una consulta previa a la AEPD

El análisis coste-beneficio realizado justifica el tratamiento legítimo de los datos:

Se indicará un resumen del juicio de proporcionalidad en sentido estricto (apartado 8c).

Se debe indicar un resumen de las conclusiones del riesgo.

3 Descripción del tratamiento

3.1 Fecha de realización de la EIPD

Fecha:	….

a.

3.2 Nombre y descripción del Tratamiento

Nombre del tratamiento: VIDsigner BIO.

Identificación de la versión del tratamiento respecto al cual se realiza la EIPD:

Versión del tratamiento:	……

Historial de cambios realizados sobre el mismo en cada una de las etapas del mismo:

Historial de cambios			
Versión	Fecha	Descripción de la acción	Etapa del tratamiento
1.0		Creación del tratamiento	---

Identificación del responsable del tratamiento: los clientes de VID que contratan los servicios VIDsigner BIO.

Identificación de la unidad responsable dentro de los clientes (responsables del tratamiento): pueden ser, en la mayoría de los casos, las unidades de datos, seguridad y asesoría jurídica.

Identificación de unidades gestoras de los datos que intervienen en alguna de las fases del tratamiento: unidades ventas y atención al cliente.

Identificación de encargados del tratamiento: VID, en la mayoría de los casos, aunque VID puede ser identificada también como subencargado del tratamiento en aquellos supuestos que una empresa externa de servicios del responsable del tratamiento es la que subcontrate a VID los servicios VIDsigner BIO.

Identificación de subencargado/s del tratamiento contratados por VID para prestarle diversos servicios:

- FIRMAPROFESIONAL, para la prestación a VID de servicios de firma electrónica.

- MICROSOFT IRELAND OPERATIONS LIMITED, para la prestación a VID de servicios de infraestructura tecnológica (AZURE).

Descripción del tratamiento: recogida de los rasgos biométricos de la firma manuscrita del firmante de un documento mediante el servicio VIDsigner BIO utilizando un dispositivo electrónico tipo "tablet".

Finalidad del tratamiento: que el responsable o el interesado puedan identificar, con las máximas garantías de seguridad jurídica, al autor de la firma y demostrar, en caso de litigio, la autoría y autenticidad de la firma. En el servicio VIDsigner Bio el proceso de firma se basa en la utilización de tecnología de firma electrónica manuscrita y emplea elementos de gran valor como la obtención de elementos biométricos de la firma codificados según estándar ISO, certificados digitales y sellos de tiempo, cifrado de los datos biométricos con claves custodiadas en sede notarial, entre otros.

Categorías de datos que se obtienen mediante VIDsigner Bio: Datos especiales de tipo biométricos

Implementación del tratamiento: se encuentra implementado en la actualidad por el responsable/no se encuentra implementado en la actualidad por el responsable.

Categorías de datos personales: Se trata de datos biométricos. Dichos datos son la posición, tiempo y presión de los rasgos de la firma.

Categorías de interesados: Personas físicas firmantes de un documento electrónico utilizando el servicio VIDsigner BIO para ser presentando ante el responsable del tratamiento.

Implementación del tratamiento: se encuentra implementado en la actualidad/ no se encuentra implementado en la actualidad.

Categorías de destinatarios a quienes se comunican los datos personales: los datos no se comunican a terceros salvo a la autoridad administrativa o judicial que los solicite y en los casos en que haya una obligación legal.

Transferencias internacionales datos personales: los datos no se comunican a terceros países.

Plazos previstos para la supresión de las diferentes categorías de datos: los datos proporcionados son objeto de conservación durante el tiempo necesario para garantizar el derecho del responsable de demostrar, ante la autoridad judicial o administrativa competente, la autoría y autenticidad de la firma realizada en su documento presentado por un ciudadano al responsable del tratamiento con el objeto de evitar cualquier responsabilidad que se pudiera derivar de reclamaciones o acciones interpuestas ante dicho responsable.

Descripción general de las medidas técnicas y organizativas de seguridad: El responsable debe indicar las medidas técnicas y organizativas de seguridad del tratamiento.

Durante el plazo temporal que el tratamiento de los datos biométricos es realizado por VID esta aplica las medidas de seguridad que se establecen en el documento de "VIDsigner security"

3.3 Categorías de Datos del Tratamiento

Se trata de datos biométricos. Dichos datos son la posición, tiempo y presión de los rasgos de la firma.

3.4 Identificación del Responsable-RGPD

Identificación del responsable del tratamiento: los clientes de VID que contratan los servicios VIDsigner BIO.

Identificación del Delegado de Protección de Datos del Responsable: ….

Identificación de la unidad responsable dentro del Responsable: pueden ser, en la mayoría de los casos, las unidades de datos, seguridad y asesoría jurídica.

Identificación de unidades gestoras de los datos que intervienen en alguna de las fases del tratamiento dentro de la organización del Responsable: unidades de atención al cliente.

3.5 Identificación de terceros implicados en el tratamiento

Identificación de encargados del tratamiento: VID, en la mayoría de los casos, aunque VID puede ser identificada también como subencargado del tratamiento en aquellos supuestos que una empresa externa de servicios (partner tecnológico) del responsable del tratamiento es la que subcontrate a VID los servicios VIDsigner BIO.

Identificación del Delegado de Protección de Datos de VID: .....

Identificación de subencargado/s del tratamiento contratados por VID para prestarle diversos servicios tecnológicos:

- FIRMAPROFESIONAL, para la prestación a VID de servicios de firma electrónica.
- MICROSOFT IRELAND OPERATIONS LIMITED, para la prestación a VID de servicios de infraestructura tecnológica (AZURE).

3.6 Contexto interno del tratamiento en la entidad

Indicar la estructura del responsable, funciones y competencias: ……

Indicar las características de las personas de la organización implicadas en el tratamiento:

- Número de personas: …
- Perfiles: …
- Roles: …

Indicar las características de los locales que puedan tener incidencia en los procesos de recogida de datos o de su tratamiento, como salas comunes para atención a los ciudadanos, lugares de trabajo en los que se comparte espacio de pantallas, teléfonos, etc: ……..

Identificar todos los procesos de la organización que pueden estar relacionados o afectados por el tratamiento en relación al mapa de procesos de la misma: ……

- Indicar el contexto del sistema/s propuesto/s para la implementación del tratamiento y el detalle de las tecnologías empleadas: ……..

3.7 Contexto externo de la entidad y el tratamiento

Actualmente son muchas las entidades que se encuentran en un periodo de transformación de procesos de un entorno tradicional papel a una gestión electrónica de algunos de sus trámites.

Concretamente el sector público, tras la aprobación de la Ley 39/2015, de 1 de octubre, del Procedimiento Común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, está actualmente inmerso en la implantación de la plena Administración Electrónica, desplegando en muchas de sus oficinas la utilización de sistemas de firma manuscrita electrónica en lugar de firma manuscrita tradicional como elemento de mejora de seguridad y la eficiencia.

En el marco de dicha normativa, dentro de este proceso de firma se han previsto diversas opciones de utilización de medios electrónicos, pudiendo implantarse por las AAPP el uso de sistemas de identificación electrónica con valor de firma electrónica, firma electrónica avanzada basada en certificados cualificados o la captura de la firma electrónica manuscrita a través de dispositivos de digitalización de firmas.

Si bien la firma electrónica cualificada (denominada “reconocida” en la Ley 59/2003) es una excelente herramienta de firma para un entorno no presencial, ha demostrado su ineficacia en entornos de personación física del ciudadano ante las dependencias administrativas, lo cual ha impedido alcanzar hasta la fecha el objetivo final de “Administración Sin Papeles”, y que la Ley 39/2015 se ha propuesto conseguir.

Los servicios de firma electrónica manuscrita de VIDsigner BIO están orientados a entornos presenciales de firma, lo cual permite a las administraciones que los ciudadanos que acudan a hacer alguna tramitación, aunque no dispongan de medios electrónicos o no deseen utilizar los sistemas IDCat o IDCat móvil (sistemas de firma electrónica proporcionados por la Administración basados en certificados electrónicos), puedan firmar, con la máxima seguridad jurídica, sus solicitudes e instancias sobre una tablet, tal como lo harían en papel. De esta forma, los ciudadanos no necesitan disponer de ningún elemento tecnológico adicional y a la administración pública le permite incluir el documento (instancia, solicitud, etc..) firmado en el expediente de forma totalmente electrónica, cumpliendo de esta forma el mandato de la Ley 39/2015. Por tanto, el servicio VIDsigner garantiza el derecho del ciudadano a firmar manuscritamente el documento electrónico presentado ante la Administración, otorgando a ambas partes la seguridad jurídica de la autoría y autenticidad de la firma.

4 Licitud del tratamiento y cumplimiento normativo

La utilización del sistema VIDsigner BIO por parte del Responsable del tratamiento permite garantizar el cumplimiento escrupuloso del derecho fundamental a la protección de datos recabados. Así, en relación a la licitud del tratamiento, el cumplimiento de la cual es responsabilidad del Responsable del tratamiento, se basa en el consentimiento explícito de los interesados al tratamiento de sus datos especiales (biométricos), conforme a los arts. 6.1 y 9.2[2] RGPD, pudiéndose recabar dicho consentimiento informado mediante el uso de un checkbox configurado en la aplicación VIDsigner (o pudiendo utilizar el cliente otro medio que considere más oportuno, por ejemplo utilizando otra aplicación informática).

Hay que indicar que el artículo 9.1 RGPD establece la prohibición del tratamiento de las categorías especiales de datos, y el 9.2, las excepciones que deben concurrir para que el mismo pueda llevarse a cabo (entre ellas, el consentimiento del usuario), indicando el apartado 4 que *"Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud"*. Sin embargo, el legislador español no desarrolló dicho apartado 4 en la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, ni tampoco la Agencia Española de Protección de Datos ha emitido, hasta la fecha, ninguna circular de obligado cumplimiento sobre este tratamiento particular, y por tanto el marco jurídico aplicable en la actualidad a dichos datos está representando únicamente por lo establecido por el RGPD[3].

De acuerdo con el RGPD, además del tratamiento de datos biométricos, por tratarse antes que nada del tratamiento de datos personales, previamente se requiere la concurrencia de, al menos, una de las seis bases jurídicas establecidas en su artículo 6 RGPD, y adicionalmente, se requiere que concurra una de esas excepciones del art. 9.2 RGPD (que en el caso de los datos biométricos obtenidos mediante VIDSigner dicha excepción es el consentimiento explícito del usuario).

En relación a los referidos aspectos de cumplimiento normativo y el resto de aspectos que deben ser revisados por el responsable del tratamiento, teniendo en cuenta la naturaleza de los datos biométricos recabados de los interesados, para garantizar y poder demostrar que el tratamiento es conforme con el RGPD, en el Anexo I se indican aquellos aspectos que dicho responsable del tratamiento debe evaluar en la EIPD respecto al cumplimiento normativo:

1. Principios relativos al tratamiento
2. Licitud del tratamiento
3. Condiciones para el consentimiento
4. Tratamiento de categorías especiales de datos
5. Derechos del interesado. transparencia de la información
6. Derechos del interesado. información a facilitar cuando los datos se obtienen del interesado

[2] Hay que observar que en el marco jurídico de la privacidad de la Unión Europea constituido por el RGPD y dentro del entorno internacional del Convenio 108 (modernizado) del Consejo de Europa, los datos biométricos se consideran datos especiales o sensibles y se encuentran sujetos a una protección especial.

[3] Excepto lo establecido por la Disposición final undécima de la LOPDGDD (Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno), que modifica el apartado 1 del artículo 15.

7. Derechos del interesado. derecho de acceso
8. Derechos del interesado. derecho de rectificación
9. Derechos del interesado. derecho de supresión («el derecho al olvido»)
10. Derechos del interesado. derecho a la limitación del tratamiento
11. Información al interesado ante rectificación, supresión o limitación en el tratamiento
12. Derechos del interesado. derecho a la portabilidad de los datos
13. Derechos del interesado. derecho de oposición
14. Derechos del interesado. decisiones individuales automatizadas, incluida la elaboración de perfiles
15. Responsabilidad del responsable del tratamiento
16. Protección de datos desde el diseño y por defecto
17. Corresponsables del tratamiento
18. Encargado del tratamiento
19. Registro de las actividades de tratamiento
20. Seguridad del tratamiento
21. Notificación de brechas de la seguridad de los datos personales a la autoridad de control
22. Comunicación de una brecha al interesado
23. Evaluación de impacto relativa a la protección de datos

5 Metodología de la EIPD

5.1 Implicados en la ejecución de la EIPD

Definir el equipo de trabajo, roles, tareas, responsabilidades, etc: ..

En general, el equipo de trabajo será multidisciplinar y dará respuesta al contexto en el que la EIPD y el tratamiento tienen lugar, contexto en el que podrán incluirse cuestiones normativas, sociales, culturales, etc

Toda vez que el tratamiento mediante VIDsigner implica el uso de una herramienta digital, se deberá contar con perfiles de carácter tecnológico capaces de describir el alcance, tanto desde el punto de vista funcional como desde el posible impacto a la privacidad, de la tecnología utilizada.

5.2 Guías, herramientas, metodologías, normas y dictámenes utilizados en la evaluación

El responsable debe escoger una metodología para llevar adelante la Evaluación de Impacto de Protección de Datos personales (EIPD), por ejemplo las basadas en las siguientes guías:

- "Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD" (Agencia de Protección de Datos Española).
- "Guía práctica para la Evaluación de impacto relativa a la Protección de datos" (Autoridad Catalana de Protección de Datos)

Estas metodologías se basan en un conjunto de etapas, estructuradas de la siguiente forma:

5.3 Extensión y límites de la EIPD: Identificar que ha quedado fuera de la evaluación

La EIPD se circunscribe al tratamiento de los datos biométricos por considerar que únicamente dicho tratamiento resulta probable que supone un riesgo significativo para los derechos y libertades de las personas.

6 Análisis del tratamiento

Este análisis supone estudiar el tratamiento dividiéndolo en etapas o fases desde el punto de vista del ciclo de vida de los datos.

En el Anexo I de la Guía de EIPD de la AEPD hay un modelo en el que se lleva a cabo una posible segmentación de los tratamientos en lo que se denomina "ciclo de vida de los datos asociados a un tratamiento".

Es recomendable tener en cuenta, al menos, las fases de: captura, clasificación y almacenamiento, uso y tratamiento o explotación de los datos, cesiones y transferencias a terceros para su tratamiento, y destrucción de los datos.

Para cada una de las fases hay que identificar los elementos de riesgo inherentes en cada una de las etapas del tratamiento, en particular.

Infraestructura informática del servicio VidSgner BIO

El servicio VidSgner BIO utiliza el siguiente sistema de información e infraestructura informática:

- Un servicio Cloud propiedad de la empresa Microsoft, denominado Microsoft Azure, servicio en la nube y alojado en los Data Centers de Microsoft y que cuenta con certificación de nivel alto según el Esquema Nacional de Seguridad (ENS). Dicho servicio y los dispositivos de los usuarios están conectados mediante líneas de telecomunicaciones cifradas.

Descripción del entorno de comunicaciones

Fibra óptica / ADSL /WIFI protegida mediante cifrado

Descripción de las aplicaciones:

- App VIDsigner Bio instalada en las tablets encargada de mostrar el documento al firmante y recoger si firma manuscrita
- Aplicación del cliente integrada con VIDsigner

A continuación, se lleva a cabo un análisis de las operaciones realizadas por el servicio VidSgner BIO sobre los datos en cada una de las cinco etapas o fases en las que se puede dividir el ciclo de vida de los datos, incluyendo información del flujo de los datos objeto de tratamiento:

6.1 Fase de entrada o captura de los datos biométricos:

Sea cual sea el canal que utilice el responsable para la obtención de los datos biométricos, estos se capturan mediante la firma de documentos electrónicos en tabletas usando el servicio VIDsigner Bio, cuyo lugar de origen puede ser uno de los tres siguientes:

- Dependencias del responsable
- Dependencias del lugar donde el ciudadano esté situado

Se identifican tres categorías de datos personales en la fase de entrada de datos:

- Datos personales básicos de identificación de los firmantes:
  - nombre y apellidos (obligatorio)
  - NIF (obligatorio)

- correo electrónico (opcional)

- Datos personales especiales de identificación de los firmantes:
  - biométricos de los rasgos de comportamiento de la firma manuscrita (obligatorio): posición, tiempo y presión de los rasgos de la firma.

- Datos personales de cualquier naturaleza, básicos y especiales, incluidos en los documentos firmados:

  - Identificación
  - económicos y seguros
  - características personales
  - circunstancias sociales
  - académicos y profesionales
  - ocupaciones
  - salud
  - afiliación sindical
  - creencias
  - origen étnico o racial
  - opiniones políticas
  - convicciones religiosas o filosóficas
  - genéticos
  - biométricos
  - vida sexual u orientación sexuales

6.2 Fase de clasificación de los datos:

En función de la utilidad del tratamiento, los datos personales se pueden clasificar en dos categorías:

- Datos que son útiles exclusivamente para identificar a las personas que firman los documentos.
- Datos que están incorporados en los documentos firmados, los cuales son útiles para ejecutar la prestación del servicio de firma electrónica, pero no para identificar las personas que firman los documentos.

6.3 Fase de tratamiento o explotación de los datos:

Las aplicaciones del responsable que consumen el servicio de VIDsigner BIO se comunican con el servicio utilizando una API REST. Esta API REST está asegurada bajo el canal SSL con un certificado SSL para que todas las comunicaciones entre las referidas aplicaciones y VIDsigner BIO estén cifradas.

Así, en el servicio de firma VIDsigner BIO la aplicación del responsable se comunica con la API REST para enviar a firmar el documento en formato PDF al dispositivo de captura de firma junto a la información de identificación del firmante: nombre y apellidos, NIF y correo electrónico (no obligatorio).

La APP VIDsigner BIO es responsable de mostrar el documento al usuario y recabar la firma que procesará el Servicio de Cloud.

Autenticación: todas las peticiones enviadas al API de VIDsigner son autenticadas siguiendo el esquema básico de autenticación HTTP como está definido en RFC-2617.

Información intercambiada

Para firmar un documento se requiere intercambiar entre el responsable y la APP VIDsigner la siguiente información:

- El documento: Este debe ser un documento PDF. Un documento puede contener información personal o confidencial, por lo que se almacena de forma segura, tal y como se explica en la sección Almacenamiento.

- Información del firmante: La información del firmante es necesaria para asegurar que la persona que lee y firma el documento es la adecuada y para mantener la evidencia de la información del firmante. Se trata de una información personal y debe ser procesada teniendo en cuenta la normativa de protección de datos. La información del firmante incluye:

- Nombre completo del firmante
- Número de identificación del firmante: Puede ser un número de identificación nacional, un pasaporte o cualquier otro número de identificación como identificación de empleado.
- Correo electrónico del firmante: Esta información es opcional y no es estrictamente necesaria en el proceso de firma.

- Información operativa: Es la información que se requiere en el proceso de firma pero que no es crítica en términos de confidencialidad, incluye:

- Posición de la firma
- Dispositivo de firma
- Orden de las firmas

Comunicaciones entre la aplicación VIDsigner Bio y VIDCloud

La APP VIDsigner Bio es la responsable de mostrar el documento al usuario y recoger la firma para ser procesada por el Servicio Cloud.

Alguna información es enviada desde la Nube a la APP y alguna otra de forma inversa. En este apartado se explican las medidas de protección de dicha información.

Confidencialidad

Todas las comunicaciones entre cualquier dispositivo y el servicio en la nube están aseguradas bajo SSL con un certificado SSL de host para que toda la información intercambiada sea cifrada.

Esto significa que todos los datos intercambiados son confidenciales.

Autenticación

Cuando se registra un dispositivo, se crea un ID de autenticación y se almacena localmente para identificar el dispositivo en la comunicación con el servicio en la nube.

Este autenticador ID se almacena en un área privada “sandboxed” para evitar que otras APP o usuarios maliciosos puedan acceder a ella. Si se elimina la APP, el authenticador ID se borra del dispositivo (¿).

Información intercambiada

- Datos del servicio a los dispositivos: El servicio envía a los dispositivos (tabletas) la información necesaria para realizar un proceso de firma, que incluye:
- Documento entregado: El documento no se envía en formato PDF sino un "render" del documento que impide que el contenido del mismo pueda ser analizado mecánicamente.
- Información del firmante: La información del firmante se presenta en el proceso de firma, por lo que debe ser enviada.
- Datos de los dispositivos (tabletas) al servicio: Los dispositivos recogen evidencias del proceso de firma y las envían al servicio en orden de asegurar y adjuntar al documento. Aquí la información recogida y enviada es la biometría de la firma manuscrita: Esto incluye, posición, tiempo y presión para todos los puntos contenidos en la firma. Esta información es posteriormente procesada en el servicio y transformada en Norma ISO.
- Evidencias de contexto: Son evidencias que añaden información extra del proceso de firma. Estas evidencias pueden diferir dependiendo del modelo de dispositivo y la configuración que pueda haber:
    - Nombre del dispositivo: Este es un nombre único que identifica al dispositivo en VIDsigner
    - ID del dispositivo
    - Tipo de SO del dispositivo
    - Versión del sistema operativo del dispositivo
    - Modelo del dispositivo

6.4 Fase de almacenamiento:

Almacenamiento en la nube (Azure)

- Almacenamiento de la base de datos

La información del firmante se almacena en una base de datos durante el proceso de firma. El acceso a esta base de datos está asegurada de dos maneras:

- IP: Sólo los servidores VIDsigner pueden acceder a la base de datos
- Contraseña: Se requiere una contraseña para acceder a los datos almacenados en la base de datos.

Además, la información de la base de datos está protegida mediante TDE (encriptación transparente de datos), por lo que aunque se acceda a la base de datos, la información sigue siendo confidencial.

- Almacenamiento de documentos

Los documentos se almacenan en un blob storage que permite guardar grandes cantidades de documentos de cualquier tamaño.

El acceso a este almacenamiento está protegido, por lo que sólo los servidores VIDsigner pueden acceder a ellos.

Esta información se almacena cifrada, así que incluso si se accede al almacenamiento la información permanece confidencial.

Proceso de almacenamiento del documento firmado con el servicio VIDsigner

Todos los datos obtenidos, una vez realizada la operación de firma mediante la herramienta VIDsigner BIO, se cargan, a través de la API correspondiente, en los sistemas centrales de Azure, los cuales quedan almacenados temporalmente en dos repositorios:

- En la base de datos del sistema (cifrado)
- En el servicio de "storage" del sistema (cifrado)

Una vez enviado el documento a la APP VIDsigner, dicho documento mismo puede firmarse, no firmarse, o rechazarse.

Documento firmado

Si el documento se firma se envían los datos biométricos de la firma al servicio Cloud que de forma automática y desasistida se cifran junto con otros datos de contexto (hash del documento e id del dispositivo) y se insertan como metadatos del documento.
Posteriormente, se firma electrónicamente el documento usando alguna de estas dos opciones:

- Mediante el uso de un certificado de sello titularidad de VID,
- Realizando una petición a FIRMAPROFESIONAL para la emisión de un certificado de un sólo uso (OTP), en cuya petición se le comunican los datos de carácter identificativo de nombre y apellidos, e-mail, DNI.

Una vez se ha firmado el documento, el emisor tiene un plazo de dos meses para descargar el documento firmado del "storage" del cloud y dependiendo del tipo documental, este podrá enviar al firmante el documento firmado.

Si el documento se ha firmado, el responsable del tratamiento tiene un plazo de 2 meses para descargarlo del servicio.

Una vez finalizado el proceso de descarga del documento por el responsable del tratamiento se eliminan los datos del firmante y los documentos, y lo único que se mantiene en el sistema de almacenamiento es un log que no contiene datos personales (estos datos son: el ID del documento, la fecha de proceso y de cuando se cargó el documento, y el hash del documento), es decir, es información anonimizada.

Documento no firmado
En caso de que el documento que se ha enviado al servicio cloud de VIDsigner no se ha firmado por el usuario, permanece almacenado en el "storage" del cloud temporalmente. El plazo de tiempo concedido al responsable del tratamiento para su firma por el ciudadano es de 1 mes. Transcurrido dicho plazo se elimina el documento.
Documento rechazado
En caso de que el documento que se ha enviado al servicio cloud se haya rechazado por el usuario, como no se ha firmado, finaliza el proceso y se elimina el documento.

6.5 Fase de destrucción de los datos

Una vez finalizado el proceso de descarga del documento por el responsable del tratamiento, VID elimina el documento y la información del firmane de sus sistemas y el responsable de tratamiento conserva el documento en sus sistemas de información durante el tiempo necesario para poder garantizar el derecho del responsable de demostrar, ante la autoridad judicial o administrativa competente, la autoría y autenticidad de la firma realizada en su documento presentado por un ciudadano al responsable del tratamiento con el objeto de evitar cualquier responsabilidad que se pudiera derivar de reclamaciones o acciones interpuestas ante dicho responsable.

7 Análisis de la obligación de realizar una EIPD: evaluación del riesgo

El responsable del tratamiento ha determinado que tiene la obligación de realizar la EIPD, pues el tratamiento puede entrar en la lista de casos enumerados en el artículo 35.3 del RGPD (“tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10”) y, específicamente, también cumple con las condiciones que se detallan en la lista de tratamientos obligados (artículo 35.4 del RGPD) establecidos en el apartado 5 de la lista publicada por la Agencia Española de Protección de Datos (“Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física”).

8 Análisis de la necesidad del tratamiento

La jurisprudencia española, tanto del Tribunal Supremo (STS 5200/2007) como del Tribunal Constitucional (STC 39/2016), así como la doctrina administrativa de la Agencia Española de Protección de datos emitida en diversas resoluciones a partir del informe nº 65/2015 de su Gabinete Jurídico (que se amparaba en el Dictamen 3/2012 del Grupo del Artículo 29 "sobre la evolución de las tecnologías biométricas"[4]), han defendido la posible utilización de sistemas biométricos, siempre que se apliquen ciertas garantías que permitan superar el triple juicio de necesidad y proporcionalidad del tratamiento de los datos que la Sentencia del Tribunal Constitucional nº 186/2000 había ya señalado:

> *"La constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo, FJ 5; 55/1996, de 28 de marzo, FFJJ 6, 7, 8 y 9; 207/1996, de 16 de diciembre, FJ 4 e), y 37/1998, de 17 de febrero, FJ 8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes:*
>
> - *si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad);*
> - *si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad);*
> - *y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)."*

En lo que respecta a los datos biométricos, la seguridad aplicada al sistema es un elemento fundamental, ya que los datos biométricos son irrevocables. Por ello, VIDsigner cifra los datos biométricos y los incrusta en el documento, empleando para ello una clave pública cuya contraparte (clave privada) se encuentra custodiada en sede notarial. Además, para garantizar la integridad del documento se emplea un certificado digital de un sólo uso para la firma electrónica del documento y un sello de tiempo reconocido. El resultado final es un documento PDF firmado conforme al estándar de firma longeva (LT) de Acrobat, lo que garantiza su validación a lo largo del tiempo.

Este sistema garantiza la seguridad y la integridad, pues evita cualquier posible mal uso de los datos (por ejemplo, utilizarse para otras finalidades no consentidas) así como el riesgo de la usurpación de la firma, pues las partes no pueden manipular el documento ni acceder a los datos biométricos (pero que sí podrían ser peritadas caligráficamente por un perito judicial) y el depósito de las claves en sede notarial garantiza que la información biométrica únicamente podrá ser descifrada ante requerimiento judicial y que estará accesible en el tiempo al formar parte del protocolo notarial.

[4] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Así, el registro de la información biométrica permite a un perito calígrafo determinar la autoría de la firma, habiendo sido codificado los datos según la ISO/IEC 19794-7 y la ISO/IEC 29109-7:2011, lo que garantiza su valoración pericial futura, con independencia de la evolución tecnológica.

De esta forma, en relación al llamado triple juicio de proporcionalidad, al analizar la proporcionalidad de un sistema biométrico, como arriba se ha visto, es preciso considerar previamente lo siguiente:

1. Si la medida adoptada es susceptible de conseguir el objetivo propuesto (**juicio de idoneidad**).

2. Si además, es necesaria, en el sentido de que no existe otra medida más moderada para la consecución de tal propósito con igual eficacia (**juicio de necesidad**).

3. Y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (**juicio de proporcionalidad en sentido estricto**), es decir, si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla.

8.1 Juicio de idoneidad

En relación al **juicio de idoneidad,** hay que dilucidar si el sistema VIDsigner es necesario para responder a una necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable.

En este sentido debe afirmarse que se considera a los servicios de firma manuscrita sobre un soporte electrónico, y en particular VIDsigner , como el servicio idóneo y esencial para la firma de documentos electrónicos, en tanto que el mismo es un medio útil y confiable para permitir identificar al autor de la firma de un documento electrónico y poder demostrar fehacientemente, si es menester, en un futuro ante la autoridad judicial correspondiente, la autoría de la misma (autenticidad) así como la integridad del documento firmado (integridad).

Por tanto, la finalidad perseguida por el sistema de firma manuscrita sobre un soporte electrónico, como VIDsigner BIO, ofrece a las organizaciones y a los usuarios de sus servicios, y a la sociedad en general, que haga uso del servicio para la firma de documentos electrónicos, una seguridad jurídica en el mundo digital que, desde la perspectiva del derecho de protección de datos, hace que sea plenamente idónea, legítima y justificada.

Los datos biométricos captados por VIDsigner BIO en ningún caso son utilizados para fines de identificación en grandes bases de datos centralizadas, dadas las consecuencias potencialmente perjudiciales para las personas afectadas, como advirtió el Grupo de Trabajo del artículo 29, sino que se conservan cifrados y firmados electrónicamente únicamente a disposición de la autoridad judicial correspondiente.

Así mismo se reconoce lo siguiente en el Dictamen 3/2012 del Grupo de Trabajo del artículo 29:

> *"Los datos biométricos se utilizan con éxito y eficacia en la investigación científica, son un elemento clave de la ciencia forense y un valioso elemento de los sistemas de control de acceso. Pueden contribuir a aumentar el nivel de seguridad y a facilitar, acelerar y simplificar los procedimientos de identificación y autenticación."*

De lo anterior cabe significar que VIDsigner es una herramienta útil y muy valiosa, por tanto, para contribuir, en el ámbito digital, al desarrollo y evolución de la ciencia forense, entendida como la ciencia aplicada que se encarga de estudiar los indicios o pruebas periciales en procedimientos judiciales, y concretamente la grafología forense, que analiza la autenticidad de un texto o firma y su autoría.

8.2 Juicio de necesidad

En relación al **juicio de necesidad**, hay que dilucidar la probabilidad de que el tratamiento sea eficaz para responder a la necesidad en cuestión del sistema VIDsigner a la luz de las características específicas de la tecnología biométrica que utiliza.

Sobre ello corresponde indicar que en el actual ecosistema digital, donde la seguridad y la confidencialidad de los datos son elementos esenciales, el uso de los datos biométricos que realiza VIDsigner sirve para que el servicio ofrezca su máxima eficacia al prestar las máximas garantías técnicas y jurídicas a los usuarios en el eventual supuesto de impugnación de la firma de documentos electrónicos en el marco de las relaciones mercantiles o laborales de las organizaciones y los ciudadanos, garantizando de esta manera la aplicación del principio constitucional del derecho a la tutela judicial efectiva (art. 24.1 CE), en su vertiente del derecho a la práctica de la prueba pericial que garantice la demostración de la autenticidad de la autoría de la firma manuscrita electrónica.

Es por este motivo que la recolección y utilización por parte de VIDsigner de los datos biométricos es necesaria para la finalidad del sistema de firma.

El propio RGPD (considerando 4) establece que el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad:

> *"El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística."*

Y no hay duda de que una solución digital de firma que no utilice datos biométricos no puede garantizar con igual eficacia, en sede judicial, la obtención de una prueba robusta y segura de una firma, como los servicios de firma electrónica manuscrita de VIDsigner.

A mayor abundamiento, como es sabido, en los últimos años la tendencia del legislador español y europeo está forzando a los ciudadanos a utilizar en exclusiva medios electrónicos, como la *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*, que obliga a las personas jurídicas, y en algunos casos incluso físicas, a relacionarse con las Administraciones Públicas únicamente por medios electrónicos. En este sentido, pues, puede afirmarse que la utilización de documentos electrónicos y en consecuencia de la firma electrónica es, hoy en día una necesidad, siendo el uso de sistemas de firma biométrica la única opción de firma electrónica posible para los casos en los que el firmante no cuenta con los medios tecnológicos necesarios para emplear otras tecnologías de firma (como el certificado digital).

En este punto, es necesario decir que, en las AAPP, la finalidad del tratamiento no se puede conseguir razonablemente por otros medios, es decir, no se dispone de una alternativa a la firma biométrica en el marco del procedimiento administrativo que garantice con igual eficacia, en sede judicial, la obtención de una prueba robusta y segura de una firma, como los servicios de firma electrónica manuscrita de VIDsigner.

Así, los Ayuntamientos ofrecen varios canales de tramitación: presencial o telemático.

Tramitación telemática

De forma telemática admiten cualquier forma de identificación y firma de los interesados de las reconocidas en los artículos 10 y 11 respectivamente de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas. Para realizar trámites online admiten los certificados digitales emitidos por las principales entidades de certificación como por ejemplo la Agencia Catalana de Certificación (CATCERT), Camerfirma, Fabrica Nacional de Moneda y Timbre (FNMT), DNI electrónico, etc ...

Tramitación presencial

La tramitación presencial se efectúa en las Oficinas de Atención Ciudadana, donde los ciudadanos disponen de diversas alternativas:

- la posibilidad de que el gestor de atención ciudadana lo acompañe para hacer la presentación de los documentos de forma telemática en el punto TIC existente en las mismas oficinas y les ayuda en la obtención del certificado electrónico llamado “IdCAT” o la clave “IdCAT mòbil”, que es un mecanismo de identificación y firma electrónica orientado a la ciudadanía y basado en el envío de una contraseña de un solo uso al teléfono móvil, ambos sistemas proporcionados por el Consorci de l’Administració Oberta de Catalunya (AOC).

La opción del certificado electrónico llamado “IdCAT” o la clave “IdCAT mòbil” no es una alternativa fiable a la firma biométrica, desde el momento que, habitualmente, muchos ciudadanos no desean utilizar esta opción para firmar, entre otros motivos posibles, porque prefieren garantizar la autenticidad de su firma realizándola manuscritamente utilizando tabletas digitalizadoras.

- formularios en papel firmados que son digitalizados y autenticados mediante la firma de los mismos con un sello electrónico de órgano utilizado para realizar copias auténticas del documento en papel. Dicho proceso de digitalización es un proceso automático (actuación

administrativa automatizada) en el que no interviene el empleado público, salvo la función de poner el documento papel en el escáner que sería una actuación preliminar y propia de asistencia a los interesados.

La digitalización y destrucción del original en papel produciría una grave indefensión en el administrado, habida cuenta de que es materialmente imposible determinar la autoría de una firma manuscrita de un documento escaneado, ya que no se conservan los rasgos identificativos de la firma y por tanto no sirve como medio de prueba ante litigio.

La única alternativa posible para cumplir con ambas obligaciones (archivo electrónico obligatorio y garantía de prueba ante litigios) es el uso de sistemas de firma electrónica manuscrita. Recordemos que el art. 17.2 de la LPAC obliga a que *"los documentos electrónicos deberán conservarse en un formato que permita garantizar la **autenticidad**, integridad y conservación del documento".*

- otro sistema posible de firma, es la figura del funcionario "habilitado" previsto en la Ley 39/2015, que es una alternativa a la firma biométrica presencial, pero que tampoco reúne las mismas garantías y el derecho del ciudadano a comunicarse electrónicamente con la Administración.

Así, ante dichas opciones, las AAPP recurren a la firma biométrica para resolver única y exclusivamente la atención y comparecencia de los ciudadanos en las oficinas físicas, ya que la Ley 39/2015 no parece dar una respuesta convincente para la firma de documentos por el ciudadano. El problema de fondo radica en que la tramitación electrónica, habitualmente se asocia (quizá erróneamente) a tramitación telemática, requiriendo esta, a su vez, de medios de identificación y firma que no están pensados ni adaptados a entornos presenciales, habitualmente centrados en sistemas basados en certificados digitales y claves concertadas.

La opción más evidente que nos ofrece la Ley 39/2015 es la utilización de los denominados funcionarios habilitados, funcionarios especialmente designados al efecto, que deben constar en un registro especialmente creado para este propósito y que tienen la función de suplir al interesado en aquellos procedimientos que requieran su firma. Pero no son pocas las voces críticas ante esta figura por diferentes motivos:

- Primero, desde el punto de vista práctico, los funcionarios habilitados deben estar registrados nominalmente y además no es posible designar personal laboral para la realización de estas tareas.
- Segundo, es reprochable desde el punto de vista jurídico e incongruente con la LPAC y la propia lógica, que existiendo medios tecnológicos al servicio de las administraciones públicas se deleguen actos personalísimos en otra persona física (aunque sea un funcionario).
- Tercero, para que se pueda hacer uso del funcionario habilitado el ciudadano no debe disponer de medios electrónicos.
- Cuarto, es criticable que, siendo la propia administración parte interesada de la mayoría de los procedimientos administrativos "se convierta en juez y parte" firmando por si misma y por la contraparte.
- Quinto, en determinados casos en los que es la propia administración la que se desplaza físicamente para la realización del trámite (inspecciones, cuerpos y fuerzas de seguridad, trabajadores sociales, autoridades portuarias, …) no es materialmente posible habilitar a todos los funcionarios implicados para asistir a los administrados, pro que se requieren necesariamente sistemas como los utilizados

- Sexto, la aplicación práctica del funcionario habilitado nos conduce a una perversa paradoja: para que un funcionario pueda actuar en nombre del ciudadano éste debe prestar su consentimiento expreso, consentimiento que, al no disponer de medios electrónicos se deberá firmar necesariamente en papel, que es precisamente lo que se trata de evitar.

Por otro lado, dejando de un lado la complejidad e inconvenientes prácticos que desaconsejan su uso y centrándonos exclusivamente en el texto legal, si se analiza con detenimiento el artículo 12 LPAC, respecto a la asistencia de las AAPP a los ciudadanos en el uso de medios electrónicos debemos observar cómo:

2. Este tipo de asistencia se configura como último recurso ante la imposibilidad de las Administraciones de dotar a los ciudadanos de dichos medios.
3. El ciudadano tiene que solicitar expresamente la asistencia del funcionario habilitado, el cual no puede ser impuesto directamente por la Administración en cuestión:

"Artículo 12. Asistencia en el uso de medios electrónicos a los interesados.

1. Las Administraciones Públicas ***deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen****.*

2. Las Administraciones Públicas asistirán en el uso de medios electrónicos a los interesados no incluidos en los apartados 2 y 3 del artículo 14 que así lo soliciten, especialmente en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas.

Asimismo, si alguno de estos interesados no dispone de los medios electrónicos necesarios, su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por un funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, ***será necesario que el interesado que carezca de los medios electrónicos necesarios se identifique ante el funcionario y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia para los casos de discrepancia o litigio****…."*

Por tanto, como conclusión, la asistencia a los interesados en las relaciones presenciales con los ciudadanos no es una alternativa viable al uso de sistemas de firma electrónica manuscrita debido a que:

1. El art. 12.1 evidencia que será obligación de la Administración poner a disposición del ciudadano los canales y sistemas necesarios para garantizar el derecho del ciudadano a utilizar los medios electrónicos para relacionarse con ella, siendo los sistemas de firma electrónica manuscrita los sistemas idóneos para ello en entornos presenciales

2. El apartado 2 del artículo 12 prohíbe expresamente la asistencia a los ciudadanos cuando estos dispongan de medios electrónicos, lo que se traduce en que:

a. A día de hoy es difícil afirmar que un ciudadano no dispone de medios electrónicos con el actual despliegue del DNI electrónico que cubre a prácticamente la totalidad de los firmantes o la posibilidad de usar sistemas de claves concertadas. Cuestión distinta son sus conocidos problemas de usabilidad que se convierten en una auténtica barrera en la tramitación presencial y que precisamente hacen que se requieran sistemas de firma alternativos, pero la ley exclusivamente de "carencia" de medios no de conocimientos ni usabilidad.

b. Al facilitar a los ciudadanos las tablets para realizar la firma está poniendo a disposición de estos los medios electrónicos requeridos.

3. El ciudadano debe dar su consentimiento expreso y este debe servir como medio de prueba ante litigios. Pues bien, la obtención de este consentimiento en papel y su posterior digitalización y destrucción del original en papel produciría una grave indefensión en el administrado (como ocurre con la firma con el sello de órgano arriba indicado), habida cuenta de que es materialmente imposible determinar la autoría de una firma manuscrita de un documento escaneado, ya que no se conservan los rasgos identificativos de la firma y por tanto no sirve como medio de prueba ante litigio. La única alternativa posible para cumplir con ambas obligaciones (archivo electrónico obligatorio y garantía de prueba ante litigios) es el uso de sistemas de firma electrónica manuscrita. Recordemos que el art. 17.2 de la LPAC obliga a que "los documentos electrónicos deberán conservarse en un formato que permita garantizar la **autenticidad**, integridad y conservación del documento".

4. En determinados casos, como se ha visto en inspecciones o atención domiciliaria, es, materialmente imposible obtener la firma del interesado por otro medio.

Entre otras AAPP que utilizan firma biométrica, por existir una alternativa de firma de documentos electrónicos por el ciudadano con igual eficacia que esta, podemos citar las siguientes:

1. Agencia Estatal de la Administración tributaria: https://www.boe.es/boe/dias/2011/02/12/pdfs/BOE-A-2011-2702.pdf (*Sexto. ... se podrán utilizar instrumentos que permitan la firma conjunta de los funcionarios actuantes y de los ciudadanos con quienes se entiendan las actuaciones, tales como tabletas digitalizadoras o asistentes personales digitales …*)
2. Servicio Público de Empleo Estatal: Resolución de 6 de abril de 2016, del Servicio Público de Empleo Estatal, por la que se aprueba el sistema de firma electrónica mediante captura de firma digitalizada con datos biométricos para relacionarse presencialmente con el Servicio Público de Empleo Estatal https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-3931
3. Seguridad social (adquisición de sistemas de firma biométrica manuscrita): https://www.boe.es/diario_boe/txt.php?id=BOE-B-2019-18121
4. Especial mención requiere el ámbito de la Administración de Justicia que en su guía de interoperabilidad incluye los sistemas de firma electrónica manuscrita (https://www.cteaje.gob.es/cteaje/PA_WebAppSGNTJCTEAJE/descarga/CTEAJE-GIS-707-Autenticaci%C3%B3n,%20Certificados%20y%20Firma%20electr%C3%B3nica.pdf?idFile=7bd7502e-262e-4e3f-a453-070bc960c750) y que ya son una realidad en algunos juzgados

(https://cadenaser.com/emisora/2019/11/19/radio_segovia/1574198596_879210.html)

8.3 Juicio de proporcionalidad en sentido estricto: análisis del balance entre riesgo-beneficio

Y, finalmente, hay que analizar si la medida de adoptar el sistema es ponderada o equilibrada, es decir, **el juicio de proporcionalidad en sentido estricto.** Lo que hay que ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados, y en consecuencia, si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no sería apropiada.

Al respecto entendemos que la injerencia producida por VIDsigner en la privacidad del usuario es la mínima posible, toda vez que el sistema capta los mínimos rasgos biométricos (principio de minimización de datos por defecto y desde el diseño del sistema[5]) exclusivamente para identificar y demostrar al autor de la firma, y por ello deja de ser una decisión arbitraria o caprichosa que pretenda examinar comportamientos o conductas del individuo utilizados para otros fines, sino que su única vocación es obtener ese fin legítimo que persigue el sistema de firma biométrica que no es otro que el de recabar una prueba segura y fehaciente de la autoría del consentimiento otorgado a un documento mediante su firma manuscrita sobre un dispositivo electrónico y poderlo demostrar en sede judicial.

Como los datos que se recaban son de la mejor calidad posible al estar codificados según la ISO/IEC 19794-7 y la ISO/IEC 29109-7:2011, ello permite únicamente recolectar los mínimos datos biométricos requeridos para cumplir con la finalidad del sistema de firma. Además, debe observarse que el sistema VIDsigner recolecta datos biométricos relativos a rasgos de comportamiento en el acto de la firma los cuales en ningún caso revelan información alguna sobre el estado de salud de la persona, lo cual sí sería excesivo para la finalidad del sistema.

Debe señalarse además que, para llevar a cabo firmas electrónicas presenciales sobre documentos electrónicos, que produzcan las máximas garantías técnicas y jurídicas en sede judicial, no existe otro medio menos invasivo de la intimidad que alcance el fin deseado por aquéllas. Es por ello, que con el uso VIDsigner entendemos que el "sacrificio" al derecho a la protección de datos está justificado pues la finalidad del tratamiento no puede lograrse razonablemente por otros medios con garantías jurídicas y técnicas, máxime cuando, a modo de garantías jurídicas, las medidas aplicadas sobre la protección de los datos biométricos del firmante se materializan con la aplicación del cifrado de los datos con una clave bajo custodia de un notario en protocolo notarial, y garantizando la integridad y evitando el mal uso, con la generación de un certificado digital en el momento para cada firmante (OTC) y con la aplicación de un sello de tiempo reconocido a cada firma.

[5] El Dictamen 3/2012 del Grupo de Trabajo del artículo 29 precisamente indica que "Por lo que respecta a los sistemas biométricos, la intimidad desde el diseño se refiere a toda la cadena de valor de los sistemas biométricos" indicando que "Por lo que respecta a la seguridad, deberán adoptarse medidas adecuadas para proteger los datos almacenados y tratados por el sistema biométrico: la información biométrica deberá almacenarse siempre de forma cifrada."

Por último, en relación al periodo de conservación de los datos biométricos, hay que indicar que el sistema VIDsigner entrega, por un medio telemático cifrado, única y exclusivamente al responsable del tratamiento, los ficheros cifrados con los datos biométricos incrustados, al cual en cada caso incumbirá determinar el periodo de conservación de los mismos que no podrá ser superior al necesario para los fines para los que dichos datos son recabados o para los que se traten ulteriormente.

Por tanto, el responsable del tratamiento deberá garantizar que los datos se supriman una vez transcurrido este periodo de tiempo justificado, y debiendo aplicar además la LODPGDD, que señala que el responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su supresión, consistiendo el bloqueo de los datos en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los Jueces y Tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Según lo anterior, pues, cuando proceda a la supresión de los datos una vez transcurrido ese periodo de tiempo justificado, deberán conservarse bloqueados exclusivamente cinco años, que es el plazo que establece el código civil (art. 1.964) de las acciones personales que no tengan plazo especial.

Para concluir, un resultado probable de la evaluación del riesgo es que aplicando las medidas expuestas en este documento para su reducción tanto por el proveedor VID como por el responsable del tratamiento, y teniendo en cuenta los beneficios expuestos para el ciudadano y las AAPP que se derivan del tratamiento, justifica sobradamente que las ventajas del tratamiento para los ciudadanos se compensan con los riesgos que corren los ciudadanos.

Medidas para la reducción del riesgo

8.4 Optimización del tratamiento

Sobre los parámetros de descripción del tratamiento se ha de optimizar, desde el punto de vista de protección de datos, la descomposición de este en etapas o subprocesos, para poder realizar una aplicación con más granularidad sobre las medidas de reducción del riesgo

De esta forma, también identificar posibles fases innecesarias, aislar las de mayor nivel de riesgo del resto de fases, determinar medidas específicas para gestionar las fases de mayor riesgo y determinar aquellas que no precisan de acceso a datos personales.

8.5 Medidas de Privacidad por Defecto y desde el Diseño

Las medidas de Privacidad por Defecto y desde el Diseño aplicables dependen del tipo de tratamiento.

El servicio de firma de VIDsigner cumple el principio de privacidad desde el diseño respecto a la minimización y ocultación de los datos pues garantiza la limitación de la accesibilidad a los datos biométricos, teniendo en cuenta que en el mismo momento de su recogida se cifran con una clave AES 256CBC y la clave de descifrado se encuentra bajo custodia notarial y sólo es accesible por una parte interesada bajo requerimiento judicial, por lo que ni el responsable del tratamiento, ni el interesado, ni el mismo prestador del servicio tienen posibilidad de acceder a esta información, lo que imposibilita cualquier tipo de análisis ni conductual ni de ningún tipo respecto de los datos recogidos.

8.6 Medidas de Accountability

El responsable debe implantar medidas de accountability, que son todas aquellas dirigidas a implementar un sistema de gobernanza de los datos personales que permitan demostrar el cumplimiento de:

- Principios
- Derechos
- Garantías para gestionar el riesgo.

En particular:

- Medidas que permitan tener un control sobre qué datos se acceden, por quién, de quien, cuando, con qué legitimación y propósito, que tratamientos se han realizado sobre ellos.
- Medidas para asegurar que los sistemas de gestión de derechos se ejecutan de forma adecuada.
- Medidas para conservar la trazabilidad de los datos comunicados a terceros.
- Nombramiento de DPD.
- Medidas para notificar a los sujetos de los datos incidentes de seguridad que afecten a sus derechos y libertades.
- Intervención humana por parte del responsable en los tratamientos que impliquen decisiones individuales automatizadas.

8.7 Medidas de Seguridad

En este apartado se debe detallar el análisis de los requisitos necesarios para minimizar riesgos para los derechos y libertades sobre los dominios de seguridad: confidencialidad, disponibilidad e integridad de los datos; y como se realiza la integración de dichos requisitos con el resto de los requisitos de seguridad (para continuidad de negocio, control de fraude, etc.) de la organización.

Puede ser conveniente anexar al documento la Declaración de Aplicabilidad de las medidas del Esquema Nacional de Seguridad firmada por el responsable de seguridad.

Respecto a las medidas de autenticación y autorización el responsable aplica las medidas siguientes:

1) Mecanismos utilizados para autenticar a los usuarios en las aplicaciones y sistemas

…

2) Política de contraseñas se utiliza para los sistemas y aplicaciones

…

3) Procedimiento para autorizar y entregar las credenciales de acceso

…

4) Procedimiento para revisar las autorizaciones y el acceso

…

5) Segregación de funciones aplicado, proporcionando detalles sobre los diversos tipos de funciones que existen

…

6) Ubicación del almacenamiento de la información de la aplicación y del sistema

…

Medidas de seguridad aplicadas al tratamiento llevadas a cabo por VID

Validated ID mantiene medidas técnicas y organizativas apropiadas conforme al artículo 32, RGPD, para asegurar un nivel de protección apropiado en relación al riesgo del tratamiento. Las siguientes medidas técnicas y organizativas han sido implementadas actualmente en Validated ID. Dichas medidas son monitorizadas y adaptadas a los desarrollos de última generación en forma continua.

<u>Perspectiva General</u>

Todas las operaciones de negocios están orientadas a un tratamiento de datos seguro, en cumplimiento con las disposiciones legales dentro del ámbito regulatorio europeo y a las recomendaciones de las autoridades de supervisión de protección de datos.

El almacenamiento de datos en las oficinas de Validated ID se evita deliberadamente y por completo. Todas las copias de seguridad se almacenan en CPD especializados bajo altos estándares de disponibilidad.

Las oficinas de Validated ID cuentan con posibilidades de acceso a los grupos de datos necesarios para la implementación de tareas relacionadas con los productos en los departamentos relevantes. Se ha implementado un concepto comprehensivo de roles y derechos para alinear en todo momento los derechos de acceso con el principio de la cuenta de usuario menos privilegiada. El concepto de protección de datos en las oficinas y con respecto a los clientes de los empleados en los respectivos departamentos es continuo, para prevenir todo acceso no autorizado a las bases de datos y a la infraestructura informática.

Dichas medidas se describen en mayor detalle a continuación:

Medidas de cifrado

Medidas o procesos a través de los cuales texto o información claramente legible se convierte en ilegible, por ejemplo tornándose no fácilmente interpretable o una secuencia de caracteres (texto encriptado) con la ayuda de procedimientos de encriptación (sistemas de cifrado).

Medidas para asegurar la confidencialidad

Medidas que deniegan acceso físico a los sistemas informáticos y a los sistemas de tratamiento de datos utilizados para tratar datos personales a personas no autorizadas, como así también a archivos confidenciales y portadores de datos:

Acceso físico a las oficinas de Validated ID

- Seguridad adicional de puertas por medio de tokens electrónicos.
- Seguridad de las oficinas por medio de equipo de vigilancia (sistema de alarma, videovigilancia del exterior)
- monitorización del edificio por parte de un encargado.
- Personal de recepción durante horas regulares de oficina.
- En líneas generales no hay visitantes externos; reglas claras para chequeos a visitantes.

Control de acceso físico al centro de datos

CPD ubicado en Azure, ubicación privada de Microsoft bajo sus políticas de acceso y auditorías.

Sistemas de control de acceso

- Autorizaciones de acceso para todos los sistemas de tratamiento de datos
- Sistemas informáticos y dispositivos de usuarios finales requieren autenticación a través de procedimientos de contraseñas, por ejemplo, inicio de sesión personal e individual cada vez que se accede al sistema
- Imposición por parte del sistema del cumplimiento de estándares para las contraseñas individuales conforme la política de contraseñas
- Listas de acceso
- Registro de intentos de inicio de sesión y terminación del proceso de inicio de sesión luego de un número determinado de intentos fallidos
- Actualización periódica de los filtros antivirus y contra spyware

- firewalls; prevención y detección de intrusión adicional; escaneos de vulnerabilidad y parches activos de seguridad en el centro de datos.

Control de acceso a datos

- Conceptos de autorización (perfiles, roles, etc.) incluyendo documentación

- Restricción de autorizaciones a través de autorizaciones grupales y jerárquicas conforme al principio de menor privilegio

- Instalación y documentación de cuentas de usuario llevadas a cabo solamente por la informática interna y sobre la base de los conceptos de autorización

- Evaluación/registro; procesos automáticos de monitoreo para los registros y para reportar anomalías

- Interfaces para bloquear la entrada y salida (por ejemplo, memorias USB, control estricto de puertos) en todos los sistemas que tratan datos personales

- Cuando un empleado deja la empresa, su cuenta de usuario, incluyendo todas las autorizaciones, son inmediatamente suprimidas; ésto siempre es cotejado con la documentación de las autorizaciones asignadas a dicho empleado.

Control de separación

- Conceptos de autorización.

- Separación de clientes del lado de la aplicación informática.

- Separación estricta de los sistemas de desarrollo, integración, preproducción de producción.

<u>Medidas para asegurar la integridad</u>

Medidas para asegurar que los datos personales no puedan ser leídos, copiados, modificados o suprimidos por personas no autorizadas cuando se transfieren electrónicamente o cuando son transportados o almacenados en portadores de datos, y medidas para examinar y establecer los destinatarios a quienes los datos personales deben ser transmitidos.

Control de transmisión de datos

- Todos los empleados tienen la obligación de cumplir con la normativa de protección de datos.

- La transmisión de datos se realiza a través de redes cifradas o conexiones de túneles; en principio los datos siempre se transmiten utilizando cifrado SSL/TLS del lado del servidor.

- Procesos de transporte bajo responsabilidad individual.

- Métodos de encriptación y certificados que detectan modificaciones efectuadas durante el transporte

Medidas para asegurar la disponibilidad y resiliencia

Los datos se encuentran en CPD propiedad de Azure, con alta disponibilidad y facilidad de movimiento entre centros de forma que si uno es afectado, otro puede ocupar su carga de trabajo.

Firmas digitales

Cada firma biométrica se completa con una firma digital. La firma digital no identifica al firmante, esto se hace utilizando la información biométrica, sólo se utiliza para garantizar la integridad del documento.

Formato

Las firmas digitales aplicadas están en formato PADES B-LT. LT significa "Long Term" (a largo plazo). Esto significa que la firma puede ser validada después de la expiración del certificado porque la información de revocación del certificado está incrustada, así como los sellos de tiempo.

Algoritmos

Las firmas digitales se realizan utilizando:

- RSA

- SHA-512

Certificados

Se emite un OTC (One time certificate) por cada firma biométrica realizada.

Por defecto, VIDsigner utiliza FirmaProfesional como TSP para la emission de OTC, pero puede ser configurado para utilizar OTC de otros TSP.

Duración

Los certificados de un solo uso se emiten con una duración de 24 horas. Esto asegura que no puede ser usado para otro propósito.

Como el formato de la firma es PADES B-LT, la firma sigue siendo válida después de la fecha de caducidad del certificado.

Sello de tiempo

Las PADES B-LT contienen un sello de tiempo para asegurar el momento en que se ha realizado la firma y que el certificado no ha sido revocado en ese momento.

El estándar RFC-3161 (TimeStamp Protocol) se utiliza para solicitar y crear los sellos de tiempo.

Por defecto, el VIDsigner utiliza el prestador de Servicios de confianza FirmaProfesional como TSP para la emisión de TimeStamps pero puede ser configurado para utilizar TimeStamps de otros TSPs.

9 Plan de acción

En este capítulo se ha de reflejar el plan de implantación de las medidas y garantías para gestionar el riesgo y las acciones de seguimiento de la efectividad de las mismas.

Una plantilla para realizar un plan de acción básico se encuentra en el Anexo IV de la Guía EIPD de la AEPD.

En el mismo se ha de detallar los objetivos, tareas, calendario, los recursos necesarios, los responsables, así como la interacción con otros tratamientos de la organización.

En particular, tienen que quedar reflejadas las medidas de privacidad desde el diseño que se han definido para que la protección de datos sea una integral al producto/servicio, no una capa añadida.

10 Conclusiones y recomendaciones

En este capítulo se establece el resultado final del análisis de riesgos, las directrices generales para la implementación del tratamiento, se determina si el riesgo es lo suficientemente bajo y si procede la Consulta Previa a la AEPD de acuerdo con el artículo 36 del RGPD.

4. ANEXO I CUADRO DE CUMPLIMIENTO

1. PRINCIPIOS RELATIVOS AL TRATAMIENTO	CUMPLE SI/NO
Se recogen los datos personales con fines determinados	
Se recogen los datos personales con fines explícitos	
Se recogen los datos personales con fines legítimos	
Los datos personales se mantienen exactos	
Se mantienen actualizados	
Se rectifican los datos personales inexactos respecto de la finalidad	
Se suprimen los datos personales inexactos respecto de la finalidad	
Se mantienen durante más tiempo del necesario respecto de la finalidad	
Se tratan con fines de archivo en interés público	
Se tratan con fines de investigación científica	
Se tratan con fines históricos	
Los datos personales se tratan con fines estadísticos	
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	
Se mantiene la trazabilidad de los fines del tratamiento	

2. LICITUD DEL TRATAMIENTO	CUMPLE SI/NO
Se tiene consentimiento para cada finalidad del tratamiento	
El tratamiento es necesario para ejecutar un contrato o precontrato	
Existe obligación legal	
El tratamiento es necesario para proteger intereses vitales	
El tratamiento es necesario para el cumplimiento de interés público	

El tratamiento es necesario para satisfacer intereses legítimos	

3. CONDICIONES PARA EL CONSENTIMIENTO	CUMPLE SI/NO
Se puede demostrar que el afectado dio su consentimiento para el tratamiento	
Se puede demostrar que el tratamiento se realiza como resultado del cumplimiento de una obligación legal	
Se solicita el consentimiento de forma clara e independiente de los demás asuntos	
Se solicita el consentimiento de forma inteligible y de fácil acceso	
Se solicita usando lenguaje claro y sencillo	
Se informa con carácter previo a recabar el consentimiento	
Se permite retirar el consentimiento con la misma facilidad que se recaba	
Se ofrecen medios para retirar el consentimiento en cualquier momento	
Se recaba el libre consentimiento	
Para prestar un servicio se solicitan sólo los datos necesarios	
Para ejecutar un contrato se solicitan sólo los datos necesarios	

4. TRATAMIENTO DE CATEGORIAS ESPECIALES DE DATOS	CUMPLE SI/NO
Se tratan los datos sólo cuando existen normas que lo exceptúen	
Se tratan los datos con consentimiento explícito y no existen normas de derecho que prohíban expresamente su tratamiento	
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que está establecido por las normas de derecho	
Es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección en la medida que existe un convenio colectivo con arreglo a derecho	
Es necesario para proteger los intereses vitales de una persona y el interesado no está capacitado, física o jurídicamente, para dar su consentimiento	
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y se refiere exclusivamente a los miembros actuales o antiguos o a personas que	

mantienen contactos regulares en relación con la finalidad (política, filosófica, religiosa o sindical)	
Se efectúa en el ámbito de actividades legítimas y con las debidas garantías y no se comunican a terceros sin consentimiento de los interesados	
Se tratan datos que el interesado ha hecho manifiestamente públicos	
Es necesario para la formulación, el ejercicio o la defensa de reclamaciones	
Es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social	
Es necesario por razones de interés público en el ámbito de la salud pública sobre la base normas de Derecho que establece medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional	
Es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en base a normas de derecho	
Se realiza cumpliendo las condiciones con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud que establece la normativa nacional	

5. DERECHOS DEL INTERESADO. TRANSPARENCIA DE LA INFORMACIÓN	CUMPLE SI/NO
Se toman medidas para facilitar al interesado toda la información relativa al tratamiento	
La información se facilita de forma concisa, transparente e inteligible	
La información se facilita en lenguaje claro y sencillo	
Se facilita por escrito o por otros medios, incluidos los electrónicos	
Se facilita verbalmente, previa acreditación de su identidad Se facilita al interesado el ejercicio de sus derechos	
Se atienden las peticiones del ejercicio de derechos aunque el tratamiento no requiera identificación salvo que no se pueda identificar al interesado	
Se informa al interesado en el plazo de un mes desde la recepción de su solitud	

Se informa ante el ejercicio de derechos complejos o ante muchas solicitudes en el plazo máximo de tres meses desde la recepción de la solicitud	
Se informa en el plazo de un mes de la prórroga de tres meses indicando el motivo de la dilación	
Se permite a los interesados el ejercicio de derechos por medios electrónicos	
Se informa por medios electrónicos cuando se recibe la solicitud por esos medios salvo que solicite que se realice por otro medio	
Se informa de las razones de la no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales, en el plazo de un mes desde la recepción de la solicitud cuando no se da curso a la solicitud	
Se facilita gratuitamente el ejercicio de derechos	
Se solicita información para acreditar la identidad de la persona física que ejerce sus derechos	
Cuando la información que se facilita utiliza iconos normalizados, el formato electrónico es legible mecánicamente	

6. DERECHOS DEL INTERESADO. INFORMACIÓN A FACILITAR CUANDO LOS DATOS SE OBTIENEN DEL INTERESADO	CUMPLE SI/NO
Se facilita la identidad y los datos de contacto del responsable y, en su caso, del representante cuando se solicitan datos	
Se facilitan los datos de contacto del delegado de protección de datos	
Se facilitan los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento	
Se facilita información sobre el interés legitimo	
Se informa sobre los destinatarios o las categorías de destinatarios	
Se informa del plazo de conservación de los datos personales o los criterios utilizados para determinarlo	
Se informa sobre la existencia del derecho a solicitar el acceso, rectificación o supresión, la limitación del tratamiento, a oponerse y el derecho a la portabilidad	
Si el tratamiento se basa en el consentimiento se informa de la existencia del derecho a retirarlo en cualquier momento	

Se informa del derecho a presentar una reclamación ante una autoridad de control	
Se informa de las cesiones basadas en requisitos legales o contractuales	
Se informa de las cesiones basadas en un requisito necesario para suscribir un contrato	
Se informa de la existencia de decisiones automatizas, elaboración de perfiles, sobre la lógica aplicada, la importancia y consecuencias previstas del tratamiento	
Antes de realizar tratamientos de datos personales para una finalidad distinta de la que fueron recogidos, se informa al interesado y la información abarca esa otra finalidad y cualquier otra información pertinente	

7. DERECHOS DEL INTERESADO. DERECHO DE ACCESO	CUMPLE SI/NO
Se informa respecto a los fines del tratamiento	
Se informa de las categorías de datos personales que se tratan	
Se informa de los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales	
Se informa del plazo previsto de conservación de los datos personales	
Se informa de los criterios utilizados para determinar el plazo de conservación	
Se informa del derecho a solicitar la rectificación o supresión de sus datos	
Se informa del derecho a solicitar la limitación del tratamiento de los datos	
Se informa del derecho a solicitar la oposición al tratamiento	
Se informa del derecho a presentar una reclamación ante una autoridad de control	
Se proporciona información sobre el origen de los datos cuando no recogen del propio interesado	
Se facilita copia de los datos personales objeto de tratamiento cuando el interesado lo solicita	
Se facilita la información en formato electrónico de uso común si lo solicita por medios electrónicos salvo que se facilite otro medio	

8. DERECHOS DEL INTERESADO. DERECHO DE RECTIFICACIÓN	CUMPLE SI/NO
Se rectifican los datos personales inexactos sin dilación indebida	
Se completan los datos personales incompletos teniendo en cuenta los fines del tratamiento	

9. DERECHOS DEL INTERESADO. DERECHO DE SUPRESIÓN («EL DERECHO AL OLVIDO»)	CUMPLE SI/NO
Se suprimen los datos cuando no son necesarios en relación con los fines para los que fueron recogidos	
Se suprimen los datos cuando se retira el consentimiento en que se basa el tratamiento	
Se suprimen los datos cuando se opone al tratamiento	
Se suprimen los datos cuando han sido tratados ilícitamente	
Se suprimen los datos cuando lo exige una obligación legal	
Se suprimen los datos cuando se obtienen en relación con la oferta de servicios de la sociedad de la información	

10. DERECHOS DEL INTERESADO. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO	CUMPLE SI/NO
Se limita el tratamiento durante un plazo para verificar la exactitud de los datos, cuando el interesado impugna su exactitud	
Se limita el tratamiento cuando es ilícito y el interesado se opone a la supresión de sus datos personales y solicita en su lugar la limitación de su uso	
Se limita el tratamiento cuando no son necesarios para los fines pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones	
Se limita el tratamiento cuando el interesado se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado	
Se informa al interesado cuando se levanta la limitación del tratamiento	

11. INFORMACIÓN AL INTERESADO ANTE RECTIFICACIÓN, SUPRESIÓN O LIMITACIÓN EN EL TRATAMIENTO	CUMPLE SI/NO
Se comunican al interesado la rectificación, supresión o limitación en el tratamiento	

12. DERECHOS DEL INTERESADO. DERECHO A LA PORTABILIDAD DE LOS DATOS	CUMPLE SI/NO
Se facilitan los datos cuando el interesado lo solicita en un formato estructurado, de uso común y lectura mecánica	
Se transmiten dichos datos a otro responsable si el tratamiento está basado en el consentimiento o en un contrato	
Se transmiten dichos datos si el tratamiento se efectúe por medios automatizados	
Se transmiten los datos al nuevo responsable que el interesado determina, si es posible técnicamente	

13. DERECHOS DEL INTERESADO. DERECHO DE OPOSICIÓN	CUMPLE SI/NO
Se atienden las solicitudes de oposición y se dejan de tratar los datos	
Se atienden las solicitudes de oposición pero no se dejan de tratar los datos por motivos legítimos imperiosos para el tratamiento que prevalecen sobre los intereses, los derechos y las libertades o para la formulación, el ejercicio o la defensa de reclamaciones	
Se ponen los medios necesarios para que pueda ejercer su derecho a oponerse por medios automatizados	

14. DERECHOS DEL INTERESADO. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES	CUMPLE SI/NO
No se realizan tratamientos que supongan la toma una decisión basada únicamente en el tratamiento automatizado y que produzca efectos jurídicos	

Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque es necesario para la celebración o la ejecución de un contrato	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque están autorizados en Derecho	
Se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos porque se cuenta con el consentimiento explícito	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para salvaguardar el derecho a obtener intervención humana por parte del responsable	
Si se realizan tratamientos que suponen la toma una decisión basada únicamente en el tratamiento automatizado y que producen efectos jurídicos se adoptan medidas adecuadas para dar al interesado ocasión de expresar su punto de vista e impugnar la decisión	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con el consentimiento del interesado	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se cuenta con habilitación legal	
Se informa a los interesados acerca de estas decisiones individuales automatizadas y de la habilitación legal de las mismas	
Se toman decisiones individuales automatizadas, incluida la elaboración de perfiles, que se basen en las categorías especiales de datos personales porque se han tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado	

15. RESPONSABILIDAD DEL RESPONSABLE DEL TRATAMIENTO	CUMPLE SI/NO
Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas	

Se tiene en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento para garantizar y poder demostrar que el tratamiento es conforme con el RGPD	
Se aplican medidas técnicas y organizativas apropiadas	
Las medidas se revisan y actualizan cuando es necesario	
Se han confeccionado políticas de protección de datos	
Se aplican las políticas de protección de datos	

16. PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO	CUMPLE SI/NO
Se analizan las medidas técnicas y organizativas apropiadas antes de determinar los medios de tratamiento Durante el diseño del tratamiento se tienen en cuenta las medidas técnicas y organizativas apropiadas para cumplir con el RGPD	
Durante el tratamiento se aplican las medidas que han sido determinadas Durante el tratamiento se comprueba la efectividad de las medidas aplicadas	
Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines	
Se aplican medidas técnicas y organizativas teniendo en cuenta la cantidad de datos personales recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad	
Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal	

17. CORRESPONSABLES DEL TRATAMIENTO	CUMPLE SI/NO
Se han determinado de modo transparente, y de mutuo acuerdo, las responsabilidades respectivas de los corresponsables en el cumplimiento de las obligaciones impuestas por el RGPD	
El acuerdo fija las respectivas obligaciones de suministro de información al interesado	
El acuerdo entre corresponsables del tratamiento refleja las funciones y relaciones respectivas de ambos en relación con los interesados	
Los aspectos esenciales del acuerdo están a disposición del interesado	

18. ENCARGADO DEL TRATAMIENTO	CUMPLE SI/NO
Se eligen los que ofrecen garantías suficientes conforme con los requisitos del RGPD y garantizando la protección de los derechos del interesado	
El encargado del tratamiento no recurre a otro encargado sin la autorización previa por escrito	
El tratamiento por el encargado se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho	
El contrato establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados así como las obligaciones y derechos del responsable	
El contrato establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable	
El contrato garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria	
El contrato establece que se tomarán las medidas de seguridad necesarias	
El contrato establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento	
El contrato establece que el encargado asistirá para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados	
El contrato establece que se suprimirán o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales	
El contrato establece que pondrá a disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable	
El contrato establece que si el encargado del tratamiento recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se imponen a este otro encargado las mismas obligaciones de protección de datos que las estipuladas en el contrato, mediante contrato u otro acto jurídico establecido con arreglo a Derecho	
El contrato consta por escrito	
Sólo se accede a los datos siguiendo instrucciones del responsable	

19. REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO	CUMPLE SI/NO
Se lleva un registro de las actividades de tratamiento	
El registro recoge el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos	
El registro recoge los fines del tratamiento	
Recoge una descripción de las categorías de interesados y de las categorías de datos personales	
Recoge las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales	
Recogen las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional	
Incluye los plazos previstos para la supresión de las categorías de datos Incluye una descripción general de las medidas técnicas y organizativas apropiadas al riesgo de los tratamientos	

20. SEGURIDAD DEL TRATAMIENTO	CUMPLE SI/NO
Para determinar las medidas a aplicar se tiene en cuenta el estado de la técnica, costes de aplicación, y la naturaleza, alcance, contexto y fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas	
Se aplican las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo	
Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento	
Medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico	
Existe un proceso de verificación, evaluación y valoración regular de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento	

Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado	
Se han tomado medidas para garantizar que las personas autorizadas a acceder a datos sólo los tratan siguiendo instrucciones	

21. NOTIFICACIÓN DE BRECHAS DE LA SEGURIDAD DE LOS DATOS PERSONALES A LA AUTORIDAD DE CONTROL	CUMPLE SI/NO
Se ha establecido un procedimiento para identificar y gestionar las brechas de seguridad	
Existe un procedimiento para que los encargados del tratamiento notifiquen las brechas al responsable en el momento en que tengan conocimiento de ellas	
Existe un procedimiento para notificar a la autoridad de control en el plazo de 72 horas	
Existe un procedimiento para documentar los motivos por los que no se puede notificar en el plazo de 72 horas	
Existe un procedimiento para facilitar la información de manera gradual cuando no es posible facilitarla simultáneamente	
Se documenta cualquier brecha de seguridad de los datos personales	
En la documentación se incluyen los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas	
Se ha comprobado que el procedimiento de notificación funciona	

22. COMUNICACIÓN DE UNA BRECHA AL INTERESADO	CUMPLE SI/NO
Existe un procedimiento para comunicar la brecha sin dilación indebida cuando sea probable que entrañe un alto riesgo para los derechos y libertades	
La comunicación al interesado se lleva a cabo en un lenguaje claro y sencillo, describe la naturaleza de la brecha	

23. EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS	CUMPLE SI/NO
Se recaba el asesoramiento del DPD	

Se realiza EIPD antes del tratamiento cuando es probable que entrañe un alto riesgo para los derechos y libertades de las personas	
Se realiza una EIPD antes en tratamientos a gran escala de categorías especiales de datos o relativos a condenas e infracciones penales	
Se realiza una EIPD antes de tratamiento que suponen una observación sistemática a gran escala de una zona de acceso público	
Se realiza una EIPD en operaciones de tratamiento incluidas en la lista publicada por la autoridad de control	
La EIPD incluye una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, y cuando procede el interés legítimo perseguido	
Incluye una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad	
La EIPD incluye una evaluación de los riesgos para los derechos y libertades Incluye medidas previstas para demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas	
Incluye las medidas previstas para afrontar los riesgos, garantías y mecanismos para garantizar la protección de datos	
Se reexaminan las EIPD siempre que es necesario y cuando exista un cambio de los riesgos que representen las operaciones de tratamiento	
Se consulta a la autoridad de control antes de proceder al tratamiento cuando una EIPD muestre que el mismo entrañaría un alto riesgo si no se toman medidas para mitigarlo	
Se informa de las responsabilidades respectivas de los implicados en el tratamiento en la consulta a la autoridad de control	
Se informa de los fines y medios del tratamiento previsto en la consulta	
Se informa de las medidas y garantías establecidas para proteger los derechos y libertades en la consulta	
Se facilitan los datos de contacto del delegado de protección de datos	
Se incluye la evaluación de impacto	
Cuando se consulta se facilita cualquier información adicional que solicite la autoridad de control	

24. DELEGADO DE PROTECCIÓN DE DATOS	CUMPLE SI/NO
Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia	
Se ha designado un DPD por requerimiento legal	
Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control	
Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales	
Se da respaldo en el desempeño sus funciones	
Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento Se le facilitan los recursos necesarios para mantener sus conocimientos	
Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones	
No se puede destituir ni sancionar al DPD por desempeñar sus funciones	
El DPD rinde cuentas directamente al más alto nivel jerárquico	
El DPD atiende las solicitudes de los interesados	
El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones	
Si el DPD desempeña otras funciones, se garantiza que no dan lugar a conflicto de intereses	
Las funciones del DPD son informar, asesorar y formar al personal de las obligaciones que les incumben	
El DPD coopera y actúa como punto de contacto con la autoridad de control	

25. TRANSFERENCIAS A PAÍSES TERCEROS U ORGANIZACIONES INTERNACIONALES	CUMPLE SI/NO
Se realizan transferencias a países, o sectores de los mismos, u organizaciones internacionales declarados de nivel de protección adecuado por la Comisión Europea	
Se realiza un seguimiento de la validez de las decisiones de adecuación de la Comisión europea	
Se realizan transferencias mediante garantías adecuadas que ofrezcan a los interesados derechos exigibles y posibilidad de acciones legales.	
Existe un instrumento jurídico vinculante y exigible entre las autoridades u organismos públicos	

Existen normas corporativas vinculantes	
Existen cláusulas tipo de protección de datos adoptadas por la Comisión	
Existen cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión	
Existe un código de conducta junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existe un mecanismo de certificación junto con compromisos vinculantes y exigibles en el tercer país que permita aplicar garantías adecuadas	
Existen cláusulas contractuales que requieren la autorización previa de la autoridad de control	
Existen acuerdos administrativos entre autoridades y organismos públicos que incorporen disposiciones que incluyan derechos efectivos y exigibles para los interesados	
Se realizan transferencias internacionales en ausencia de decisión de adecuación de la Comisión europea y de garantías adecuadas	
Se dispone del consentimiento explícito del interesados y se le ha informado de los posibles riesgos	
Son necesarias para la ejecución de un contrato con el interesado o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado	
Son necesarias para la formulación, ejercicio o la defensa de reclamaciones	
Son necesarias para la protección de los intereses vitales del interesado o de otras personas, cuando el interesado esté incapacitado para dar su consentimiento	
Por intereses legítimos imperiosos	
Afecta a un número limitado de interesados y no es repetitiva	

Se han evaluado todas las circunstancias concurrentes y se han ofrecido garantías apropiadas	
Se ha informado a la autoridad de control	