NOR09 – Política de protecció de dades

Compliment del reglament (UE) 2016/679 i la normativa espanyola de protecció de dades.

CONTROL DE FIRMES

	DATA	FIRMA
ELABORAT PER MARIA SANCHIS	24/05/2021	
APROVAT PER COMITÉ DE SEGURETAT DE LA INFORMACIÓ	24/05/2021	

CONTROL DE VERSIONS

VERSIÓ	DATA	AUTOR	CANVIS
1.0	24/05/2021	María Sanchis	Versió inicial del document.
2.0	16/09/2024	María Sanchis	Actualització de l'apartat 3 i 4.

ÍNDEX DE CONTINGUT

IDENTIFICACIÓ DE LA PERSONA RESPONSABLE DEL TRACTAMENT

a) Nom i dades de contacte de la persona responsable del tractament:

- Denominació social / Nom i cognoms: AJUNTAMENT DE PAIPORTA
- CIF/NIF: P4618800I
- Activitat: ADMINISTRACIÓ PÚBLICA, AJUNTAMENT
- Telèfon de contacte: 96 397 12 22
- Domicili social: CARRER MESTRE MÚSIC VICENT PRATS I TARAZONA S/N, 46200 , PAIPORTA, (València)
- Domicili a efecte de notificacions: CARRER MESTRE MÚSIC VICENT PRATS I TARAZONA S/N, 46200, PAIPORTA, (València)
- Adreça electrònica de contacte: secretaria@paiporta.es
- Pàgina web (URL): https://paiporta.es/

b) Nom i dades de contacte de la persona corresponsable del tractament:

- No existeix la figura de la persona corresponsable del tractament.

c) Nom i dades de contacte de la persona representant del responsable:

- La persona representant del tractament està establida en el territori de la Unió Europea.

d) Nom i dades de contacte de la persona delegada de protecció de dades:

- Denominació social / Nom i cognoms: AUDIDAT 3.0 SLU.
- Adreça electrònica de contacte: dpd@audidat.com

I. OBJECTE DEL DOCUMENT.

L'Agència Espanyola de Protecció de Dades va plasmar, en el seu Pla estratègic 2015-2019, la seua voluntat que les persones responsables del tractament aconseguisquen un elevat compliment de les obligacions que la normativa de protecció de dades els imposa, que fomenten una cultura de la protecció de dades que supose una clara millora de la competitivitat, compatible amb el desenvolupament econòmic.

El Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) (DOUE L 119/1, 04-05-2016) (d'ara en avant, RGPD), proporciona un marc modernitzat i basat en la rendició de comptes per a la protecció de les dades a Europa.

En tal sentit, l'article 5, apartat 2, del Reglament (UE) 2016/679, estableix expressament el principi de «responsabilitat proactiva», segons el qual la persona responsable del tractament serà responsable del compliment (i capaç de demostrar-lo) dels següents principis relatius al tractament:

- Les dades personals seran tractades de manera lícita, lleial i transparent en relació amb la persona interessada («licitud, lleialtat i transparència»).

- Les dades personals seran arreplegades amb finalitats determinades, explícites i legítimes, i no seran tractades ulteriorment de manera incompatible amb aquestes finalitats; d'acord amb l'article 89, apartat 1, el tractament ulterior de les dades personals amb finalitats d'arxiu en interès públic, finalitats d'investigació científica i històrica o finalitats estadístiques no es considerarà incompatible amb les finalitats inicials («limitació de la finalitat»).
- Les dades personals seran adequades, pertinents i limitades al necessari en relació amb les finalitats per a les quals són tractades («minimització de dades»).
- Les dades personals seran exactes i, si fora necessari, actualitzades; s'adoptaran totes les mesures raonables perquè se suprimisquen o rectifiquen sense dilació les dades personals que siguen inexactes respecte a les finalitats per a les quals es tracten («exactitud»).
- Les dades personals seran mantingudes de manera que es permeta la identificació de les persones interessades durant no més temps del necessari per a les finalitats del tractament de les dades personals; les dades personals podran conservar-se durant períodes més llargs sempre que es tracten exclusivament amb finalitats d'arxiu en interès públic, finalitats d'investigació científica o històrica o finalitats estadístiques, de conformitat amb l'article 89, apartat 1, sense perjudici de l'aplicació de les mesures tècniques i organitzatives apropiades que imposa el present Reglament a fi de protegir els drets i llibertats de la perdona interessada («limitació del termini de conservació»).
- Les dades personals seran tractades de tal manera que es garantisca una seguretat adequada de les dades personals, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seua pèrdua, destrucció o mal accidental, mitjançant l'aplicació de mesures tècniques o organitzatives apropiades («integritat i confidencialitat»).

En síntesi, el principi de «responsabilitat proactiva» exigeix una actitud conscient, diligent i proactiva per part de les organitzacions enfront de tots els tractaments de dades personals que duguen a terme.

En tal sentit, la Direcció / Òrgan de Govern d'AJUNTAMENT DE PAIPORTA advoca per una política proactiva de compliment, darrere d'aconseguir que en el desenvolupament de les seues finalitats es respecte de forma activa el dret fonamental a la protecció de dades.

En la seua conseqüència, el present document s'elabora a fi d'establir la Política d'AJUNTAMENT DE PAIPORTA en relació amb el compliment 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 (Reglament general de protecció de dades) (DOUE L 119/1, 04-05-2016), i en la normativa espanyola de protecció de dades de caràcter personal (Llei orgànica, les seues normes de desenvolupament i la legislació sectorial específica).

II. COMPROMÍS DE LA DIRECCIÓ / ÒRGAN DE GOVERN AMB LA PROTECCIÓ DE DADES.

La Direcció / Òrgan de Govern d'AJUNTAMENT DE PAIPORTA (d'ara en avant, el responsable del tractament), assumeix la màxima responsabilitat i compromís amb l'establiment, implementació i manteniment de la present Política de Protecció de Dades, i garanteix la millora contínua del responsable del tractament amb l'objectiu d'aconseguir l'excel·lència en relació amb el compliment 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 (Reglament general de protecció de dades) (DOUE L 119/1, 04-05-2016), i de la normativa espanyola de protecció de dades de caràcter personal (Llei orgànica, legislació sectorial específica i les seues normes de desenvolupament).

La Política de Protecció de Dades d'AJUNTAMENT DE PAIPORTA descansa en el principi de responsabilitat proactiva, segons el qual el responsable del tractament és responsable del compliment del marc normatiu i jurisprudencial que governa aquesta Política, i és capaç de demostrar-lo davant les autoritats de control competents.

En tal sentit, el responsable del tractament es regirà pels següents principis que han de servir a tot el seu personal com a guia i marc de referència en el tractament de dades personals:

1. Protecció de dades des del disseny: el responsable del tractament aplicarà, tant en el moment de determinar els mitjans de tractament com en el moment del propi tractament, mesures tècniques i organitzatives apropiades, com la seudonimització, concebudes per a aplicar de forma efectiva els principis de protecció de dades, com la minimització de dades, i integrar les garanties necessàries en el tractament.
2. Protecció de dades per defecte: el responsable del tractament aplicarà les mesures tècniques i organitzatives apropiades amb la intenció de garantir que, per defecte, només siguen objecte de tractament les dades personals que siguen necessàries per a cadascuna de les finalitats específiques del tractament.
3. Protecció de dades en el cicle de vida de la informació: les mesures que garantisquen la protecció de les dades personals seran aplicables durant el cicle complet de la vida de la informació.
4. Licitud, lleialtat i transparència: les dades personals seran tractades de manera lícita, lleial i transparent en relació amb l'interessat.
5. Limitació de la finalitat: les dades personals seran arreplegades amb finalitats determinades, explícides i legítimes, i no seran tractades ulteriorment de manera incompatible amb aquestes finalitats.
6. Minimització de dades: les dades personals seran adequades, pertinents i limitades al necessari en relació amb les finalitats per a les quals són tractades.
7. Exactitud: les dades personals seran exactes i, si fora necessari, actualitzades; s'adoptaran totes les mesures raonables perquè se suprimisquen o rectifiquen sense dilació les dades personals que siguen inexactes respecte a les finalitats per a les quals es tracten.
8. Limitació del termini de conservació: les dades personals seran mantingudes de manera que es permeta la identificació de les persones interessades durant no més temps del necessari per a les finalitats del tractament de les dades personals.
9. Integritat i confidencialitat: les dades personals seran tractades de tal manera que es garantisca una seguretat adequada de les dades personals, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seua pèrdua, destrucció o mal accidental, mitjançant l'aplicació de mesures tècniques o organitzatives apropiades.
10. Informació i formació: una de les claus per a garantir la protecció de les dades personals és la formació i informació que es facilite al personal involucrat en el tractament d'aquests. Durant el cicle de vida de la informació, tot el personal amb accés a les dades serà convenientment

format i informat sobre les seues obligacions en relació amb el compliment de la normativa de protecció de dades.

La Política de Protecció de Dades d'AJUNTAMENT DE PAIPORTA és comunicada a tot el personal del responsable del tractament i posada a la disposició de totes les parts interessades.

En la seua conseqüència, la present Política de Protecció de Dades involucra a tot el personal del responsable del tractament, que ha de conèixer-la i assumir-la, i considerar-la com a pròpia, sent cada membre responsable d'aplicar-la i de verificar les normes de protecció de dades aplicables a la seua activitat, així com identificar i aportar les oportunitats de millora que considere oportunes amb l'objectiu d'aconseguir l'excel·lència en relació amb el seu compliment.

Aquesta Política serà revisada per la Direcció / Òrgan de Govern d'AJUNTAMENT DE PAIPORTA, tantes vegades com es considere necessari, per a adequar-se, en tot moment, a les disposicions vigents en matèria de protecció de dades de caràcter personal.

III. NECESSITAT DE DISPOSAR D'UNA PERSONA DELEGADA DE PROTECCIÓ DE DADES.

Es detecta la necessitat de disposar d'una persona delegada de Protecció de Dades, sobre la base dels següents supòsits:

- El tractament el duu a terme una autoritat o organisme públic.

Concepte d' "observació habitual i sistemàtica"

La noció d'observació habitual i sistemàtica de persones interessades no està definida en el RGPD, però el concepte d' «observació del comportament dels interessats» s'esmenta en el considerant 24 i inclou clarament tota forma de seguiment i creació de perfils en internet, també amb finalitats de publicitat comportamental:

> Per a determinar si es pot considerar que una activitat de tractament controla el comportament dels interessats, ha d'avaluar-se si les persones físiques són objecte d'un seguiment en internet, inclusivament el potencial ús posterior de tècniques de tractament de dades personals que consistisquen en l'elaboració d'un perfil d'una persona física amb la finalitat, en particular, d'adoptar decisions sobre ell o d'analitzar o predir les seues preferències personals, comportaments i actituds.

No obstant això, el concepte d'observació no es limita a l'entorn en línia i el seguiment en línia ha de considerar-se només un exemple d'observació del comportament dels interessats.

El Grup de Treball de l'article 29 interpreta «habitual» amb un o més dels següents significats:

- Continuat o que es produeix a intervals concrets durant un període concret.
- Recurrent o repetit en moments prefixats.
- Que té lloc de manera constant o periòdica.

El Grup de Treball interpreta «sistemàtic» amb un o més dels següents significats:

- Que es produeix d'acord amb un sistema.

- Preestablit, organitzat o metòdic.
- Que té lloc com a part d'un Pla general de recollida de dades.
- Dut a terme com a part d'una estratègia.

Exemples d'activitats que poden constituir una observació habitual i sistemàtica d'interessats són:

- Operar una xarxa de telecomunicacions.
- Prestar serveis de telecomunicacions.
- Redirigir correus electrònics.
- Activitats de màrqueting basades en dades.
- Elaborar de perfils i atorgar puntuació amb finalitats d'avaluació de riscos (p. ex. per a determinar la qualificació creditícia, establir primes d'assegurances, prevenir el frau, detectar blanqueig de diners).
- Dur a terme un seguiment de la ubicació, per exemple, mitjançant aplicacions mòbils.
- Programes de fidelitat.
- Publicitat comportamental.
- Seguiment de les dades de benestar, estat físic i salut mitjançant dispositius ponibles.
- Televisió de circuit tancat.
- Dispositius connectats, com a comptadors intel·ligents, cotxes intel·ligents, domòtica, etc.

Concepte d' "a gran escala"

El Grup de Treball de l'article 29 recomana que es tinguen en compte els següents factors a l'hora de determinar si el tractament es realitza a gran escala:

- El nombre de persones interessades afectats, bé com a xifra concreta o com a proporció de la població corresponent.
- El volum de dades o la varietat d'elements de dades que són objecte de tractament.
- La duració, o permanència, de l'activitat de tractament de dades.
- L'abast geogràfic de l'activitat de tractament.

Com a exemples de tractament a gran escala cal citar:

- El tractament de dades de pacients en el desenvolupament normal de l'activitat d'un hospital.
- El tractament de dades de desplaçament de les persones que utilitzen el sistema de transport públic d'una ciutat (p. ex. seguiment a través de targetes de transport).
- El tractament de dades de geolocalització en temps real de clients d'una cadena internacional de menjar ràpid amb finalitats estadístics per part d'un responsable del tractament especialitzat en la prestació d'aquests serveis.
- El tractament de dades de clients en el desenvolupament normal de l'activitat d'una companyia d'assegurances o d'un banc.
- El tractament de dades personals per a publicitat comportamental per un motor de cerca.
- El tractament de dades (contingut, trànsit, ubicació) per empreses proveïdores de serveis de telefonia o internet.

Com a casos que no constitueixen tractament a gran escala cal assenyalar:

- El tractament de dades de pacients per part de només una persona mèdica.
- El tractament de dades personals relatives a condemnes i infraccions penals per part d'una persona advocada.

IV. NECESSITAT DE REALITZAR UNA AVALUACIÓ D'IMPACTE.

NO es detecta la necessitat de realitzar una avaluació d'impacte.

Això és pel fet que **no** es dona cap dels següents supòsits:

- El responsable realitza una **avaluació sistemàtica i exhaustiva** d'aspectes personals de persones físiques que es basa en un tractament automatitzat, com **l'elaboració de perfils**, i sobre la base dels quals es prenen decisions que produïsquen efectes jurídics per a les persones físiques o que els afecten significativament de manera similar.

- El responsable realitza tractaments **a gran escala** de **categories especials** de dades personals:
  - Dades personals que revelen l'origen ètnic o racial.
  - Dades personals que revelen les opinions polítiques.
  - Dades personals que revelen les conviccions religioses o filosòfiques.
  - Dades personals que revelen l'afiliació sindical.
  - Dades genètiques.
  - Dades biomètriques dirigides a identificar de manera unívoca a persones físiques.
  - Dades relatives a la salut (física o mental).
  - Dades relatives a la vida sexual o l'orientació sexual de persones físiques.

- Dades relatives a condemnes i infraccions penals, així com a procediments i mesures cautelars i de seguretat connexes.

- El responsable realitza una observació sistemàtica a gran escala d'una zona d'accés públic.

Concepte de "sistemàtic"

El Grup de Treball interpreta «sistemàtic» amb un o més dels següents significats:

- *Que es produeix d'acord amb un sistema.*
- *Preestablit, organitzat o metòdic.*
- *Que té lloc com a part d'un pla general de recollida de dades.*
- *Dut a terme com a part d'una estratègia.*

V. AVALUACIÓ DEL RISC.

Determinació del risc

La major novetat que presenta el Reglament (UE) 2016/679 és l'evolució d'un model basat, fonamentalment, en el control del compliment a un altre que descansa en el principi de responsabilitat activa, la qual cosa exigeix una prèvia valoració pel responsable del tractament del risc que poguera generar el tractament de les dades de caràcter personal per a, a partir d'aquesta valoració, adoptar les mesures que procedisquen.

De tal manera, el responsable del tractament està obligat a aplicar mesures oportunes i eficaces i ha de poder demostrar la conformitat de les activitats de tractament amb el citat Reglament, amb la Llei orgànica, les seues normes de desenvolupament i la legislació sectorial específica, inclosa l'eficàcia d'aquestes mesures. Aquestes mesures han de tenir en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, així com el risc per als drets i llibertats de les persones físiques.

En la seua conseqüència, el responsable del tractament aplicarà les mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc. En avaluar l'adequació del nivell de seguretat es tindran particularment en compte els riscos que presente el tractament de dades, en particular com a conseqüència de la destrucció, pèrdua o alteració accidental o il·lícita de dades personals transmeses, conservades o tractades d'una altra forma, o la comunicació o accés no autoritzats a aquestes dades.

En tal sentit, els riscos per als drets i llibertats de les persones físiques, de gravetat i probabilitat variables, poden deure's al tractament de dades que pogueren provocar danys i perjudicis físics, materials o immaterials, en particular en els casos següents:

- En els casos en els quals el tractament puga donar lloc a problemes de discriminació, usurpació d'identitat o frau, pèrdues financeres, mal per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la seudonimització o qualsevol altre perjudici econòmic o social significatiu.
- En els casos en els quals es prive a les persones interessades dels seus drets i llibertats o se'ls impedisca exercir el control sobre les seues dades personals.
- En els casos en els quals les dades personals tractades revelen l'origen ètnic o racial, les opinions polítiques, la religió o creences filosòfiques, la militància en sindicats i el tractament de dades genètiques, dades relatives a la salut o dades sobre la vida sexual, o les condemnes i infraccions penals o mesures de seguretat connexes.
- En els casos en els quals s'avaluen aspectes personals, en particular l'anàlisi o la predicció d'aspectes referits al rendiment en el treball, situació econòmica, salut, preferències o interessos personals, fiabilitat o comportament, situació o moviments, amb la finalitat de crear o utilitzar perfils personals.
- En els casos en els quals es tracten dades personals de persones vulnerables, en particular xiquets.
- En els casos en els quals el tractament implique una gran quantitat de dades personals i afecte un gran nombre de persones interessades.

Determinació del risc de les operacions de tractament.

La probabilitat i la gravetat del risc per als drets i llibertats de la persona interessada ha de determinar-se amb referència a la naturalesa, l'abast, el context i les finalitats del tractament de dades. Així, el risc ha de ponderar-se sobre la base d'una avaluació objectiva mitjançant la qual es determine si les operacions de tractament de dades suposen un **escàs risc, risc (risc estàndard) o un alt risc**.

A l'efecte de la present política de protecció de dades, haurà de considerar-se que les operacions del tractament suposen un **alt risc** per als drets i llibertats de les persones físiques en els següents supòsits:

1. Quan el tractament puga generar situacions de discriminació, usurpació d'identitat o frau, pèrdues financeres, mal per a la reputació, pèrdua de confidencialitat de dades subjectes al secret professional, reversió no autoritzada de la seudonimització o qualsevol altre perjudici econòmic, moral o social significatiu per a les persones afectades.

2. Quan el tractament puga privar a les persones afectades dels seus drets i llibertats o puga impedir-les l'exercici del control sobre les seues dades personals.

3. Quan es produïsca el tractament no merament incidental o accessori de les següents categories de dades:

- Dades personals que revelen l'origen ètnic o racial.
- Dades personals que revelen les opinions polítiques.
- Dades personals que revelen les conviccions religioses o filosòfiques.
- Dades personals que revelen l'afiliació sindical.
- Dades genètiques.
- Dades biomètriques dirigides a identificar de manera unívoca a una persona física.
- Dades relatives a la salut.
- Dades relatives a la vida sexual o l'orientació sexual d'una persona física.
- Dades personals relatives a condemnes i infraccions penals, així com a procediments i mesures cautelars i de seguretat connexes.

4. Quan el tractament implicara una avaluació d'aspectes personals de les persones afectades amb la finalitat de crear o utilitzar perfils personals d'aquests, en particular mitjançant l'anàlisi o la predicció d'aspectes referits al seu rendiment en el treball, la seua situació econòmica, la seua salut, les seues preferències o interessos personals, la seua fiabilitat o comportament, la seua solvència financera, la seua localització o els seus moviments.

5. Quan es duga a terme el tractament de dades de grups d'afectats en situació d'especial vulnerabilitat i, en particular, de menors d'edat i persones amb discapacitat.

6. Quan es produïsca un tractament massiu que afecte un gran nombre de persones afectades o implique la recollida d'una gran quantitat de dades personals.

7. Quan les dades de caràcter personal anaren a ser objecte de transferència, amb caràcter habitual, a tercers Estats o organitzacions internacionals respecte dels quals no s'haguera declarat un nivell adequat de protecció. En tal sentit, es considera que tenen un nivell adequat de protecció els següents Estats:

   - Els Estats de **l'Espai Econòmic Europeu (EEE):**

     - Estats de la Unió Europea.
     - Islàndia.
     - Liechtenstein.
     - Noruega.

   - **Suïssa**. Decisió 2000/518/CE de la Comissió, de 26 de juliol de 2000.
   - **El Canadà**. Decisió 2002/2/CE de la Comissió, de 20 de desembre de 2001, respecte de les entitats subjectes a l'àmbit d'aplicació de la llei canadenca de protecció de dades.
   - **L'Argentina.** Decisió 2003/490/CE de la Comissió, de 30 de juny de 2003.
   - **Guernsey**. Decisió 2003/821/CE de la Comissió, de 21 de novembre de 2003.

- **Illa de Man**. Decisió 2004/411/CE de la Comissió, de 28 d'abril de 2004.
- **Jersey.** Decisió 2008/393/CE de la Comissió, de 8 de maig 2008.
- **Illes Fèroe**. Decisió 2010/146/UE de la Comissió, de 5 de març de 2010.
- **Andorra**. Decisió 2010/625/UE de la Comissió, de 19 d'octubre de 2010.
- **Israel**. Decisió 2011/61/UE de la Comissió, de 31 de gener de 2011.
- **L'Uruguai**. Decisió 2012/484/UE de la Comissió, de 21 d'agost de 2012.
- **Nova Zelanda**. Decisió 2013/65/UE de la Comissió, de 19 de desembre de 2012.
- **Els Estats Units**. Aplicable a les entitats certificades en el marc de l'Escut de Privacitat UE-EEUU Decisió (UE) 2016/1250 de la Comissió, de 12 de juliol de 2016. En la pàgina web de l'Escut de privacitat s'accedeix a la relació de les entitats certificades: https://www.privacyshield.gov/list.

8. Altres supòsits de risc sobre la base de l'activitat del responsable del tractament.

VI. REGISTRE D'ACCIONS INFORMATIVES I FORMATIVES.

La Política de Protecció de Dades d'AJUNTAMENT DE PAIPORTA descansa en el principi de responsabilitat proactiva, segons el qual el responsable del tractament és responsable del compliment del marc normatiu i jurisprudencial que governa aquesta Política, i és capaç de demostrar-lo davant les autoritats de control competents.

En tal sentit, el responsable del tractament es regeix, entre altres, pel principi d'informació i formació, segons el qual una de les claus per a garantir la protecció de les dades personals és la formació i informació que es facilite al personal involucrat en el tractament d'aquests, educant als empleats i empleades en la denominada cultura de la protecció de dades.

En la seua conseqüència, tot el personal de l'entitat amb accés a les dades serà convenientment format i informat sobre les seues obligacions en relació amb el compliment de la normativa de protecció de dades, i rebran l'apropiat coneixement, capacitació i actualitzacions regulars de la Política de Protecció de Dades d'AJUNTAMENT DE PAIPORTA.

En relació amb la metodologia de les accions informatives i formatives, es recomana la combinació de diferents metodologies per a una millor assimilació dels coneixements per part de les persones participants, citant a tall d'exemple les següents:

- Exposició de continguts o classe magistral: el docent explica els continguts de forma teòrica amb ajuda de recursos com són presentacions de PowerPoint.
- Simulacions o estudi del cas: el docent proposa situacions a resoldre per part de les persones participants, que li permeten assimilar millor els coneixements adquirits.
- Dinàmiques de grup: amb la finalitat d'activar la interacció entre les persones participants i el docent.

En relació amb el personal docent, es recomana acudir a professionals de la protecció de dades i de la privacitat amb experiència docent prèvia. Aquesta funció pot recaure sobre la persona delegada de protecció de dades de l'entitat responsable del tractament, en el cas que s'haguera designat com a tal.

Així mateix, en finalitzar l'acció formativa, s'aconsella la realització de proves d'avaluació de coneixements a les persones participants.

Amb la finalitat de la gestió de control intern del compliment del principi d'informació i formació en el si de l'entitat, s'ha elaborat un "Registre d'accions formatives i informatives" per al personal en matèria de protecció de dades.

REGISTRE D'ACCIONS INFORMATIVES I FORMATIVES		
REF. ACCIÓ INFORMATIVA I/O FORMATIVA Nº 1		
Identificació de l'acció informativa i/o formativa		
Denominació de l'acció		
Nom de l'entitat impartidora		
Dades de contacte de l'entitat impartidora		
Caracterització de l'acció informativa i/o formativa		
Modalitat de formació		Formació presencial
		Teleformació
Objetius de l'acció formativa		
Perfil de les persones participants		
Duració de l'acció formativa		
Descripció abreviada del programa i continguts de l'acció formativa		
Metodologia de l'acció formativa		
Personal docent		
Recursos didàctics utilitzats en la formació		
Avaluació de la formació		

REGISTRE D'ACCIONS INFORMATIVES I FORMATIVES		
REF. ACCIÓ INFORMATIVA i/O FORMATIVA Nº 2		
Identificació de l'acció informativa i/o formativa		
Denominació de l'acció		
Nom de l'entitat impartidora		
Dades de contacte de l'entitat impartidora		
Caracterització de l'acció informativa i/o formativa		
Modalitat de formació		Formació presencial
		Teleformació
Objetius de l'acció formativa		
Perfil de les persones participants		
Duració de l'acció formativa		
Descripció abreviada del programa i continguts de l'acció formativa		
Metodologia de l'acció formativa		
Personal docent		
Recursos didàctics utilitzats en la formació		
Avaluació de la formació		

NOR09 – Política de protección de datos

Cumplimiento del reglamento (UE) 2016/679 y la normativa española de protección de datos.

CONTROL DE FIRMAS

	DATA	FIRMA
ELABORADO POR MARIA SANCHIS	24/05/2021	
APROBADO POR COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	24/05/2021	

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	24/05/2021	María Sanchis	Versión inicial del documento.
2.0	16/09/2024	María Sanchis	Actualización del apartado 3 y 4.

ÍNDICE DE CONTENIDO

IDENTIFICACIÓN DEL RESPONSABLE DEL TRATAMIENTO

a) Nombre y datos de contacto del responsable del tratamiento:

- Denominación social / Nombre y apellidos: AYUNTAMIENTO DE PAIPORTA
- CIF/NIF: P4618800I
- Actividad: ADMINISTRACIÓN PÚBLICA, AYUNTAMIENTO
- Teléfono de contacto: 96 397 12 22
- Domicilio social: CARRER MESTRE MÚSIC VICENT PRATS I TARAZONA S/N, 46200 , PAIPORTA, (Valencia/València)
- Domicilio a efecto de notificaciones: CARRER MESTRE MÚSIC VICENT PRATS I TARAZONA S/N, 46200 , PAIPORTA, (Valencia/València)
- Dirección electrónica de contacto: secretaria@paiporta.es
- Página web (URL): https://paiporta.es/

b) Nombre y datos de contacto del corresponsable del tratamiento:

- No existe la figura del corresponsable del tratamiento

c) Nombre y datos de contacto del representante del responsable:

- El representante del tratamiento está establecido en el territorio de la Unión Europea

d) Nombre y datos de contacto del delegado de protección de datos:

- Denominación social / Nombre y apellidos: AUDIDAT 3.0 SLU
- Dirección electrónica de contacto: dpd@audidat.com

I. OBJETO DEL DOCUMENTO.

La Agencia Española de Protección de Datos plasmó, en su Plan Estratégico 2015-2019, su voluntad de que los responsables del tratamiento alcancen un elevado cumplimiento de las obligaciones que la normativa de protección de datos les impone, fomentando una cultura de la protección de datos que suponga una clara mejora de la competitividad, compatible con el desarrollo económico.

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016) (en adelante, RGPD), proporciona un marco modernizado y basado en la rendición de cuentas para la protección de los datos en Europa.

En tal sentido, el artículo 5, apartado 2, del Reglamento (UE) 2016/679, establece expresamente el principio de «responsabilidad proactiva», según el cual el responsable del tratamiento será responsable del cumplimiento (y capaz de demostrarlo) de los siguientes principios relativos al tratamiento:

- Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

- Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

- Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

- Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

- Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

- Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

En síntesis, el principio de «responsabilidad proactiva» exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

En tal sentido, la Dirección / Órgano de Gobierno de AYUNTAMIENTO DE PAIPORTA aboga por una política proactiva de cumplimiento, en pos de conseguir que en el desarrollo de sus fines se respete de forma activa el derecho fundamental a la protección de datos.

En su consecuencia, el presente documento se elabora con el objeto de establecer la Política de AYUNTAMIENTO DE PAIPORTA en relación con el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), y en la normativa española de protección de datos de carácter personal (Ley Orgánica, sus normas de desarrollo y la legislación sectorial específica).

II. COMPROMISO DE LA DIRECCIÓN / ÓRGANO DE GOBIERNO CON LA PROTECCIÓN DE DATOS.

La Dirección / Órgano de Gobierno de AYUNTAMIENTO DE PAIPORTA (en adelante, el responsable del tratamiento), asume la máxima responsabilidad y compromiso con el establecimiento, implementación y mantenimiento de la presente Política de Protección de Datos, garantizando la mejora continua del responsable del tratamiento con el objetivo de alcanzar la excelencia en relación con el cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), y de la normativa española de protección de datos de carácter personal (Ley Orgánica, legislación sectorial específica y sus normas de desarrollo).

La Política de Protección de Datos de AYUNTAMIENTO DE PAIPORTA descansa en el principio de responsabilidad proactiva, según el cual el responsable del tratamiento es responsable del cumplimiento del marco normativo y jurisprudencial que gobierna dicha Política, y es capaz de demostrarlo ante las autoridades de control competentes.

En tal sentido, el responsable del tratamiento se regirá por los siguientes principios que deben servir a todo su personal como guía y marco de referencia en el tratamiento de datos personales:

1. Protección de datos desde el diseño: el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento.

2. Protección de datos por defecto: el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

3. Protección de datos en el ciclo de vida de la información: las medidas que garanticen la protección de los datos personales serán aplicables durante el ciclo completo de la vida de la información.

4. Licitud, lealtad y transparencia: los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado.

5. Limitación de la finalidad: los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

6. Minimización de datos: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

7. Exactitud: los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

8. Limitación del plazo de conservación: los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

9. Integridad y confidencialidad: los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

10. Información y formación: una de las claves para garantizar la protección de los datos personales es la formación e información que se facilite al personal involucrado en el tratamiento de los mismos. Durante el ciclo de vida de la información, todo el personal con acceso a los datos será convenientemente formado e informado acerca de sus obligaciones en relación con el cumplimiento de la normativa de protección de datos.

La Política de Protección de Datos de AYUNTAMIENTO DE PAIPORTA es comunicada a todo el personal del responsable del tratamiento y puesta a disposición de todas las partes interesadas.

En su consecuencia, la presente Política de Protección de Datos involucra a todo el personal del responsable del tratamiento, que debe conocerla y asumirla, considerándola como propia, siendo cada miembro responsable de aplicarla y de verificar las normas de protección de datos aplicables a su actividad, así como identificar y aportar las oportunidades de mejora que considere oportunas con el objetivo de alcanzar la excelencia en relación con su cumplimiento.

Esta Política será revisada por la Dirección / Órgano de Gobierno de AYUNTAMIENTO DE PAIPORTA, tantas veces como se considere necesario, para adecuarse, en todo momento, a las disposiciones vigentes en materia de protección de datos de carácter personal.

III. NECESIDAD DE DISPONER DE UN DELEGADO DE PROTECCIÓN DE DATOS.

Se detecta la necesidad de disponer de un Delegado de Protección de Datos, en base a los siguientes supuestos:

- El tratamiento lo lleva a cabo una autoridad u organismo público

Concepto de "observación habitual y sistemática"

La noción de observación habitual y sistemática de interesados no está definida en el RGPD, pero el concepto de «observación del comportamiento de los interesados» se menciona en el considerando 24 e incluye claramente toda forma de seguimiento y creación de perfiles en internet, también con fines de publicidad comportamental:

> Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una

persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

No obstante, el concepto de observación no se limita al entorno en línea y el seguimiento en línea debe considerarse solo un ejemplo de observación del comportamiento de los interesados.

El Grupo de Trabajo del artículo 29 interpreta «habitual» con uno o más de los siguientes significados:

- Continuado o que se produce a intervalos concretos durante un periodo concreto;
- Recurrente o repetido en momentos prefijados;
- Que tiene lugar de manera constante o periódica.

El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados:

- Que se produce de acuerdo con un sistema;
- Preestablecido, organizado o metódico;
- Que tiene lugar como parte de un plan general de recogida de datos;
- Llevado a cabo como parte de una estrategia.

Ejemplos de actividades que pueden constituir una observación habitual y sistemática de interesados son:

- Operar una red de telecomunicaciones;
- Prestar servicios de telecomunicaciones;
- Redireccionar correos electrónicos;
- Actividades de mercadotecnia basadas en datos;
- Elaborar de perfiles y otorgar puntuación con fines de evaluación de riesgos (p. ej. para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude, detectar blanqueo de dinero);
- Llevar a cabo un seguimiento de la ubicación, por ejemplo, mediante aplicaciones móviles;
- Programas de fidelidad;
- Publicidad comportamental;
- Seguimiento de los datos de bienestar, estado físico y salud mediante dispositivos ponibles;
- Televisión de circuito cerrado;
- Dispositivos conectados, como contadores inteligentes, coches inteligentes, domótica, etc.

Concepto de "a gran escala"

El Grupo de Trabajo del artículo 29 recomienda que se tengan en cuenta los siguientes factores a la hora de determinar si el tratamiento se realiza a gran escala:

- El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
- El volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
- La duración, o permanencia, de la actividad de tratamiento de datos;
- El alcance geográfico de la actividad de tratamiento.

Como ejemplos de tratamiento a gran escala cabe citar:

- El tratamiento de datos de pacientes en el desarrollo normal de la actividad de un hospital;

- El tratamiento de datos de desplazamiento de las personas que utilizan el sistema de transporte público de una ciudad (p. ej. seguimiento a través de tarjetas de transporte);
- El tratamiento de datos de geolocalización en tiempo real de clientes de una cadena internacional de comida rápida con fines estadísticos por parte de un responsable del tratamiento especializado en la prestación de estos servicios;
- El tratamiento de datos de clientes en el desarrollo normal de la actividad de una compañía de seguros o de un banco;
- El tratamiento de datos personales para publicidad comportamental por un motor de búsqueda;
- El tratamiento de datos (contenido, tráfico, ubicación) por proveedores de servicios de telefonía o internet.

Como casos que no constituyen tratamiento a gran escala cabe señalar:

- El tratamiento de datos de pacientes por parte de un solo médico;
- El tratamiento de datos personales relativos a condenas e infracciones penales por parte de un abogado.

IV. NECESIDAD DE REALIZAR UNA EVALUACIÓN DE IMPACTO.

NO se detecta la necesidad de realizar una evaluación de impacto.

Esto es debido a que **no** se da ninguno de los siguientes supuestos:

- El responsable realiza una **evaluación sistemática y exhaustiva** de aspectos personales de personas físicas que se basa en un tratamiento automatizado, como la **elaboración de perfiles**, y sobre cuya base se toman decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.

- El responsable realiza tratamientos **a gran escala** de **categorías especiales** de datos personales:
  - Datos personales que revelen el **origen étnico o racial.**
  - Datos personales que revelen las **opiniones políticas.**
  - Datos personales que revelen las **convicciones religiosas o filosóficas.**
  - Datos personales que revelen la **afiliación sindical.**
  - Datos **genéticos.**
  - Datos **biométricos** dirigidos a identificar de manera unívoca a personas físicas.
  - Datos relativos a la **salud** (física o mental).
  - Datos relativos a la **vida sexual** o la **orientación sexual** de personas físicas.
  - Datos relativos a **condenas e infracciones penales**, así como a procedimientos y medidas cautelares y de seguridad conexas.

- El responsable realiza una **observación sistemática a gran escala** de una **zona de acceso público.**

Concepto de "sistemático"

El Grupo de Trabajo interpreta «sistemático» con uno o más de los siguientes significados:

- *Que se produce de acuerdo con un sistema;*
- *Preestablecido, organizado o metódico;*
- *Que tiene lugar como parte de un plan general de recogida de datos;*
- *Llevado a cabo como parte de una estrategia.*

V. EVALUACIÓN DEL RIESGO.

Determinación del riesgo

La mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan.

De tal modo, el responsable del tratamiento está obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el citado Reglamento, con la Ley Orgánica, sus normas de desarrollo y la legislación sectorial específica, incluida la eficacia de dichas medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

En su consecuencia, el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

En tal sentido, los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos siguientes:

- En los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo;

- En los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales;

- En los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas;

- En los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales;

- En los casos en los que se traten datos personales de personas vulnerables, en particular niños;

- En los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

Determinación del riesgo de las operaciones de tratamiento

La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. Así, el riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un **escaso riesgo**, **riesgo (riesgo estándar)** o un **alto riesgo**.

A los efectos de la presente política de protección de datos, deberá considerarse que las operaciones del tratamiento suponen un **alto riesgo** para los derechos y libertades de las personas físicas en los siguientes supuestos:

1. Cuando el tratamiento pueda generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

2. Cuando el tratamiento pueda privar a los afectados de sus derechos y libertades o pueda impedirles el ejercicio del control sobre sus datos personales.

3. Cuando se produzca el tratamiento **no meramente incidental o accesorio** de las siguientes categorías de datos:

    - Datos personales que revelen el origen étnico o racial.
    - Datos personales que revelen las opiniones políticas.
    - Datos personales que revelen las convicciones religiosas o filosóficas.
    - Datos personales que revelen la afiliación sindical.
    - Datos genéticos.
    - Datos biométricos dirigidos a identificar de manera unívoca a una persona física.
    - Datos relativos a la salud.
    - Datos relativos a la vida sexual o la orientación sexual de una persona física.
    - Datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas.

4. Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

5. Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

6. Cuando se produzca un tratamiento masivo que afecte a un gran número de afectados o implique la recogida de una gran cantidad de datos personales.

7. Cuando los datos de carácter personal fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección. En tal sentido, se considera que tienen un nivel adecuado de protección los siguientes Estados:

    - Los Estados del **Espacio Económico Europeo (EEE)**:
        - Estados de la Unión Europea.
        - Islandia.
        - Liechtenstein.
        - Noruega.

    - **Suiza**. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.
    - **Canadá**. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.
    - **Argentina**. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
    - **Guernsey**. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
    - **Isla de Man**. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
    - **Jersey**. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
    - **Islas Feroe**. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
    - **Andorra**. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
    - **Israel**. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
    - **Uruguay**. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
    - **Nueva Zelanda**. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.
    - **Estados Unidos**. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016. En la página web del Escudo de privacidad se accede a la relación de las entidades certificadas: https://www.privacyshield.gov/list.

8. Otros supuestos de riesgo en base a la actividad del responsable del tratamiento.

VI. REGISTRO DE ACCIONES INFORMATIVAS Y FORMATIVAS.

La Política de Protección de Datos de AYUNTAMIENTO DE PAIPORTA descansa en el principio de responsabilidad proactiva, según el cual el responsable del tratamiento es responsable del cumplimiento del marco normativo y jurisprudencial que gobierna dicha Política, y es capaz de demostrarlo ante las autoridades de control competentes.

En tal sentido, el responsable del tratamiento se rige, entre otros, por el principio de información y formación, según el cual una de las claves para garantizar la protección de los datos personales es la formación e información que se facilite al personal involucrado en el tratamiento de los mismos, educando a los empleados en la denominada cultura de la protección de datos.

En su consecuencia, todo el personal de la entidad con acceso a los datos será convenientemente formado e informado acerca de sus obligaciones en relación con el cumplimiento de la normativa de protección de datos, recibiendo el apropiado conocimiento, capacitación y actualizaciones regulares de la Política de Protección de Datos de AYUNTAMIENTO DE PAIPORTA.

En relación con la metodología de las acciones informativas y formativas, se recomienda la combinación de diferentes metodologías para una mejor asimilación de los conocimientos por parte de los participantes, citando a modo de ejemplo las siguientes:

- Exposición de contenidos o clase magistral: El docente explica los contenidos de forma teórica con ayuda de recursos como son presentaciones de PowerPoint.

- Simulaciones o estudio del caso: El docente propone situaciones a resolver por parte de los participantes, que le permiten asimilar mejor los conocimientos adquiridos.

- Dinámicas de grupo: Con el fin de activar la interacción entre los participantes y el docente.

En relación con el personal docente, se recomienda acudir a profesionales de la protección de datos y de la privacidad con experiencia docente previa. Esta función puede recaer sobre el propio delegado de protección de datos de la entidad responsable del tratamiento, en el caso de que se hubiese designado como tal. Asimismo, al finalizar la acción formativa, se aconseja la realización de pruebas de evaluación de conocimientos a los participantes.

Con la finalidad de la gestión de control interno del cumplimiento del principio de información y formación en el seno de la entidad, se ha elaborado un “Registro de acciones formativas e informativas” para el personal en materia de protección de datos.

REGISTRO DE ACCIONES INFORMATIVAS Y FORMATIVAS		
REF. ACCIÓN INFORMATIVA Y/O FORMATIVA N.º 1		
Identificación de la acción informativa y/o formativa		
Denominación de la acción		
Nombre de la entidad impartidora		
Datos de contacto de la entidad impartidora		
Caracterización de la acción informativa y/o formativa		
Modalidad de formación		Formación presencial
		Teleformación
Objetivos de la acción formativa		
Perfil de las personas participantes		
Duración de la acción formativa		
Descripción abreviada del programa y contenidos de la acción formativa		
Metodología de la acción formativa		
Personal docente		
Recursos didácticos utilizados en la formación		
Evaluación de la formación		

REGISTRO DE ACCIONES INFORMATIVAS Y FORMATIVAS		
REF. ACCIÓN INFORMATIVA Y/O FORMATIVA N.º 2		
Identificación de la acción informativa y/o formativa		
Denominación de la acción		
Nombre de la entidad impartidora		
Datos de contacto de la entidad impartidora		
Caracterización de la acción informativa y/o formativa		
Modalidad de formación	☐	Formación presencial
	☐	Teleformación
Objetivos de la acción formativa		
Perfil de las personas participantes		
Duración de la acción formativa		
Descripción abreviada del programa y contenidos de la acción formativa		
Metodología de la acción formativa		
Personal docente		
Recursos didácticos utilizados en la formación		
Evaluación de la formación		