NOR015 – Política d'ús del sistema d'informació

Normes d'ús del conjunt de tractaments, programes, suports i equips emprats per al tractament de dades de caràcter personal i altres informacions protegides pel deure de secret responsabilitat d'AJUNTAMENT DE PAIPORTA

Clasificació de la Informació:

Nivel del Document	Normativa
Nom del Fitxer	NOR015 - Politica de uso de seguridad de la informacion.docx
Tipus	Difusión limitada
Àmbit de Difusió	Comité de Seguretat de l'AJUNTAMENT DE PAIPORTA
Responsable	Responsable de Seguretat de l'AJUNTAMENT DE PAIPORTA

CONTROL DE FIRMAS

	DATA	FIRMA
ELABORAT PER MARIA SANCHIS	11/03/2022	
APROVAT PER COMITÉ DE SEGURETAT DE LA INFORMACIÓ	11/03/2022	

CONTROL DE VERSIONS

VERSIÓ	DATA	AUTOR	CANVIS
1.0	11/03/2022	María Sanchis	Versió inicial del document.
2.0		María Sanchis	Actualització de l'apartat 4 i 5.

ÍNDEX

1. Objectiu del document 2
2. Àmbit d'aplicació 3
3. Confidencialitat i secret 3
4. Instruccions de la persona responsable del tractament 4
5. Normes de seguretat 5
6. Normes d'ús del correu electrònic 7
7. Usos no acceptables 8
8. Responsabilitat 9

1. Objectiu del document

El 4 de maig de 2016, es va publicar en el Diari Oficial de la Unió Europea 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.

Així mateix, l'Agència Espanyola de Protecció de Dades va plasmar, en el 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, i fomentar una cultura de la protecció de dades que supose una clara millora de la competitivitat, compatible amb el desenvolupament econòmic.

En aquest sentit, el Considerant 39 del Reglament europeu assenyala que "l'ús de dades personals han de tractar-se d'una manera que garantisca una seguretat i confidencialitat adequades de les dades personals, inclusivament per a impedir l'accés o ús no autoritzats d'aquestes dades i de l'equip utilitzat en el tractament".

Referent a això, l'article 5 del Reglament (UE) 2016/679, sota la rúbrica "Principis relatius al tractament", estableix que les dades personals hauran de ser "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»)" (art. 5.1 f RGPD). Així mateix, la persona responsable del tractament serà responsable del compliment del que es disposa en aquest apartat i haurà de ser capaç de demostrar-ho («responsabilitat proactiva») (art. 5.4 RGPD).

En la seua conseqüència, la Direcció / Òrgan de Govern d'AJUNTAMENT DE PAIPORTA aposta 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.

De tal manera, l'article 32 del Reglament (UE) 2016/679, sota l'epígraf "Seguretat del tractament", estableix el següent:

> *1. Tenint en compte l'estat de la tècnica, els costos d'aplicació, i la naturalesa, l'abast, el context i les finalitats del tractament, així com riscos de probabilitat i gravetat variables per als drets i llibertats de les persones físiques, el responsable i l'encarregat del tractament aplicaran mesures tècniques i organitzatives apropiades per a garantir un nivell de seguretat adequat al risc, que si escau incloga, entre altres:*
>
> *a) la seudonimització i el xifrat de dades personals;*
>
> *b) la capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament;*

c) la capacitat de restaurar la disponibilitat i l'accés a les dades personals de forma ràpida en cas d'incident físic o tècnic;

d) un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives per a garantir la seguretat del tractament.

Així, en l'art. 32.4 RGPD, la persona responsable del tractament haurà de prendre les mesures per a garantir que qualsevol persona que actue sota la seua autoritat i tinga accés a dades personals només puga tractar aquestes dades seguint les instruccions de la persona responsable.

D'un altre costat, a la fi de l'any 2018 va ser aprovada a Espanya la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (BOE núm. 294, 06-12-2018) (LOPDGDD). Aquesta Llei orgànica adapta l'ordenament jurídic espanyol al model establit en el Reglament general de protecció de dades, i introdueix nous aspectes mitjançant el desenvolupament de matèries contingudes en aquest.

En tal sentit, la citada LOPDGDD arreplega un article específic relatiu al deure de confidencialitat, assenyalant el següent:

Article 5. Deure de confidencialitat.

1. Els responsables i encarregats del tractament de dades així com totes les persones que intervinguen en qualsevol fase d'aquest estaran subjectes al deure de confidencialitat al qual es refereix l'article 5.1.f) del Reglament (UE) 2016/679.

2. L'obligació general assenyalada en l'apartat anterior serà complementària dels deures de secret professional de conformitat amb la seua normativa aplicable.

3. Les obligacions establides en els apartats anteriors es mantindran tot i que haguera finalitzat la relació de l'obligat amb el responsable o encarregat del tractament.

Com a corol·lari de tot l'anterior, el present document s'elabora a fi d'establir la política d'ús del sistema d'informació de l'AJUNTAMENT DE PAIPORTA, amb la finalitat de donar compliment amb el que s'estableix en els articles 5.1 f) i 32.1 i 32.4 del Reglament (UE) 2016/679 i en l'article 5 de la Llei orgànica 3/2018.

2. Àmbit d'aplicació

Les normes contingudes en la present política d'ús seran aplicable a totes les persones usuàries del sistema d'informació responsabilitat de l'AJUNTAMENT DE PAIPORTA, i s'entenen per tal el conjunt de tractaments, programes, suports i equips emprats per al tractament de dades de caràcter personal i altres informacions protegides pel deure de secret.

3. Confidencialitat i secret

La persona usuària del sistema d'informació responsabilitat de l'AJUNTAMENT DE PAIPORTA ha de guardar la deguda confidencialitat sobre els fets, informacions, coneixements, documents,

objectes i qualsevol altres elements protegits pel secret, als quals tinga accés amb motiu de la relació amb la persona responsable del tractament.

En tal sentit, i sense caràcter limitatiu o excloent, el citat deure de confidencialitat i secret comprèn la següent informació:

1. Qualsevol informació sobre persones físiques identificades o identificables, protegida per la normativa sobre protecció de les persones físiques pel que fa al tractament de dades personals.
2. Qualsevol informació protegida per la Llei orgànica 1/1982, de 5 de maig, sobre protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge.
3. Qualsevol informació subjecta al deure de secret professional.
4. Qualsevol informació protegida per la normativa sobre propietat intel·lectual i industrial.
5. Els coneixements tècnics i la informació empresarial no divulgats (secrets comercials).
6. Qualsevol altra informació que per la seua naturalesa no puga ser revelada a tercers aliens a la persona responsable del tractament i que, per tant, no siga de coneixement públic.

El compliment d'aquesta obligació subsistirà, fins i tot, després de finalitzar la relació amb l'AJUNTAMENT DE PAIPORTA.

4. Instruccions de la persona responsable del tractament

La persona usuària del sistema d'informació ha de complir amb les normes de seguretat que afecten el desenvolupament de les seues funcions en el marc de la relació amb la persona responsable del tractament, que així mateix són d'obligat compliment per a les persones amb accés al conjunt de tractaments, programes, suports i equips emprats per al tractament de dades de caràcter personal i altres informacions protegides pel deure de secret responsabilitat de l'AJUNTAMENT DE PAIPORTA.

Així mateix, deu usar les dades de caràcter personal responsabilitat de l'AJUNTAMENT DE PAIPORTA exclusivament amb les finalitats determinades, explícites i legítimes, necessàries per al desenvolupament de les seues funcions en la citada entitat, per a les quals haja sigut autoritzat en el marc de la relació amb aquesta.

D'igual manera, se l'informa de la prohibició d'accedir a les dades de caràcter personal responsabilitat de l'AJUNTAMENT DE PAIPORTA que no siguen precises per al desenvolupament de les seues funcions en el marc de la relació amb la citada entitat, sense autorització expressa d'aquesta.

El compliment d'aquestes obligacions subsistirà, fins i tot, després de finalitzar la relació amb l'AJUNTAMENT DE PAIPORTA.

5. Normes de seguretat

A continuació, es resumeixen les principals obligacions en matèria de protecció de dades per a les persones amb accés al conjunt de tractaments, programes, suports i, si escau, equips emprats per al tractament de dades de caràcter personal responsabilitat de l'AJUNTAMENT DE PAIPORTA:

- Cada persona usuària haurà d'accedir exclusivament a aquelles dades o recursos que precise per al desenvolupament de les seues funcions, prèvia autorització de la persona responsable del tractament.
- Cada persona usuària serà responsable de la confidencialitat de la seua contrasenya. En cas que la mateixa siga coneguda fortuïtament o fraudulentament per persones no autoritzades, haurà de notificar-ho com a incidència i sol·licitar immediatament el canvi d'aquesta.
- Les contrasenyes hauran de ser prou complexes i difícilment endevinable per tercers, evitaran l'ús del propi identificador com a contrasenya o paraules senzilles, el nom propi, data de naixement, etc.

  Per a això se seguiran les següents pautes en l'elecció de les contrasenyes:

  - Hauran de tenir una longitud mínima de 8 caràcters alfanumèrics.
  - No hauran de coincidir amb el codi d'usuari.
  - No hauran d'estar basades en cadenes de caràcters que siguen fàcilment associables a la persona usuària (nom, cognoms, ciutat i data de naixement, DNI, noms de familiars, matrícula del cotxe, etc.).

  Amb ànim d'assegurar el control sobre els mitjans de treball i per a garantir la continuïtat de l'activitat productiva en cas d'absència de la persona usuària del sistema d'informació, l'entitat emmagatzemarà de manera segura les contrasenyes generades.
- Tant les pantalles com les impressores o un altre tipus de dispositius connectats al lloc de treball hauran d'estar físicament situats en llocs que garantisquen la confidencialitat de les dades de caràcter personal.
- Quan la persona responsable d'un lloc de treball l'abandone, bé temporalment o bé en finalitzar el seu torn de treball, haurà de deixar-ho en un estat que impedisca la visualització de les dades de caràcter personal, com per exemple un protector de pantalla amb contrasenya. La represa del treball implicarà la desactivació de la pantalla protectora amb la introducció de la contrasenya corresponent.
- En el cas de les impressores, la persona usuària haurà d'assegurar-se que no queden documents impresos en la safata d'eixida que continguen dades de caràcter personal. Si les impressores són compartides amb altres persones no autoritzades per a accedir a les citades dades, les persones responsables de cada lloc hauran de retirar els documents conforme vagen sent impresos.

- Mentre la documentació amb dades de caràcter personal no es trobe arxivada en els corresponents dispositius d'emmagatzematge, per estar en procés de revisió o tramitació, ja siga previ o posterior al seu arxiu, la persona que es trobe al càrrec de la mateixa haurà de custodiar-la i impedir en tot moment que puga ser accedida per persona no autoritzada.
- Els llocs de treball des dels quals es té accés a les dades de caràcter personal tindran una configuració fixa en les seues aplicacions i sistema operatiu que només podrà ser canviada sota autorització de la persona responsable del tractament.
- Queda expressament prohibit el tractament de dades de caràcter personal amb programes ofimàtics, com a processadors de text o fulls de càlcul, sense comunicar-ho per a la seua aprovació a la persona responsable del tractament perquè es procedisca a implantar les mesures de seguretat adequades.
- Quan les dades de caràcter personal s'emmagatzemen en dispositius portàtils o es tracten fora dels locals de la persona responsable del tractament, la persona usuària haurà de sol·licitar l'autorització prèvia de la persona responsable del tractament, havent de garantir-se, en tot cas, el nivell de seguretat adequat al risc de l'activitat de tractament.
- Quan la persona usuària tinga coneixement de qualsevol anomalia que afecte o poguera afectar la seguretat de les dades, haurà de comunicar-la sense dilació indeguda a la persona responsable del tractament perquè es faça constar el tipus d'incidència, el moment en què s'ha produït, o si escau, detectat, la persona que realitza la notificació, a qui se li comunica, els efectes que s'hagueren derivat de la mateixa i les mesures correctores aplicades.
- Quan la persona usuària tinga coneixement d'una violació de la seguretat que ocasione 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, haurà de comunicar-la sense dilació indeguda a la persona responsable del tractament perquè es notifique a l'autoritat de control competent i, si escau, a les persones interessades.
- Els suports que continguen dades de caràcter personal hauran de ser emmagatzemats en llocs al que no tinguen accés persones no autoritzades per a l'ús d'aquests.
- L'eixida de suports informàtics i documents que continguen dades de caràcter personal, incloses les compreses i/o annexos a un correu electrònic, fora dels locals sota el control de la persona responsable del tractament haurà de ser autoritzada pel responsable del tractament.
- L'eixida de suports informàtics i documents que continguen dades de caràcter personal, incloses les compreses i/o annexos a un correu electrònic, haurà de realitzar-se xifrant aquestes dades o bé utilitzant un altre mecanisme que garantisca que aquesta informació no siga accessible o manipulada durant el seu transport, en aquells supòsits en què l'activitat de tractament siga considerada d'alt reg.
- Així mateix, s'hauran de xifrar les dades de caràcter personal que continguen els dispositius portàtils quan aquests es troben fora de les instal·lacions que estan sota el control de la

persona responsable del fitxer, en aquells supòsits en què l'activitat de tractament siga considerada d'alt reg.

- La persona usuària haurà d'esborrar o destruir aquells fitxers temporals o còpies de documents que haguera creat exclusivament per a la realització de treballs temporals o auxiliars una vegada que haja deixat de ser necessari per a les finalitats que van motivar la seua creació.
- Es prohibeix l'ús de dispositius personals (portàtils, telèfons intel·ligents, tauletes), propietat de l'empleat o empleada, per al tractament de dades de caràcter personal responsabilitat de l'AJUNTAMENT DE PAIPORTA, llevat que medie autorització expressa de la persona responsable del tractament i prèvia adopció de les mesures de seguretat adequades al risc de l'activitat de tractament.

6. Normes d'ús del correu electrònic

Les persones usuàries dels comptes de correu electrònic titularitat de l'AJUNTAMENT DE PAIPORTA han de complir les següents normes d'ús:

- El compte de correu electrònic proporcionat per l'AJUNTAMENT DE PAIPORTA no ha de ser utilitzat per a finalitats privades, personals o lúdiques, ja que constitueix una eina de treball.
- Quan s'envien missatges de correu electrònic a múltiples persones destinatàries, s'ha d'utilitzar el camp "amb Còpia Oculta (CCO)" per a introduir les adreces d'aquestes, a fi de salvaguardar els deures de confidencialitat i secret.
- Queda prohibit l'enviament de comunicacions publicitàries o promocionals per correu electrònic que prèviament no hagen sigut sol·licitades o expressament autoritzades per les persones destinatàries d'aquestes.
- Queda prohibit l'enviament de dades de caràcter personal, en aquells supòsits en què l'activitat de tractament siga considerada d'alt reg, sense aplicar mecanismes de xifrat o qualssevol altres que garantisquen que aquesta informació no siga accessible per persona no autoritzada.
- Queda prohibit l'enviament de missatges de correu electrònic de caràcter racista, xenòfob, pornogràfic, sexista, d'apologia del terrorisme, perillós, amenaçador, difamatori, obscè, o que vulneren de qualsevol altra manera el valor jurídic fonamental de la dignitat de la persona.
- Queda prohibit l'enviament de missatges de correu electrònic que vulneren els drets fonamentals a la protecció de dades de caràcter personal, a la intimitat, a l'honor, i/o a la pròpia imatge.
- Queda prohibit l'enviament de missatges de correu electrònic que vulneren els drets de propietat intel·lectual o industrial.

- Queda prohibit l'enviament de missatges de correu electrònic que violen qualsevol altra normativa vigent.
- Amb l'exclusiva finalitat de garantir la continuïtat de la nostra activitat en absència de la persona treballadora, l'empresa podrà accedir al seu compte de correu electrònic corporatiu, per a això es valorarà, en tot cas, la necessitat d'aquesta intervenció per a la continuïtat dels nostres serveis.
- En cap cas s'accedirà a cap missatge que puga identificar-se clarament com a privat o personal, subratllant-li l'assenyalada prohibició d'utilitzar el seu compte de correu electrònic corporatiu per a finalitats privades, personals o lúdics.

7. Usos no acceptables

Al marge de les prohibicions fins ací assenyalades, tindran la consideració d'usos no acceptables (i, per tant, prohibits) del sistema d'informació de l'AJUNTAMENT DE PAIPORTA, els següents:

- L'ús del sistema d'informació de l'AJUNTAMENT DE PAIPORTA per a finalitats privades, personals, lúdics o qualssevol altres no estrictament relacionades amb el desenvolupament de les seues funcions en el marc de la relació amb la citada entitat, llevat que medie autorització expressa de la persona responsable del tractament.
- L'accés a dades o recursos del sistema d'informació de l'AJUNTAMENT DE PAIPORTA per als quals la persona usuària no estiga degudament autoritzat per la persona responsable del tractament.
- Facilitar l'accés a dades o recursos del sistema d'informació de l'AJUNTAMENT DE PAIPORTA a persones no autoritzades.
- Compartir dades o recursos amb altres persones usuàries autoritzades sense l'adopció de les mesures de seguretat adequades al risc de l'activitat de tractament.
- La realització d'accions la fi de les quals siga l'obtenció de contrasenyes d'altres persones usuàries autoritzades, sense que medie autorització expressa de la persona responsable del tractament.
- Proporcionar accés extern des de la pròpia xarxa de comunicacions, mitjançant la instal·lació de dispositius d'accés remot, llevat que medie autorització expressa de la persona responsable del tractament.
- La modificació no autoritzada de permisos o privilegis en relació amb l'accés a dades o recursos del sistema d'informació de l'AJUNTAMENT DE PAIPORTA.
- La instal·lació de qualsevol programa en els equips del sistema d'informació de l'AJUNTAMENT DE PAIPORTA sense que medie autorització expressa de la persona responsable del tractament.

- No fer un ús racional, eficient i considerat dels recursos proporcionats per la persona responsable del tractament, tals com: espai en disc, memòria, xarxes de comunicacions, etc.
- La destrucció no autoritzada de dades o recursos del sistema d'informació de l'AJUNTAMENT DE PAIPORTA.
- L'intent de causar qualsevol tipus de mal físic o lògic al sistema d'informació de l'AJUNTAMENT DE PAIPORTA

8. Responsabilitat

L'AJUNTAMENT DE PAIPORTA, en virtut del que s'estableix en l'article 20.3 del text refós de la Llei de l'Estatut dels Treballadors, aprovat pel Reial decret legislatiu 2/2015, de 23 d'octubre, podrà supervisar, presencialment o a través de qualsevol altres eines o mesures de control, l'estació de treball de la persona usuària, amb vista a comprovar la correcció del seu ús de conformitat amb la present política d'ús, sense perjudici de la possible aplicació d'altres mesures de caràcter preventiu, com l'exclusió de determinades connexions.

L'incompliment de les normes d'ús del sistema d'informació de l'AJUNTAMENT DE PAIPORTA, establides en el present document, podrà tenir com a conseqüència la imposició de les sancions disciplinàries corresponents, sense perjudici de l'exercici de les accions laborals, civils o penals que, si escau, procedisquen i les responsabilitats que d'aquest exercici es deriven.

NOR015 – Política de uso del sistema de información

Normas de uso del conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto responsabilidad de AYUNTAMIENTO DE PAIPORTA

Clasificación de la Información:

Nivel del Documento	Normativa
Nombre del Fichero	NOR015 - Politica de uso del sistema de informacion.docx
Tipo	Difusión limitada
Ámbito de Difusión	Comité de Seguridad del AYUNTAMIENTO DE PAIPORTA
Responsable	Responsable de Seguridad del AYUNTAMIENTO DE PAIPORTA

CONTROL DE FIRMAS

	FECHA	FIRMA
ELABORADO POR MARIA SANCHIS	11/03/2022	
APROBADO POR COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	11/03/2022	

CONTROL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	11/03/2022	María Sanchis	Versión inicial del documento.
2.0		María Sanchis	Actualización del apartado 4 y 5.

ÍNDICE

1. Objetivo del documento 2
2. Ámbito de aplicación 3
3. Confidencialidad y secreto 3
4. Instrucciones del responsable del tratamiento 4
5. Normas de seguridad 4
6. Normas de uso del correo electrónico 7
7. Usos no aceptables 8
8. Responsabilidad 9

1. Objetivo del documento

El 4 de mayo de 2016, se publicó en el Diario Oficial de la Unión Europea 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.

Así mismo, 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.

En este sentido, el Considerando 39 del Reglamento europeo señala que "los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

A este respecto, el artículo 5 del Reglamento (UE) 2016/679, bajo la rúbrica "Principios relativos al tratamiento", establece que los datos personales deberán ser "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»)" (art. 5.1 f RGPD). Así mismo, el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en dicho apartado y deberá ser capaz de demostrarlo («responsabilidad proactiva») (art. 5.4 RGPD).

En su consecuencia, la Dirección / Órgano de Gobierno de AYUNTAMIENTO DE PAIPORTA apuesta 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.

De tal modo, el artículo 32 del Reglamento (UE) 2016/679, bajo el epígrafe "Seguridad del tratamiento", establece lo siguiente:

> *1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Así, *ex* art. 32.4 RGPD, el responsable del tratamiento deberá tomar las medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo las instrucciones del responsable.

De otro lado, a finales del año 2018 fue aprobada en España la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, 06-12-2018) (LOPDGDD). Dicha Ley Orgánica adapta el ordenamiento jurídico español al modelo establecido en el Reglamento general de protección de datos, introduciendo nuevos aspectos mediante el desarrollo de materias contenidas en el mismo.

En tal sentido, la citada LOPDGDD recoge un artículo específico relativo al deber de confidencialidad, señalando lo siguiente:

Artículo 5. Deber de confidencialidad.

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Como corolario de todo lo anterior, el presente documento se elabora con el objeto de establecer la Política de uso del sistema de información de AYUNTAMIENTO DE PAIPORTA, con la finalidad de dar cumplimiento con lo establecido en los artículos 5.1 f) y 32.1 y 32.4 del Reglamento (UE) 2016/679 y en el artículo 5 de la Ley Orgánica 3/2018.

2. Ámbito de aplicación

Las normas contenidas en la presente Política de Uso serán de aplicación a todos los usuarios del sistema de información responsabilidad de AYUNTAMIENTO DE PAIPORTA, entendiéndose por tal el conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto.

3. Confidencialidad y secreto

El usuario del sistema de información responsabilidad de AYUNTAMIENTO DE PAIPORTA debe guardar la debida confidencialidad sobre los hechos, informaciones, conocimientos, documentos,

objetos y cualesquiera otros elementos protegidos por el secreto, a los que tenga acceso con motivo de la relación con el responsable del tratamiento.

En tal sentido, y sin carácter limitativo o excluyente, el citado deber de confidencialidad y secreto comprende la siguiente información:

1. Cualquier información sobre personas físicas identificadas o identificables, protegida por la normativa sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales.
2. Cualquier información protegida por la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
3. Cualquier información sujeta al deber de secreto profesional.
4. Cualquier información protegida por la normativa sobre propiedad intelectual e industrial.
5. Los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales).
6. Cualquier otra información que por su naturaleza no pueda ser revelada a terceros ajenos al responsable del tratamiento y que, por lo tanto, no sea de conocimiento público.

El cumplimiento de dicha obligación subsistirá aun después de finalizar la relación con AYUNTAMIENTO DE PAIPORTA.

4. Instrucciones del responsable del tratamiento

El usuario del sistema de información debe cumplir con las normas de seguridad que afecten al desarrollo de sus funciones en el marco de la relación con el responsable del tratamiento, que asimismo son de obligado cumplimiento para las personas con acceso al conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto responsabilidad de AYUNTAMIENTO DE PAIPORTA.

Asimismo, debe usar los datos de carácter personal responsabilidad de AYUNTAMIENTO DE PAIPORTA exclusivamente con las finalidades determinadas, explícitas y legítimas, necesarias para el desarrollo de sus funciones en la citada entidad, para las cuales haya sido autorizado en el marco de la relación con la misma.

De igual manera, se le informa de la prohibición de acceder a los datos de carácter personal responsabilidad de AYUNTAMIENTO DE PAIPORTA que no sean precisos para el desarrollo de sus funciones en el marco de la relación con la citada entidad, sin autorización expresa de la misma.

El cumplimiento de dichas obligaciones subsistirá aun después de finalizar la relación con AYUNTAMIENTO DE PAIPORTA.

5. Normas de seguridad

A continuación, se resumen las principales obligaciones en materia de protección de datos para las personas con acceso al conjunto de tratamientos, programas, soportes y, en su caso, equipos

empleados para el tratamiento de datos de carácter personal responsabilidad de AYUNTAMIENTO DE PAIPORTA:

- Cada usuario deberá acceder exclusivamente a aquellos datos o recursos que precise para el desarrollo de sus funciones, previa autorización del responsable del tratamiento.
- Cada usuario será responsable de la confidencialidad de su contraseña. En caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá notificarlo como incidencia y solicitar inmediatamente el cambio de la misma.
- Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento, etc.

  Para ello se seguirán las siguientes pautas en la elección de las contraseñas:

  - Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
  - No deberán coincidir con el código de usuario.
  - No deberán estar basadas en cadenas de caracteres que sean fácilmente asociables al usuario (nombre, apellidos, ciudad y fecha de nacimiento, DNI, nombres de familiares, matrícula del coche, etc.).

  Con ánimo de asegurar el control sobre los medios de trabajo y para garantizar la continuidad de la actividad productiva en caso de ausencia del usuario del sistema de información, la entidad almacenará de manera segura las contraseñas generadas.
- Tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad de los datos de carácter personal.
- Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos de carácter personal, como por ejemplo un protector de pantalla con contraseña. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
- En el caso de las impresoras, el usuario deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los citados datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
- Mientras la documentación con datos de carácter personal no se encuentre archivada en los correspondientes dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la

misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

- Los puestos de trabajo desde los que se tiene acceso a los datos de carácter personal tendrán una configuración fija en sus aplicaciones y sistema operativo que solo podrá ser cambiada bajo autorización del responsable del tratamiento.
- Queda expresamente prohibido el tratamiento de datos de carácter personal con programas ofimáticos, como procesadores de texto u hojas de cálculo, sin comunicarlo para su aprobación al responsable del tratamiento para que se proceda a implantar las medidas de seguridad adecuadas.
- Cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del tratamiento, el usuario deberá solicitar la autorización previa del responsable del tratamiento, debiendo garantizarse, en todo caso, el nivel de seguridad adecuado al riesgo de la actividad de tratamiento.
- Cuando el usuario tenga conocimiento de cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, deberá comunicarla sin dilación indebida al responsable del tratamiento para que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
- Cuando el usuario tenga conocimiento de una violación de la seguridad que ocasione 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, deberá comunicarla sin dilación indebida al responsable del tratamiento para que se notifique a la autoridad de control competente y, en su caso, a los interesados.
- Los soportes que contengan datos de carácter personal deberán ser almacenados en lugares a lo que no tengan acceso personas no autorizadas para el uso de los mismos.
- La salida de soportes informáticos y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del tratamiento deberá ser autorizada por el responsable del tratamiento.
- La salida de soportes informáticos y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, deberá realizarse cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riego.
- Así mismo, se deberán cifrar los datos de carácter personal que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del

responsable del fichero, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riego.

- El usuario deberá borrar o destruir aquellos ficheros temporales o copias de documentos que hubiese creado exclusivamente para la realización de trabajos temporales o auxiliares una vez que haya dejado de ser necesario para los fines que motivaron su creación.
- Se prohíbe el uso de dispositivos personales (portátiles, smartphones, tablets), propiedad del empleado, para el tratamiento de datos de carácter personal responsabilidad de AYUNTAMIENTO DE PAIPORTA, salvo que medie autorización expresa del responsable del tratamiento y previa adopción de las medidas de seguridad adecuadas al riesgo de la actividad de tratamiento.

6. Normas de uso del correo electrónico

Los usuarios de las cuentas de correo electrónico titularidad de AYUNTAMIENTO DE PAIPORTA deben cumplir las siguientes normas de uso:

- La cuenta de correo electrónico proporcionada por AYUNTAMIENTO DE PAIPORTA no debe ser utilizada para fines privados, personales o lúdicos, ya que constituye una herramienta de trabajo.
- Cuando se envíen mensajes de correo electrónico a múltiples destinatarios, se ha de utilizar el campo “Con Copia Oculta (CCO)” para introducir las direcciones de los mismos, a fin de salvaguardar los deberes de confidencialidad y secreto.
- Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico que previamente no hayan sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
- Queda prohibido el envío de datos de carácter personal, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riego, sin aplicar mecanismos de cifrado o cualesquiera otros que garanticen que dicha información no sea accesible por persona no autorizada.
- Queda prohibido el envío de mensajes de correo electrónico de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, peligroso, amenazador, difamatorio, obsceno, o que vulneren de cualquier otro modo el valor jurídico fundamental de la dignidad de la persona.
- Queda prohibido el envío de mensajes de correo electrónico que vulneren los derechos fundamentales a la protección de datos de carácter personal, a la intimidad, al honor, y/o a la propia imagen.
- Queda prohibido el envío de mensajes de correo electrónico que vulneren los derechos de propiedad intelectual o industrial.

- Queda prohibido el envío de mensajes de correo electrónico que violen cualquier otra normativa vigente.
- Con la exclusiva finalidad de garantizar la continuidad de nuestra actividad en ausencia de la persona trabajadora, la empresa podrá acceder a su cuenta de correo electrónico corporativo, para lo cual se valorará, en todo caso, la necesidad de dicha intervención para la continuidad de nuestros servicios.
- En ningún caso se accederá a ningún mensaje que pueda identificarse claramente como privado o personal, subrayándole la señalada prohibición de utilizar su cuenta de correo electrónico corporativo para fines privados, personales o lúdicos.

7. Usos no aceptables

Al margen de las prohibiciones hasta aquí señaladas, tendrán la consideración de usos no aceptables (y, por ende, prohibidos) del sistema de información de AYUNTAMIENTO DE PAIPORTA, los siguientes:

- El uso del sistema de información de AYUNTAMIENTO DE PAIPORTA para fines privados, personales, lúdicos o cualesquiera otros no estrictamente relacionados con el desarrollo de sus funciones en el marco de la relación con la citada entidad, salvo que medie autorización expresa del responsable del tratamiento.
- El acceso a datos o recursos del sistema de información de AYUNTAMIENTO DE PAIPORTA para los que el usuario no esté debidamente autorizado por el responsable del tratamiento.
- Facilitar el acceso a datos o recursos del sistema de información de AYUNTAMIENTO DE PAIPORTA a personas no autorizadas.
- Compartir datos o recursos con otros usuarios autorizados sin la adopción de las medidas de seguridad adecuadas al riesgo de la actividad de tratamiento.
- La realización de acciones cuyo fin sea la obtención de contraseñas de otros usuarios autorizados, sin que medie autorización expresa del responsable del tratamiento.
- Proporcionar acceso externo desde la propia red de comunicaciones, mediante la instalación de dispositivos de acceso remoto, salvo que medie autorización expresa del responsable del tratamiento.
- La modificación no autorizada de permisos o privilegios en relación con el acceso a datos o recursos del sistema de información de AYUNTAMIENTO DE PAIPORTA.
- La instalación de cualesquiera programas en los equipos del sistema de información de AYUNTAMIENTO DE PAIPORTA sin que medie autorización expresa del responsable del tratamiento.
- No hacer un uso racional, eficiente y considerado de los recursos proporcionados por el responsable del tratamiento, tales como: espacio en disco, memoria, redes de comunicaciones, etc.

- La destrucción no autorizada de datos o recursos del sistema de información de AYUNTAMIENTO DE PAIPORTA.
- El intento de causar cualquier tipo de daño físico o lógico al sistema de información de AYUNTAMIENTO DE PAIPORTA

8. Responsabilidad

AYUNTAMIENTO DE PAIPORTA, en virtud de lo establecido en el artículo 20.3 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, podrá supervisar, presencialmente o a través de cualesquiera otras herramientas o medidas de control, la estación de trabajo del usuario, en orden a comprobar la corrección de su uso de conformidad con la presente Política de Uso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

El incumplimiento de las normas de uso del sistema de información de AYUNTAMIENTO DE PAIPORTA, establecidas en el presente documento, podrá tener como consecuencia la imposición de las sanciones disciplinarias correspondientes, sin perjuicio del ejercicio de las acciones laborales, civiles o penales que, en su caso, procedan y las responsabilidades que de dicho ejercicio se deriven.