Ajuntament de L'Armentera

X2019000469

INSTRUCCIÓ DE MESURES DE SEGURETAT EN EL TRACTAMENT DE DADES PERSONALS DE L'AJUNTAMENT DE L'ARMENTERA.

Vigent a partir de:

APROVACIÓ:..... DATA:.....

SUMARI

ANNEXOS

1. Objecte del Document

En el present Document figuren les mesures de seguretat que s'apliquen en el tractament de dades de caràcter personal (en endavant les dades) per part de l'Ajuntament com a responsable del tractament. Van orientades a evitar l'alteració, destrucció o pèrdua de les dades de manera accidental o il·lícita, així com el seu accés i la seva comunicació no autoritzades.

Aquest Document s'ha redactat i adoptat en 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 o RGPD) i de la *Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals* (LOPDGDD).

El contingut del Document s'actualitzarà regularment. Prèviament a la seva actualització el Delegat de Protecció de Dades (DPD) informarà sobre les propostes de canvis. Les modificacions s'aprovaran per mitjà de Decret d'Alcaldia.

La informació d'aquest Document es complementa o guarda relació amb els documents següents:

- Instruccions funcions i responsabilitats.
- Registre d'activitats de tractament.

2. Àmbit d'aplicació

1. Les mesures de seguretat que figuren en aquest document són de compliment obligatori en el tractament de dades que efectua l'Ajuntament. Obliga tant el personal propi com el personal extern que, sense mantenir una relació laboral amb l'Ajuntament, li presti serveis i que, amb aquesta finalitat, tracti o pugui tractar dades. Als efectes d'aquest Document cada una d'aquestes persones tindrà la consideració d'usuari.

2. Aquestes mesures de seguretat s'apliquen:

a) als locals on es porta a terme el tractament de les dades que estan sota la responsabilitat de l'Ajuntament. Disposa dels següents centres de treball:

- Ajuntament i arxiu, carrer Pau Casals, 2.

Altres locals municipals:

- Casal d'Avis i Sala de Lectura, al carrer Pau Casals 2
- Llar d'infants, carrer de la Figuera s/n.
- Sala d'entitats, Espai Jove, Sala nova i sala polivalent.

b) als equips, sistemes informàtics i entorn de comunicacions que permeten tractar les dades. Aquests recursos consisteixen en una xarxa integrada per 8 ordinadors. Un dels quals fa la funció de servidor.

c) als equips portàtils, sistemes d'accés a la xarxa Internet, al correu electrònic o a qualsevol classe de suport o sistema que permeti el tractament de dades.

d) als suports de qualsevol classe, inclosos els documents en suport paper, on figurin dades i, en conseqüència, als locals i al mobiliari destinats a la custòdia de

suports, tant si són documents auxiliars o de treball com documents conservats pel seu valor legal o informatiu.

3. Mesures organitzatives generals

1. L'accés als locals es controla de la manera següent:
   - L'accés del públic està controlat. Queda restringit l'accés a zones internes de treball.
   - El servidor central està ubicat a un despatx de la primera planta de l'Ajuntament. Espai tancat amb clau.

2. Existeix un sistema de videovigilància. Les imatges es conserven en un ordinador de les oficines municipals durant un període màxim d'un mes. Únicament són accessibles per part del personal municipal que indiqui la memòria corresponent (X2022000460). Les imatges s'eliminen automàticament. Les càmeres permeten visionar els espais següents:
   - Deixalleria municipal.

4. Mesures lògiques generals

1. Els sistemes dels equips informàtics utilitzats per a l'emmagatzematge i el tractament de les dades personals s'hauran de mantenir actualitzats.

2. En els servidors i ordinadors es disposarà d'un sistema antivirus per evitar, tant com sigui possible, el robatori o destrucció de la informació i dades. El sistema d'antivirus s'ha de revisar i actualitzar de forma periòdica.

3. Els servidors i els ordinadors es connectaran a la xarxa elèctrica per mitjà d'un SAI.

4. Per evitar accessos remots no autoritzats a les dades es disposarà d'un talla foc que protegeixi els servidors.

5. Únicament els administradors del sistema poden canviar o configurar elements del sistema, instal·lar o desinstal·lar aplicacions informàtiques, o modificar o habilitar qualsevol altre recurs que permeti el tractament de les dades.

5. Llocs de treball

1. Cada lloc de treball està sota la responsabilitat de la persona a qui se li hagi assignat o l'ocupi. Aquesta persona ha de garantir que la informació que des d'allà es pot veure o tractar no quedi accessible a persones no autoritzades. Les pantalles han d'estar orientades correctament per evitar que persones no autoritzades visualitzin la informació. S'activarà un protector de pantalla després de 5 minuts d'inactivitat.

2. Quan s'abandoni temporalment i quan finalitzi la jornada laboral, el lloc de treball ha de quedar en un estat que no permeti l'accés a informació o dades reservades.

3. Els armaris i calaixos propis o compartits es tancaran de manera que el seu contingut no sigui accessible a persones no autoritzades.

6. Alta, modificació de perfil o baixa d'usuari

1. L'alta, modificació de perfil o la baixa d'un usuari la decideix l'alcalde. Es donen instruccions a l'administrador del sistema sobre els permisos, recursos i accessos que ha de tenir o que ha de deixar de tenir.

2. En l'alta s'atorga un nom d'usuari específic per a cada persona a qui s'autoritza accedir als sistemes o equips. El nom d'usuari es correspon amb un únic usuari i l'identifica de manera inequívoca. Es forma amb la inicial del nom seguit del primer cognom.

7. Política de contrasenyes

1. Cada usuari és responsable de la confidencialitat de la seva contrasenya o contrasenyes. No podrà comunicar-la a una altra persona. Si la contrasenya arriba a ser coneguda per una altra persona qualsevol que en tingui coneixement ho ha de notificar mitjançant el procediment de notificació d'incidències.

2. La política de contrasenyes es fonamenta en les pautes següents:
- La contrasenya d'inici de sessió tindrà almenys 8 caràcters (números i lletres).
- S'utilitza una altra contrasenya per accedir a aplicacions.
- S'utilitza una altra contrasenya per accedir al correu.

3. En qualsevol cas la contrasenya o contrasenyes:
- És personal i secreta.
- Ha de ser específica. No pot ser la mateixa que s'utilitzi per altres finalitats.
- Es custodia de manera segura i no accessible a altres persones.
- L'usuari ha de garantir-ne la confidencialitat i informar, mitjançant el registre d'incidències, en el cas que una altra persona arribi a conèixer-la.
- La contrasenya d'inici de sessió es renova almenys un cop l'any.
- En la renovació no es permeten repeticions ni formar-la de manera derivada.
- Les contrasenyes es guarden encriptades i sota la responsabilitat de l'administrador del sistema.

8. Còpia de seguretat

1. Les còpies de seguretat s'efectuen seguint el procediment següent:
- el servidor de l'Ajuntament fa còpies diàries de matinada, amb disc dur extern, que en període inferior al setmanal: un connectat i l'altre a la caixa forta.

2. L'administrador del sistema comprovarà regularment, almenys un cop cada sis mesos, el correcte funcionament del sistema de còpia. Es deixarà constància en el registre d'incidències de les que es puguin produir en la realització de les còpies. L'administrador del sistema comprovarà regularment, almenys un cop cada sis mesos, el correcte funcionament dels sistema de còpia.

3. En cas de pèrdua d'informació, en base a l'anàlisi de la incidència i dels seus efectes, el secretari avaluarà la conveniència de procedir a la seva recuperació i decidirà, si escau, que es recuperi a partir d'una còpia. En el cas que es considerés necessari la

recuperació s'efectuaria aproximant-se el màxim possible a l'estat en el qual es trobaven en el moment previ a la incidència.

4. En el registre d'incidències es deixarà constància de les operacions de recuperació, de la persona que va efectuar el procés, de les dades recuperades i de com s'efectuà la recuperació.

5. Els suports que continguin dades com a conseqüència de procediments regulars i periòdics de realització de còpies que tinguin entitat física pròpia, hauran d'estar inventariats i clarament identificats amb una indicació del seu contingut. Els suports es guardaran en lloc protegit, de manera que cap persona no autoritzada hi tingui accés.

9. Treballs des de fora dels sistemes i locals

1. L'autorització d'accés des de fora de la xarxa interna als sistemes i recursos que permeten el tractament de les dades i /o l'ús de dispositius portàtils que permetin l'emmagatzematge o l'accés a dades l'atorgarà prèviament i expressament el secretari. Aquesta autorització no serà necessària quan les característiques, perfil o naturalesa del lloc de treball requereixin aquest accés remot.

2. L'enregistrament de dades en un dispositiu o suport (memòria USB, DVD, disc dur extern o similars) només s'efectuarà quan sigui imprescindible, estigui autoritzat prèviament i en els suports proporcionats per l'Ajuntament. Quan els dispositius hagin de sortir dels locals hauran d'estar protegits de manera que no hi puguin tenir accés persones no autoritzades.

3. La persona autoritzada a treballar des de fora de la xarxa interna, a emmagatzemar dades en dispositius, o a treballar per mitjà de dispositius portàtils, haurà d'aplicar mesures de seguretat per garantir la seguretat i confidencialitat de les dades.

4. El secretari portarà un registre de les persones autoritzades a efectuar els tractaments indicats en els apartats precedents, indicant cada usuari autoritzat o bé el perfil d'usuaris que obtenen aquesta autorització. S'indicarà el període de validesa de les autoritzacions.

10. Enviament de dades

Únicament poden efectuar enviaments de dades les persones autoritzades, ja sigui de forma expressa i singular o en el desenvolupament de les funcions que tingui assignades. Les sortides de dades que s'efectuïn mitjançant correu electrònic es realitzaran des de comptes d'usuaris autoritzats per a realitzar aquesta funció. Igualment si l'entrada o sortida de dades s'efectua mitjançant sistemes d'enviament de fitxers per xarxa, només podrà realitzar-ho un usuari expressament autoritzat.

11. Documents temporals o còpies de treball

Els documents de suport, creats per a portar a terme treballs temporals, puntuals o auxiliars, seran eliminats un cop deixin de ser necessaris per a les finalitats que en van motivar la creació.

12. Impressores

En la safata de sortida de les impressores s'evitarà que quedin sense control documents amb dades. Si les impressores són compartides amb persones no autoritzades a accedir a les dades, l'usuari que hagi ordenat la impressió haurà de retirar els documents de la safata de sortida tan bon punt hi apareguin.

13. Custòdia dels documents en suport paper

1. Els expedients, dossiers, llistats o fulls, o bé qualsevol classe de document en suport paper que contingui dades de caràcter personal, hauran de ser tractats en tot moment de forma que se'n garanteixi la reserva. Tots els documents hauran d'estar controlats i localitzables en tot moment, tant mentre duri la seva utilització com a l'hora de ser guardats en un espai d'arxiu.

2. Mentre els documents en paper no estiguin dipositats en el lloc d'arxiu, la persona que l'estigui utilitzant o elaborant assumeix la responsabilitat de la seva custòdia i d'evitar que pugui ser accedit o utilitzat per persona no autoritzada.

3. Els armaris, arxivadors o similars que serveixin per a guardar els documents en paper han d'estar dotats amb mecanismes que en permetin controlar l'accés. Si aquests armaris o arxivadors no ho permetessin, s'adoptaran mesures alternatives per impedir l'accés a persones no autoritzades.

14. Trasllat dels documents en suport paper

En els trasllats de la documentació en paper s'han d'adoptar les mesures de seguretat suficients per a evitar-ne la sostracció, pèrdua o un accés indegut. La persona responsable de custodiar la documentació utilitzarà sobres, bosses o altres contenidors que en garanteixin la reserva i que, en el moment de ser rebuts pel destinatari, si és el cas, permetin verificar que durant el trasllat ha quedat garantida la reserva.

15. Reutilització i eliminació dels documents en suport paper

1. La reutilització de documents que contenen dades de caràcter personal, per exemple per a la utilització de la cara posterior en blanc, no es podrà efectuar quan aquesta reutilització pugui comportar l'accés a les dades per part de persones no autoritzades.

2. L'eliminació de documents que continguin dades de caràcter personal s'efectuarà mitjançant un sistema que faci absolutament impossible la visualització o comprensió de les dades, o la seva recuperació posterior.

16. Gestió d'incidències

1. Es registrarà qualsevol anomalia que suposi o pugui suposar un perill per a la confidencialitat, integritat o disponibilitat de les dades. L'usuari que tingui coneixement d'u-

na incidència l'ha de notificar per mitjà de correu electrònic per tal que en quedi constància.

2. El registre d'incidències és administrat pel secretari.

3. El registre d'incidències haurà de contenir almenys les dades següents: tipus d'incidència, data i hora en què es va produir, persona que realitza la notificació, efectes que pot produir, descripció detallada de la incidència, seguiment, mesures adoptades.

4. Quan una incidència constitueixi una violació de seguretat el secretari la comunicarà a l'Autoritat Catalana de Protecció de Dades (www.apd.cat) de manera immediata i, en qualsevol cas, en un termini màxim de 72 hores després que se n'hagi tingut constància. No serà obligatori notificar-la quan sigui improbable que la violació de la seguretat constitueixi un risc per als drets i les llibertats de les persones. Si la notificació no es produeix en el termini de 72 hores, s'informarà dels motius de la dilació. En els casos previstos a l'art. 34 del RGPD les violacions de seguretat es comunicaran també als afectats.

17. Verificació del compliment de les mesures de seguretat

1. El secretari revisarà periòdicament el compliment de les mesures establertes en el present Document. El Delegat de protecció de dades podrà efectuar en qualsevol moment les comprovacions que consideri adequades per conèixer el grau de compliment d'aquestes mesures.

2. El secretari analitzarà les incidències registrades per tal d'aplicar les mesures correctores que evitin aquestes incidències en el futur, amb independència de les mesures puntuals adoptades en el moment que es produeixi la incidència.

3. S'efectuaran regularment revisions per tal de verificar el compliment dels protocols de treball i mesures de seguretat i procedir, si escau, a la seva actualització. Correspon al secretari, amb l'assessorament del Delegat de Protecció de Dades, efectuar o encarregar la realització dels processos de verificació i actualització.

4. En qualsevol cas es revisaran protocols de treball i l'aplicació o eficàcia de mesures de seguretat en els casos següents:

- Quan ho recomani el Delegat de protecció de dades.
- Quan es constati la reiteració d'incidències de seguretat.
- Quan ho indiquin les conclusions dels informes d'auditoria, de les avaluacions de riscos o de les avaluacions d'impacte en la protecció de dades.

5. És obligació de tot usuari informar de qualsevol qüestió de transcendència relativa a un incorrecte tractament de dades, o error observat, o contradicció amb el present Document, o mesura que a criteri seu mereixi ser actualitzada o revisada.

6. Almenys un cop a l'any s'efectuarà una revisió per a dictaminar el grau de compliment de les mesures de seguretat que figuren en el present Document, per identificar deficiències i proposar mesures correctores o de millora. Els informes seran analitzats pel Secretari. Es notificaran al Delegat de protecció de dades. A partir d'aquesta anàlisi s'adoptaran les mesures correctores adients. Si és el cas es modificarà el present Document per deixar constància de les noves mesures. Correspondrà al secretari adoptar els acords i fer implementar les mesures correctores o de millora necessàries.

7. Els resultats dels controls periòdics i de les auditories generals es conservaran a disposició de l'Autoritat Catalana de Protecció de Dades (www.apd.cat).

DISPOSICIÓ ADDICIONAL

El contingut del present Document s’actualitzarà quan correspongui incorporar les modificacions i actualitzacions resultants de les auditories o verificacions de compliment. Prèviament a la seva actualització el Delegat de Protecció de Dades (DPD) informarà sobre les propostes de canvis. Les modificacions s’aprovaran per mitjà Decret d'Alcaldia.

ANNEXOS

I. Conceptes i definicions

II. Procediment de notificació i registre d'incidències

III. Notificació de violació de seguretat a persona interessada

IV. Autorització d'accés remot als sistemes

V. Registre d'usuaris autoritzats a disposar de suports de còpia de treball

VI. Autorització per a efectuar còpia de dades a suports externs

VII. Compromís de compliment de mesures de seguretat en retirada d'equips

I - Conceptes i definicions

- *Accessos autoritzats*: Autoritzacions concedides a un usuari per la utilització de diversos recursos.
- *Administrador del sistema*: Persona a càrrec de mantenir els sistemes d'informació, gestionant-los de manera adequada, amb capacitat per instal·lar i configurar nou software en els sistemes d'informació, entre altres funcions.
- ***Afectat o interessat*:** Persona física titular de les dades que siguin objecte de tractament.
- *Autenticació*: Procediment de comprovació de la identitat d'un usuari.
- *Cessió o comunicació de dades*: Revelació de dades a persones diferents de l'afectat.
- ***Consentiment de l'afectat*:** Manifestació de voluntat, lliure i inequívoca, específica i informada, mitjançant la que l'interessat autoritza el tractament de les seves dades personals.
- *Contrasenya*: Informació confidencial, freqüentment formada per una cadena de caràcters, que pot ser utilitzada en l'autenticació d'un usuari o en l'accés a un recurs.
- *Control d'accés*: Mecanisme que permet accedir a dades o recursos en funció de la identificació ja autentificada.
- *Còpia de seguretat*: Còpia de les dades en un suport o mitjà que possibiliti la seva recuperació.
- ***Dades de caràcter personal*:** Qualsevol informació concernent a persones físiques identificades o identificables.
- *Destinatari o cessionari*: La persona física o jurídica, pública o privada o òrgan administratiu, al que es comuniquen dades.
- *Document*: Tot escrit, gràfic, so, imatge o qualsevol classe d'informació que pot ser tractada en un sistema d'informació com a una unitat diferenciada.
- ***Encarregat del Tractament*:** Persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o conjuntament amb altres, s'encarrega de tractar les dades personals. Aquest encarregat treballa a càrrec del Responsable del Tractament, de forma que ha de seguir i respectar la finalitat, contingut i ús que aquest ha definit.
- *Identificació*: Procediment de reconeixement de la identitat de l'usurari.
- ***Incidència*:** Qualsevol anomalia que afecti o pugui afectar a la seguretat de les dades.
- *Lloc de treball*: el conjunt de mitjans o dispositius des dels quals es treballa regularment i es pot accedir a les dades.
- *Perfil d'usurari*: Accessos autoritzats a un grup d'usuraris.
- *Procediment de Seguretat*: Tota mesura, mecanisme, procediment o dispositiu necessari i establert pel Responsable del Fitxer amb l'objectiu de protegir els recursos i, en general, les dades personals contingudes en els Sistemes d'Informació.
- *Recurs*: Qualsevol element que forma part d'un sistema d'informació.
- ***Responsable del tractament*:** la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que, sol o juntament amb d'altres, determina les finalitats i els mitjans del tractament.
- *Sistema d'informació*: Conjunt de fitxers, tractaments, programes, aplicacions i suports, utilitzats pel tractament de dades.
- *Suport*: Objecte físic que emmagatzema o conté dades o documents, o objecte susceptible de ser tractat en un sistema d'informació i sobre el que es pot gravar i recuperar dades.

- *Tercers*: La persona física o jurídica, pública o privada o òrgan administratiu diferent de l'afectat o interessat, del Responsable del tractament, de l'Encarregat del Tractament i de les persones autoritzades per tractar dades sota l'autoritat directe del Responsable del tractament.
- ***Tractament de dades*:** Operació o procediment tècnic de caràcter automatitzat o no, que permet la recollida, gravació, conservació, elaboració, modificació, bloqueig i cancel·lació de les dades personals, així com, les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències.
- *Transmissió de dades*: Qualsevol trasllat de comunicació, enviament, lliurament o divulgació de les dades.
- *Usuari*: Persona autoritzada a accedir a dades o recursos.

II. Procediment de notificació i registre d'incidències

FORMULARI DE NOTIFICACIÓ I REGISTRE D'INCIDÈNCIES		
Incidència núm.		
Data de notificació		
Classe d'incidència		
Data i hora de la incidència		
Persona que comunica la incidència		
Persona a qui es comunica		
Efectes:		
Descripció detallada		
Persona que intervé		
Solució adoptada		
Mesures correctores adoptades (si és el cas):		

EN CAS DE PÈRDUA DE DADES		
S’ha realitzat recuperació de dades?		
Procediment seguit		
Dades recuperades		
Persona que ho autoritza		
Dades gravades novament		
Persona que va recuperar		

III. Notificació de violació de seguretat a persona interessada

Benvolgut Sr. / Benvolguda Sra. […],

De conformitat amb l'article 34 del Reglament (UE) núm. 2016/679, general de protecció de dades us comuniquem que aquest Ajuntament ha patit una violació de seguretat que podria comportar un risc per als vostres drets i interessos. Com vostè sap tractem les seves dades personals amb la finalitat de […].

El dia […] vam constatar que s'havia produït una incidència de seguretat que pot haver suposat l'alteració, destrucció o pèrdua de les dades, o el seu accés o comunicació no autoritzats. La incidència va consistir en [breu descripció]. Aquesta incidència podria comportar que hi hagi intens de suplantar la vostra identitat // es puguin produir intromissions .... [indicar possibles conseqüències de l'incident].

Com a reacció a aquests incidència hem adoptat un conjunt de mesures d'entre les quals destaquem les següents: […]. Hem informat també dels fets a l'Autoritat Catalana de Protecció de Dades (www.apd.cat).

Us recomanem que [recomanacions per eliminar o minimitzar els efectes negatius de la incidència].

Lamentem les molèsties que us pugui provocar i quedem a la vostra disposició per aclarir els vostres dubtes o ampliar la informació.

Atentament,

IV. Autorització d'accés remot als sistemes

....., en qualitat d .....

autoritzo a [persona autoritzada] l'accés als recursos informàtics, inclòs el correu electrònic, i a la informació que figura a la xarxa corporativa de l'Ajuntament, des d'equips ubicats fora dels locals i xarxes pròpies, fins i tot per mitjà d'equips privats, per tal de poder portar a terme treballs relacionats amb les responsabilitats i funcions que li corresponen com a [càrrec o funció].

D'acord amb l'article 20 de la Llei 10/2021, de 9 de juliol, de treball a distància, les persones treballadores, en el desenvolupament del treball a distància, hauran de complir les instruccions que estableixi l'Ajuntament en el marc de la legislació sobre protecció de dades i sobre seguretat de la informació. Per això mateix, l'accés i utilització de recursos s'haurà de portar a terme d'acord amb les instruccions que s'hagin aprovat o s'aprovin i sota la responsabilitat directa de la persona autoritzada i en especial donant compliment a les condicions següents:

- Mantenir la confidencialitat del nom d'usuari i contrasenya que té assignats com a usuari/a dels recursos i sistemes.

- No copiar de cap forma ni en cap suport la informació a la que tindrà accés.

- No permetre la visualització per part d'altres persones de la informació a la que accedirà.

L'Armentera, ... d ..... de 20...

V. Registre d'usuaris autoritzats a disposar de suports de còpia de treball

NOM O PERFIL	DISPOSITIU	PERÍODE	OBSERVACIONS

VI. Autorització per a efectuar còpia de dades a suports externs

....., en qualitat d .....

autoritza a ..... l'ús de suports de còpia, com llapis de memòria per a l'emmagatzematge i transport d'informació, documents i dades de l'Ajuntament de l'Armentera (en endavant l'Ajuntament), per al desenvolupament de la seva activitat laboral.

En la utilització i custòdia d'aquests suports la persona autoritzada haurà d'adoptar les mesures de seguretat necessàries per evitar l'alteració, destrucció o pèrdua de les dades de manera accidental o il·lícita, així com el seu accés i la seva comunicació no autoritzades.

No podrà enregistrar-se en aquests suports informació aliena a l'Ajuntament. En cas de pèrdua o sostracció d'un suport que contingui informació, documents o dades, la persona autoritzada ho haurà de comunicar immediatament per al seu registre com a incidència.

L'Armentera, ... d ..... de 20...

VII. Compromís de compliment de mesures de seguretat en retirada d'equips

..... actuant en aquest acte en nom i representació de l'empresa .....

D E C L A R O

Que en compliment de l'encàrrec rebut de part de l'Ajuntament de l'Armentera (en endavant l'Ajuntament), amb CIF P1701100H i domicili a carrer Pau Casals 2 de l'Armentera (CP 17472) en el dia que figura a la data del present document procedim a retirar l'aparell ..... per a la seva reparació, substitució o destrucció.

Que hem estat informats per l'Ajuntament de l'existència en la memòria de l'aparell de dades de caràcter personal i d'altres informacions mereixedores de reserva.

Que la nostra empresa està al corrent del compliment de la normativa de protecció de dades; el nostre personal ha estat informat sobre les seves obligacions i protocols a seguir i s'apliquen en tot moment les mesures que figuren en el Document de seguretat de l'empresa.

Que, atesa la necessitat de garantir la confidencialitat de les esmentades dades i informacions, ens comprometem a aplicar en tot moment, siguin quins siguin els treballs o actuacions que s'hagin de portar a terme, les mesures de seguretat necessàries per a garantir la confidencialitat de les dades. S'aplicaran les mesures descrites en el Reglament (UE) 2016/679 de 27 d'abril de 2016.

Que el personal de l'empresa no accedirà a les dades o informacions que puguin figurar a l'esmentada memòria, ni efectuarà reproduccions del seu contingut en altres suports. No obstant, en el cas que resultés imprescindible l'accés als continguts per portar a terme l'encàrrec rebut de l'Ajuntament, aquest accés es portaria a terme únicament per part del personal imprescindible, se'n deixaria constància documental i se'n donaria coneixement a l'Ajuntament.

Que en el cas que hagués calgut accedir a les dades o informacions, assumim que l'obligació de secret professional té una durada indefinida i, en conseqüència, es manté en vigor amb posterioritat a la realització dels treballs.

Que si calgués procedir a l'eliminació de l'aparell o el suport on figura la informació, l'eliminació s'efectuaria de forma segura, amb l'adopció de les mesures necessàries per a evitar l'accés a la informació continguda en el suport o la seva recuperació posterior. S'expediria certificat amb indicació del procediment seguit i les mesures de seguretat adoptades i es lliuraria a l'Ajuntament.

L'Armentera, ... d ..... de 20...