PROTOCOL DE SEGURETAT INFORMÀTICA

Agrupació d'Empreses Municipals de Tarragona

AJUNTAMENT DE TARRAGONA

ÍNDEX pàg.

1. PRELIMINAR

Les presents normes bàsiques sobre seguretat informàtica de **L'AGRUPACIÓ D'EMPRESES MUNICIPALS DE TARRAGONA, AIE (**en endavant l'AIE**),** té com a objecte i finalitat establir unes normes internes de prohibició de determinades conductes i de seguretat.

Les presents normes són d'aplicació a les empreses municipals de Tarragona que formen part de l'anomenada agrupació essent aquestes les següents:

1) SERVEI MUNICIPAL DE L'HABITATGE I ACTUACIONS URBANES, S.A **- SMHAUSA -**

2) EMPRESA MUNICIPAL DE MITJANS DE COMUNICACIÓ DE TARRAGONA, S.A. **- EMMCTSA -**

3) EMPRESA MUNICIPAL DE DESENVOLUPAMENT ECONÒMIC DE TARRAGONA, S.A. **- EMDETSA -**

4) EMPRESA MUNICIPAL DE TRANSPORTS PÚBLICS DE TARRAGONA, S.A. **- EMTSA -**

5) EMPRESA D'APARCAMENTS MUNICIPALS DE TARRAGONA, S.A. **- AMTSA -**

6) AGRUPACIÓ D'EMPRESES MUNICIPALS DE TARRAGONA, AIE **- AEMT AIE -**

Per tant, quan ens referim en les presents normes a l'AIE també fem referència a totes les societats mercantil municipals que conformen aquesta agrupació.

2.- PROTOCOLS DE SEGURETAT INFORMÀTICA I DE SISTEMES DE VIDEOVIGILÀNCIA

2.1.- INTRODUCCIÓ

La preocupació per la seguretat, respecte dels propis clients i proveïdors de l'AIE i, en general, la dels afectats pel codi ètic i del codi de conducta-sancionador, és una prioritat en tots els models de prevenció de delictes.

La seguretat no pot dissociar-se de la protecció que mitjançant la mateixa ha de realitzar-se a les dades de caràcter personal de les que disposa l'empresa, però a més d'aquelles informacions privilegiades que per raó del tràfic mercantil posseeixi o es disposi, així com la dels treballadors i empleats, administradors i directius, entre d'altres, això afecta doncs a diversos delictes i qüestions d'índole mercantil.

En el nostre entorn jurídic ha calat certa obsessió per la seguretat, del tot justificable, i així estan sorgint especialitats jurídiques únicament encaminades o dirigides a la seguretat dels mitjans informàtics i TIC.

És evident, i així es demostra en tota l'activitat empresarial, que els elements informàtics són veritables recursos empresarials i mitjans de producció, i no dels seus empleats, per aquest motiu el control de tals elements, la seva compra o adquisició, control d'existència i ús, mesures de seguretat dels mateixos i limitacions de l'ús o inclusivament prohibicions són bàsics per a qualsevol empresa.

En el cas de l'AIE, concorre el supòsit de control dels elements informàtics per a la protecció dels drets fonamentals com el dret de la intimitat dels qui els usin, i de les dades als quals accedeixen. La seguretat informàtica en el present cas va molt més allà i és d'afectació de tercers, especialment clients, molt especialment en el cas de disposar com d'accedir a dades reservades de caràcter personal, com ho és el domicili, el DNI, o fins i tot dades de caràcter econòmic o de situacions personals, que afecten algun grau d'incapacitat.

Aquestes dades personals, poden ser consultades per diversos motius per una deguda gestió dels serveis públics que es presten per part d'empreses de l'AIE. Aquestes dades però tenen un accés molt restringit pel què fa a la seva consulta i obtenció, ens referim al supòsit d'SMHAUSA, de l'AMT i també de l'EMT en que està absolutament bloquejat el sistema de forma que només hi accedeixen des de punts determinats informàtics i persones molt concretes i de responsabilitat.

2.2.- SEGURETAT INFORMÀTICA, PROTECCIÓ DE DADES I CONFIDENCIALITAT

L'AIE, a través de cada una de les empreses que la conformen, disposa d'un departament responsable de serveis generals o administració, que realitza les tasques de serveis informàtics.

Sens perjudici de les millores que es vulguin aplicar, de forma individual per les empreses que conformen l'AIE o en el seu conjunt, el marc mínim de seguretat en els elements informàtics ha de ser el següent:

- Mesures de seguretat quant a l'inici de sessió, amb paraules de seguretat, contrasenyes, en tots els elements informàtics de treball.

- Mesures de seguretat quant a l'ús que acreditin la persona que opera amb l'element informàtic, sistemes d'identificació / autenticació.

- Bloqueig dels elements en cas de no ús durant un període de temps (+- 10 minuts).

▪ Prohibició absoluta d'ús d'un element informàtic amb contrasenya o en sessió iniciada per una altra persona, o bé cedir les dades per tal que una altre persona accedeixi en nom del cedent.

▪ Impossibilitat de descàrregues no autoritzades, bloquejos.

▪ Bloqueig de forma remota en cas de pèrdua (mòbils / portàtils; 12 mesos)

▪ Sistema de còpies de seguretat, diari, setmanal o mensual.

▪ Prohibició d'instal·lar programes que infringeixin la llei de propietat intel·lectual o industrial (impossibilitat de realitzar-ho).

▪ Realització anual d'auditoria de sistemes informàtics, del hardware i del software que s'usi en les empreses de l'AIE.

▪ Prohibició d'instal·lar programes que infringeixin la llei de propietat intel·lectual o industrial (impossibilitat de realitzar-ho).

▪ Prohibició de guardar documents privats en elements informàtics de l'empresa, possibilitat de realitzar un esborrat programat cada 30-90 dies (implementació en 12 mesos).

▪ Destrucció d'elements informàtics obsolets, avariats, prèviament han de guardar-se les seves dades en disc extern (12 mesos).

▪ Control mitjançant protocols comptables i fiscals d'amortitzacions, de tots els elements informàtics, telefonia i tecnològics, que disposi l'empresa. (3 mesos)

▪ Control de seguretat a les xarxes privades que s'usen o puguin ser usades per al teletreball (risc de revisió 3 mesos).

▪ Usar sempre connexions externes segures i autoritzades, en tot cas.

Aquets controls i protocols de seguretat s'han de realitzar i executar per professionals, sent els responsables de transmetre les instruccions, formar al personal i executar les mesures de seguretat, així com millorar-les i adaptar-les a nous sistemes o requeriments.

Respecte a la protecció de dades de caràcter personal consta en totes les empreses que conformen l'AIE, els corresponents documents de seguretat, realitzat per professionals del sector.

▪ Per les empreses autoritzades a l'ús de dades o arxius de tercers, en aquest cas Ajuntament de Tarragona:

- Guardar degudament document d'autorització d'ús.
- Limitació física d'ordinadors que puguin accedir a dades personals en arxius de tercers. (claus d'accés)
- Limitació de persones autoritzades que puguin accedir a dades personals en arxius de tercers. (claus personals d'accés)
- Control intern de llistats puntuals per dies, setmanes o mesos, de dades consultades, equips informàtics i comprovar la necessitat de la consulta.

- Control extern d'us i consulta de dades, reunions mínimes anuals amb responsables de protecció de dades i seguretat informàtica de l'Ajuntament de Tarragona, per tal de fer puntejos d'accés i la seva necessitat.

2.3.- PROTOCOL EN CAS D'USAR SISTEMES DE VIDEOVIGILÀNCIA

Independentment del contingut de cadascun dels documents de seguretat de les empreses que conformen l'AIE, és molt important tenir present en cas d'usar-se càmeres de videovigilància, que, conforme a l'article 5.1 del RLOPD (vigent -abril 2017), una dada de caràcter personal és «qualsevol informació numèrica, alfabètica, gràfica, fotogràfica, acústica, o de qualsevol altre tipus, concernent a persones físiques identificades o identificables».

Les imatges amb independència del format en el qual estiguin contingudes, formen part de les dades de caràcter personal. Això s'estén a l'ús de càmeres, càmeres de vídeo i a qualsevol mitjà que capti o registri imatges. La videovigilància va substituint a altres maneres de mantenir la seguretat encara que en alguns casos pot tenir una finalitat de control en el cas de les empreses. Conforme aquest raonament, és essencial ser molt escrupolós en la seva utilització i han de seguir-se rigorosament les normes en les quals es regula aquesta matèria (LOPD (RCL 1999, 3058) i RLOPD (RCL 2008, 150)). És destacable també la Instrucció 1/2006, de 12 de desembre, de l'AEPD sobre el tractament de dades personals amb finalitats de vigilància a través de sistemes de càmeres o càmeres de vídeo. D'altra banda, els Estats Membres van a anar establint guies d'actuació per a empreses en aquesta matèria, ja que, per a maig de 2018 les normes que estableix el Reglament Europeu de Protecció de Dades han d'incloure's en les legislacions dels diferents Estats Membres.

Per evitar incórrer en aquest tipus de riscos, és important que es segueixin aquestes recomanacions:

▪ Abans que s'instal·li un sistema de videovigilància s'ha d'analitzar amb deteniment si és el més idoni d'acord amb l'objectiu que pretén. És d'interès les recomanacions que l'AEPD inclou en la seva guia sobre videovigilància, ja que, informa de com la utilització d'aquests dispositius pot afectar al dret de protecció de dades.

▪ La utilització de càmeres de vídeo ha d'estar sempre subjecta al principi de proporcionalitat i ha de ser molt rigorós en entorns sensibles.

▪ Quan les càmeres estiguin connectades a Internet s'establiran especials mesures de seguretat, com per exemple procediments d'identificació i autenticació d'usuaris que formen part del sistema i no permetre l'accés a usuaris no autoritzats.

▪ En cas d'entorns especialment sensibles, la zona video-vigilada ha de ser la mínima imprescindible i mai incloent banys o vestuaris.

▪ En el cas de càmeres que tinguin accés a la via pública, no poden captar, com a norma general imatges del carrer des d'instal·lacions privades. Pot concórrer l'excepció si es impossible de fer-ho per la seva ubicació o perquè resulta absolutament imprescindible.

▪ En tot cas les empreses que conformen l'AIE assessoraran o dirigiran les consultes als seus professionals de protecció de dades en cas que fos necessari.

▪ Si la videovigilància afecta l'àmbit d'una relació laboral ha de garantir-se el respecte dels drets dels treballadors.

▪ En les instal·lacions video-vigilades, per complir amb el deure d'informació que exigeix l'article 5 de la LOPD, ha de col·locar-se com a mínim un distintiu que sigui visible que inclogui les paraules «ZONA VIDEO-VIGILADA».

▪ L'organització que compti amb sistemes de videovigilància ha de tenir a la disposició dels interessats impresos informatius legalment establerts.

▪ El fitxer de videovigilància ha d'estar inscrit en el Registre General de Protecció de Dades, tret que els enregistraments siguin solament a temps real.

▪ Les imatges gravades han de conservar-se com a màxim durant el termini d'un mes des de la captació.

▪ En el cas que una empresa de seguretat sigui l'encarregada del sistema de videovigilància, ha d'haver-se subscrit forçosament un contracte que inclogui clàusules de protecció de dades.

El present Reglament ha estat aprovat pel Consell d'Administració en sessió del **30 de novembre de 2017.**

El present Reglament es difondrà per correu electrònic a tot el personal de l'AIE per a coneixement del seu equip humà.