

Protecció de dades

[Fotografies i imatges d'exemple]

■ Presentació

El mes d'abril de 2016 es va aprovar el Reglament (UE) 2016/679 del Parlament 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 4.5.2016).

Aquesta nova regulació, que per primera vegada es fa a través d'un reglament europeu, ha comportat canvis significatius en la protecció de dades de caràcter personal, tant des del punt de vista dels drets de les persones com de les obligacions de les persones i entitats que tracten dades de caràcter personal.

Les entitats socials, per la seva tasca d'atenció directa, compten amb moltes dades personals de persones usuàries i voluntàries, que ara han de gestionar i protegir de manera diferent a com ho feien fins al moment. Moltes d'elles han contractat un DPO (Delegat de Protecció de Dades), però moltes no tenen capacitat per contractar aquesta figura i tenen dificultat per saber com han de gestionar les seves dades.

Des de fa dos anys, la Taula d'entitats a través del projecte m4Social ofereix formació gratuïta a les entitats per tal d'empoderar personal intern en aquesta matèria. Com a part d'aquest procés s'ofereix un banc de recursos amb l'objectiu de sintetitzar coneixements, exposar els casos que generen més dubtes i oferir una sèrie de documents guia.

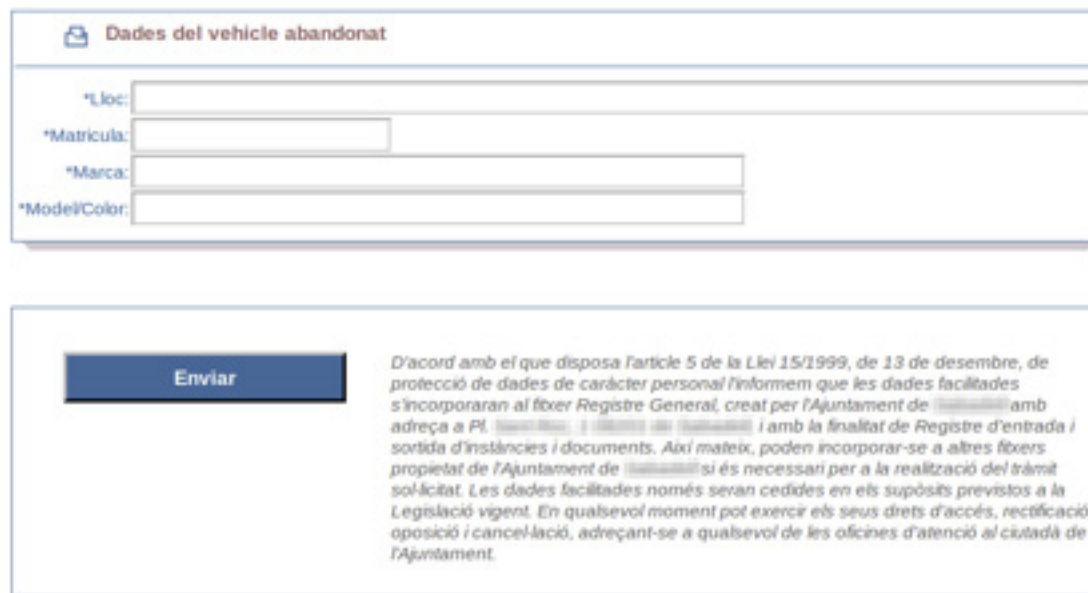
Aquesta presentació conté exemples de situacions a tenir en compte, bones i males pràctiques detectades de forma recurrent i casos que ens ajudaran a recordar tota la dimensió de la protecció de les dades personals.

Problemes a les pàgines web i xarxes socials

■ Formulari web

S'observen els següents problemes:

1. S'esmenta la llei antiga
2. Es parla de fitxers en lloc de tractaments
3. Els drets no es poden exercir a través del web
4. La finalitat no està vinculada amb el formulari



Dades del vehicle abandonat

*Lloc:

*Matrícula:

*Marca:

*Model/Color:

Enviar

D'acord amb el que disposa l'article 5 de la Llei 15/1999, de 13 de desembre, de protecció de dades de caràcter personal informem que les dades facilitades s'incorporaran al fitxer Registre General, creat per l'Ajuntament de [redacted] amb adreça a Pl. [redacted] i [redacted] i amb la finalitat de Registre d'entrada i sortida d'instàncies i documents. Així mateix, poden incorporar-se a altres fitxers propietat de l'Ajuntament de [redacted] si és necessari per a la realització del tràmit sol·licitat. Les dades facilitades només seran cedides en els supòsits previstos a la Legislació vigent. En qualsevol moment pot exercir els seus drets d'accés, rectificació, oposició i cancel·lació, adreçant-se a qualsevol de les oficines d'atenció al ciutadà de l'Ajuntament.

Més informació: https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/V10-CAT-Guia-sobre-el-deure-dinformar-en-el-RGPD-amb-disseny.pdf

■ Fotos a les xarxes socials

S'observen els següents problemes a la fotografia:

1. Fa identificables persones menors d'edat
2. Fa identificables persones d'una cultura concreta
3. Es produeix en una situació que dificulta l'exercici del dret a l'oposició (1)

(1) **Més informació:** <https://apdcat.gencat.cat/ca/documentacio/RGPD/novetats/#bloc7>



Participació Poble @ParticipacioPoble . 2 de juny

Desfilada de vestits tradicionals Chadda Magrebí a Càrrrec de l'Associació X



■ Fotos a les xarxes socials

S'observen els següents problemes a la fotografia:

1. Fa identificable una persona amb nom i cognoms
2. La fotografia és un primer pla molt explícit



Ajuntament d'un Poble @AjuntamentdunPoble . 13 de juliol ✓

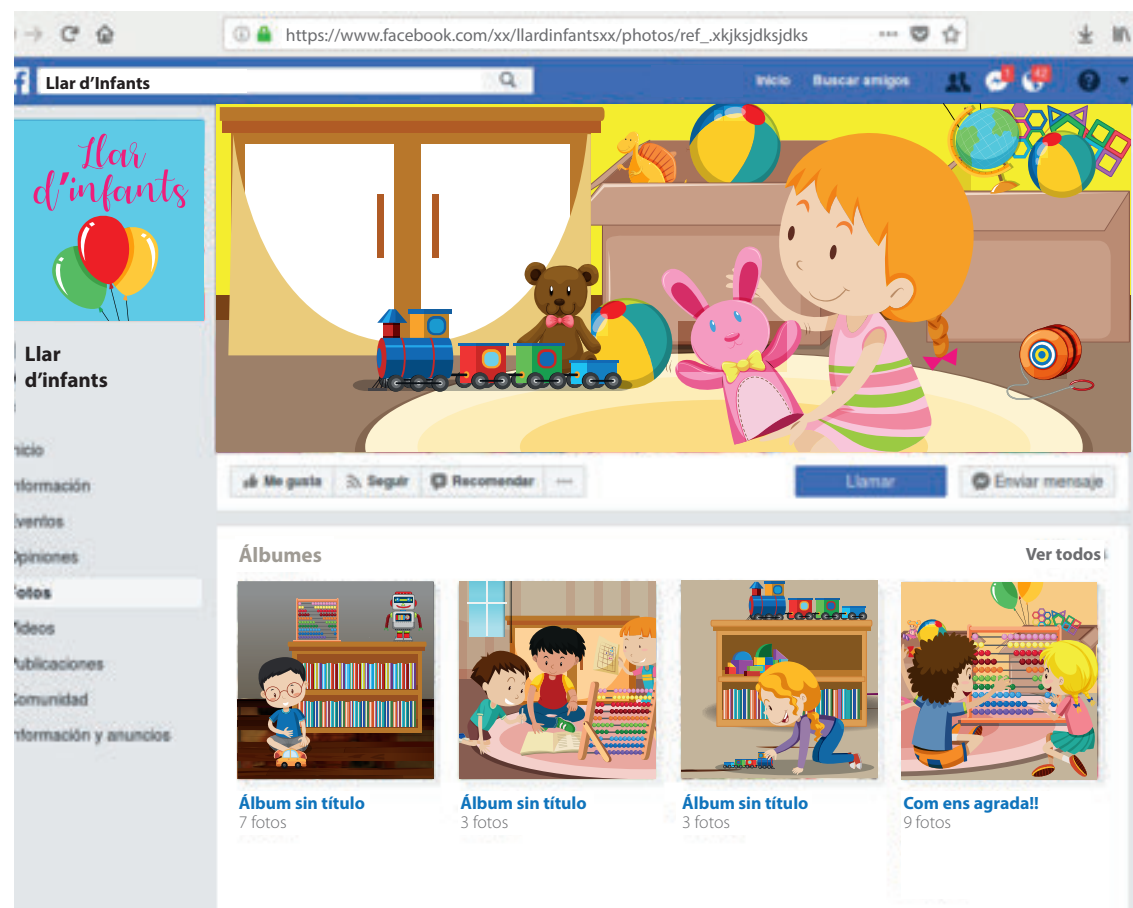
El nen Jordi Mestrex Gonzàex va ser seleccionat pel equip de la Comarca en la trobada territorial benjamins del poble veí. Moltes felicitats Jordi!



■ Ús de les xarxes socials

S'observen els següents problemes amb l'ús d'aquest perfil de Facebook

1. No és proporcional l'ús d'imatges on es poden identificar els infants amb un projecte educatiu com el del centre
2. Els àlbums no només són accessibles per les famílies interessades sinó a qualsevol visitant d'Internet



■ Protecció a les xarxes socials

En aquesta fotografia s'aconsegueix:

1. Donar la notícia que interessa als destinataris
2. Protegir la identitat de les persones que hi apareixen



Ajuntament d'un Poble

@AjuntamentdunPoble

Segueix



La Policia Municipal de #Poble estrena uniforme demà. S'adapta així al canvi que han adoptat totes les #policieslocals de Catalunya



17:34 · 1 d'Agost 2023

4 retuits 3 agradaments



■ Fotos a xarxes socials

S'observen els següents problemes a la fotografia:

1. Fa identificables persones amb risc d'exclusió o diversitat funcional

Es produeix en una situació que dificulta l'exercici del dret a l'oposició (1)

(1) **Més informació:** <https://apdc.cat/gencat.cat/ca/documentacio/RGPD/novetats/#bloc7>



Ajuntament d'un Poble

@AjuntamentdunPoble

Segueix



#Poble acosta l'oferta cultural a persones en risc d'exclusió social o amb discapacitat mitjançant el #programaAProp



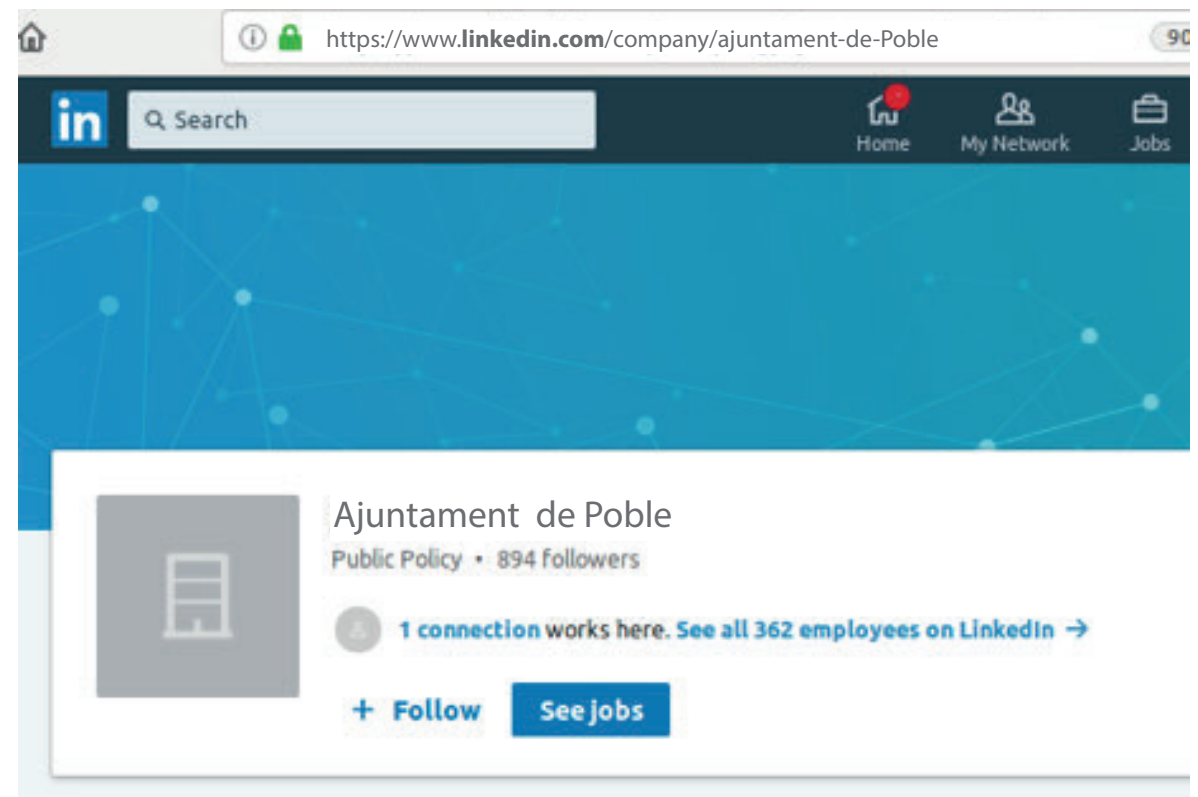
17:14 · 12 d'Agost 2023

6 retuits 9 agradaments

■ Desprotecció a les xarxes socials

A la següent imatge s'observa amb quina facilitat es poden conèixer les identitats de totes les persones treballadores d'una entitat.

Això facilita la feina als que volen realitzar un robatori de dades.



Política de privacitat

La política de privacitat del web ha de ser correcte, clara i suficient.



Problemes amb proveïdors i treballadors

■ Garanties dels proveïdors

S'ha de sol·licitar als proveïdors que aportin proves del seu compliment en matèria de protecció de dades.

Algunes d'aquestes proves poden ser:

1. Certificació de compliment amb mesures de seguretat.
2. Resums executius d'haver superat favorablement auditories.

¿Por qué IIISectorSOFT?

- ✓ cumplimiento RGPD
- ✓ integración con ERP
- ✓ segmentación de clientes
- ✓ campañas automáticas
- ✓ gestor de citas
- ✓ página web y App móvil
- ✓ pago online
- ✓ y ¡mucho mas!

 IIISectorSOFT



Contacto

Nombre

Correo Electrónico

Teléfono

Mensaje

Acepto la política de privacidad

Política de privacidad

Actualizadas a 21/5/18

En cumplimiento del Capítulo II de la ley 34/2002, LSSICE, los informamos que la presente **III Sector SOFT** de ahora en adelante también el Prestador, domiciliada a Av. xxxxxx (Barcelona), con CIF xxxxxxxx teléfono de contacto xxxxxxxx y email: xxxxxx@xxxxx

III Sector SOFT como responsable del presente Sitio web y en conformidad con lo que dispone la normativa vigente en materia de protección de datos personales, el Reglamento (UE) 2016/679 de 27 de abril de 2016 (RGPD) relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y por la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE), tiene implementadas todas las medidas de seguridad, de índole técnica y organizativas, establecidas en el Real decreto 1720/2007 de 21 de Diciembre, (que desarrolla la LOPD) para garantizar y proteger la confidencialidad, integridad y disponibilidad de los datos introducidos.

Dicho Fichero se encuentra debidamente inscrito en el Registro de Ficheros de la Agencia Española de Protección de Datos.

■ Compromís i salut corporativa

S'han d'implementar mecanismes que assegurin la salut corporativa i redueixin el risc de robatori de dades per part de les persones treballadores.

Per exemple, mitjançant:

1. Verificar mitjançant indicadors en els processos de selecció
2. Supervisió i entrenament



EL ESPAÑOL

Jordi Roubes, presidente de Mediapro. Europa Press

FÚTBOL

Robert Cama, el informático en el centro del espionaje de Rosell

Como director técnico de Mediapro supuestamente sustrajo cientos de e-mails para filtrárselos a Sandro Rosell quien, ya presidente del Barça, lo contrató para idéntico puesto por 100.000 €.

6 febrero 2016 - 02:29

■ Supervisió de les persones usuàries

S'han d'implementar mecanismes que permetin verificar que l'ús que es realitza dels sistemes d'informació és l'adequat.

En cas de pèrdua o robatori de dades s'ha de disposar d'un sistema de control que permeti identificar la persona que ha comès l'acte il·lícit.

Artículo 66. Control empresarial

La empresa podrá adoptar las medidas de verificación de los sistemas informáticos que crea necesarias con el fin de comprobar su correcta aplicación, poder certificar el óptimo rendimiento y seguridad de la red de la empresa y que su utilización por parte de los trabajadores usuarios no derive a fines extra profesionales.

A estos efectos las empresas podrán utilizar software de control automatizado para controlar el material creado, almacenado, enviado o recibido en la red de la empresa, así como controlar sitios visitados por sus trabajadores usuarios en Internet, espacios de charla o grupos de noticias, revisar historiales descargados de la red de Internet por usuarios de la empresa, revisar historiales de mensajes, de correo electrónico enviados y recibidos por los trabajadores usuarios.

En la adopción de las medidas de verificación de los sistemas telemáticos habrá de tenerse en cuenta:

- El acceso ha de ser necesario para facilitar razonablemente las operaciones empresariales; si existen medios de menor impacto para el empleado, la empresa hará uso de ellos.
- La privacidad y la dignidad del usuario estarán siempre garantizadas.
- El correo electrónico y los archivos serán inspeccionados en el puesto de trabajo, durante

■ Supervisió de les contrasenyes

S'ha d'assegurar que les contrasenyes de l'entitat no s'han divulgat per Internet. Per exemple, mitjançant eines com: haveibeenpwned.com

S'ha d'entrenar a les persones usuàries amb simulacres d'atacs (com per exemple *phishing*) que permetin reduir la probabilitat de patir enganys.

També s'ha d'assegurar que s'utilitzen contrasenyes segures.

A la imatge es pot observar un exemple de correus electrònics i contrasenyes.



Problemes informàtics

■ Protegir-se dels lladres de dades

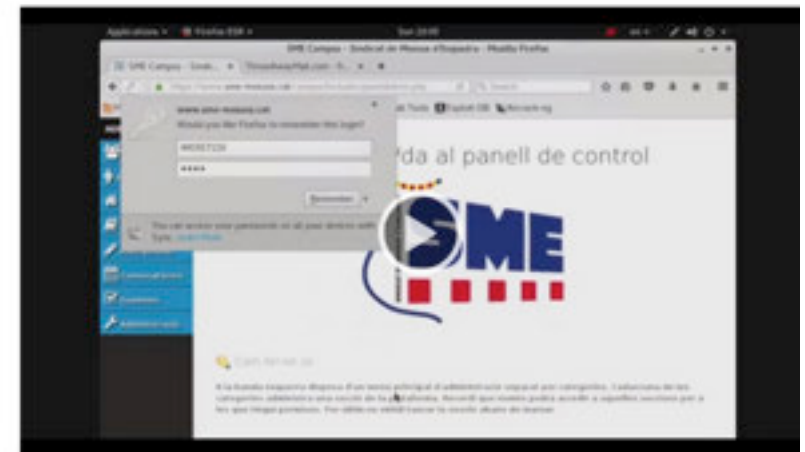
Els lladres de dades aprofiten les vulnerabilitats del sistema d'informació per robar la informació.

S'han d'aplicar les mesures de seguretat suficients per protegir-se.

S'ha de revisar periòdicament l'eficàcia de les mesures mitjançant auditories (per exemple de Ciberseguretat).

TRIBUNALES · Vídeo

¿Cómo actuó el hacker que atacó el sindicato de los Mossos?



El 'hacker' de la web de los Mossos afirma que se animó a 'hacer un sencillo ataque'

- Piratas informáticos hackean y filtran datos de miles de mossos
- Arranca en Gijón el juicio contra la cúpula española de Anonymous

■ Sales de servidors

L'espai on s'ubiquen els sistemes d'informació central han d'estar ben condicionats.

Els servidors han d'estar tancats dins de l'armari de comunicacions.

Les còpies de seguretat s'han de guardar en un lloc diferent i segur, no dins de la mateixa sala .

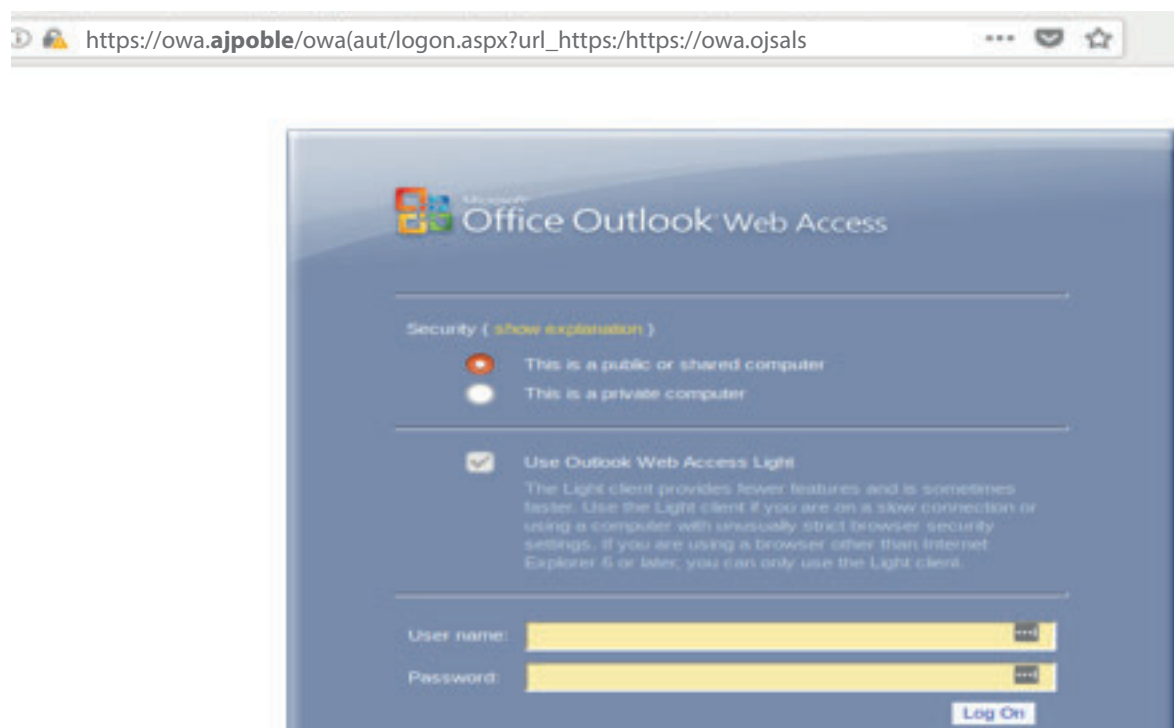


■ Accessos remots

Si hi han accessos remots al sistema d'informació, s'han d'assegurar disposant d'un control d'accés avançat.

Una autenticació on només s'utilitza una contrasenya és insuficient.

És necessari, a més de la contrasenya, incorporar un segon factor d'autenticació (com per exemple un codi al mòbil).



■ Suports segurs

Si hi ha persones usuàries de la documentació que traslladen dispositius informàtics, s'ha d'evitar el risc de pèrdua.

Els suports informàtics han d'incorporar un xifrat predeterminat i una clau d'accés per desxifrar.



Problemes de custòdia de les dades

■ Zona d'arxiu

La zona d'arxiu ha d'assegurar-se:

1. No ubicant la documentació en zones de pas.
2. Ubicant la documentació en sales que es puguin tancar.
3. Ubicant la documentació dins de mobiliari amb sistema de tancament.
4. Creant un criteri d'arxiu que permeti identificar ràpidament on es troba la documentació d'una persona.



■ Llocs de treball

Els llocs de treball han d'assegurar-se:

1. Permetent tancar amb clau els llocs de treball on hi hagi documentació o suports informàtics.
2. Disposant d'un mobiliari amb sistema de tancament per la documentació.
3. Evitant que totes les persones usuàries abandonin el lloc de treball, sense tancar, i deixant sense custòdia les dades.



■ Atenció al públic

Les zones d'atenció al públic han d'evitar que, quan s'atengui una persona al taulell, hi pugui haver persones escoltant la conversa.



■ Trasllet de documentació

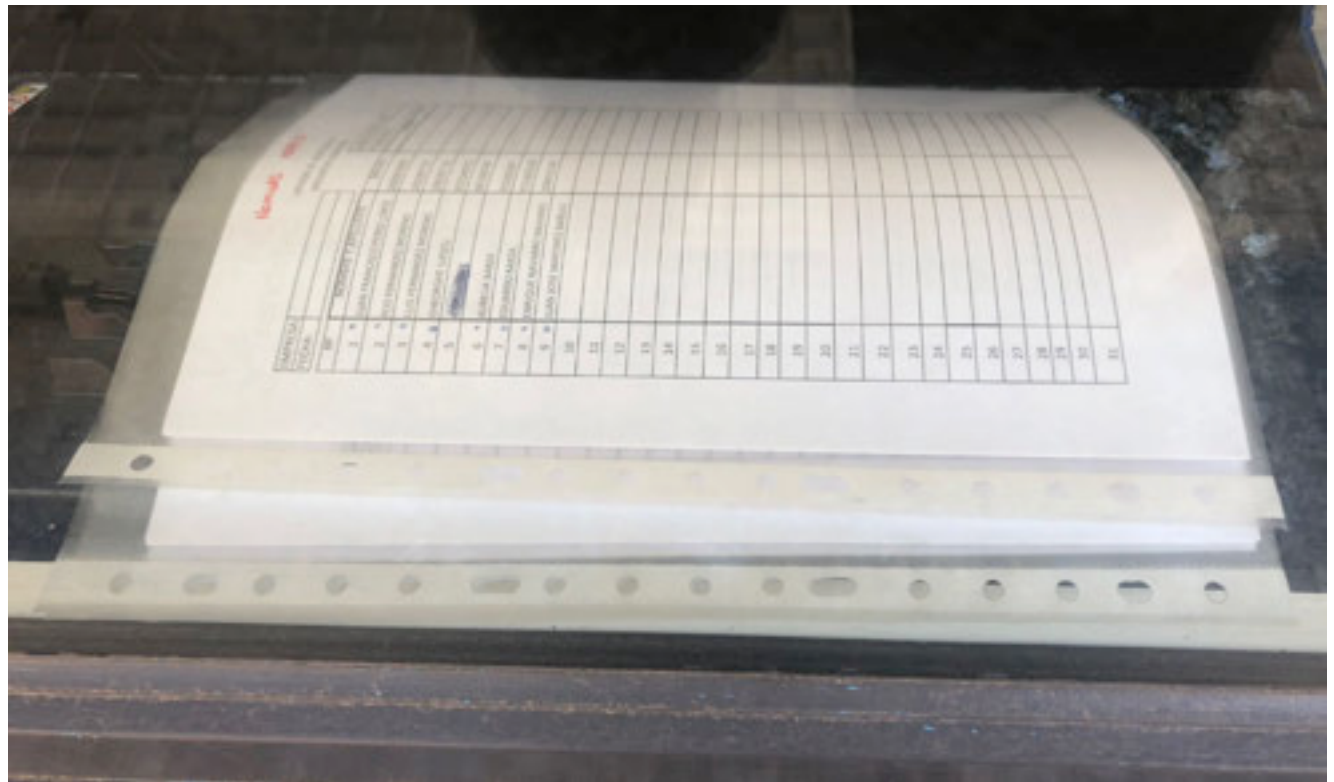
Exemple amb un camió que transporta carpetes amb informació relativa a subvencions atorgades.

Durant el trasllat de documentació cal que s'adoptin mesures adients per garantir la confidencialitat, integritat i disponibilitat de les dades



■ Deixadesa en la custòdia d'informació

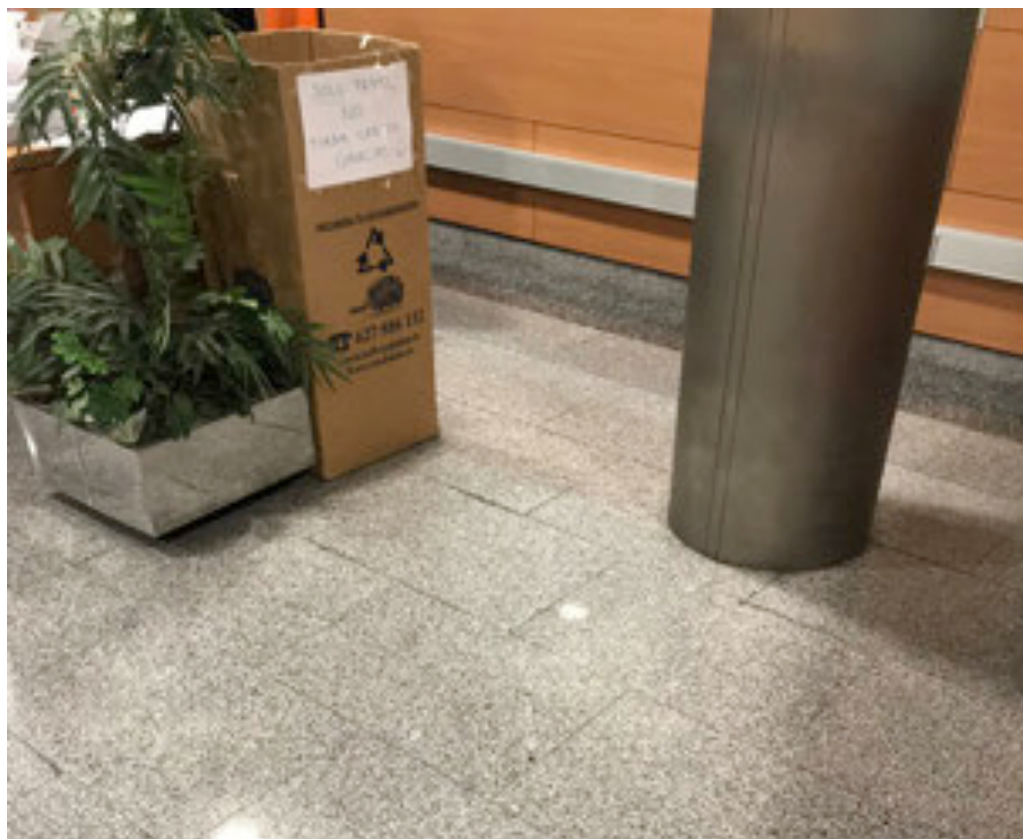
Exemple d'un local obert al públic que deixa documents amb informació sobre nòmines al terra de tal manera que són visibles des de la via pública. Aquests documents contenen nom, cognoms i DNI dels afectats



■ Destrucció d'informació

Exemple d'una sala d'espera d'un hospital públic han col·locat un contenidor amb un cartell que indica: “Sólo papel, no tirar cartón. Gracias!”

Cal recordar que la destrucció d'informació en format paper és un tractament de dades i s'han d'aplicar mesures de seguretat que, entre altres, garantitzin la confidencialitat de la informació i el deure de secret.



■ Empreses destructores de documentació

Exemple d'un treballador d'una empresa que es dedica a la destrucció de la documentació que abandona la furgoneta en aquest estat. No es realitza una custòdia de la documentació, ni es garanteix la confidencialitat, integritat ni la disponibilitat de les dades. Es recomanaria a l'empresa la implementació de protocols d'actuació per complir la normativa de protecció de dades i l'adopció de mesures de seguretat adients a l'efecte.



■ Àmbit educatiu

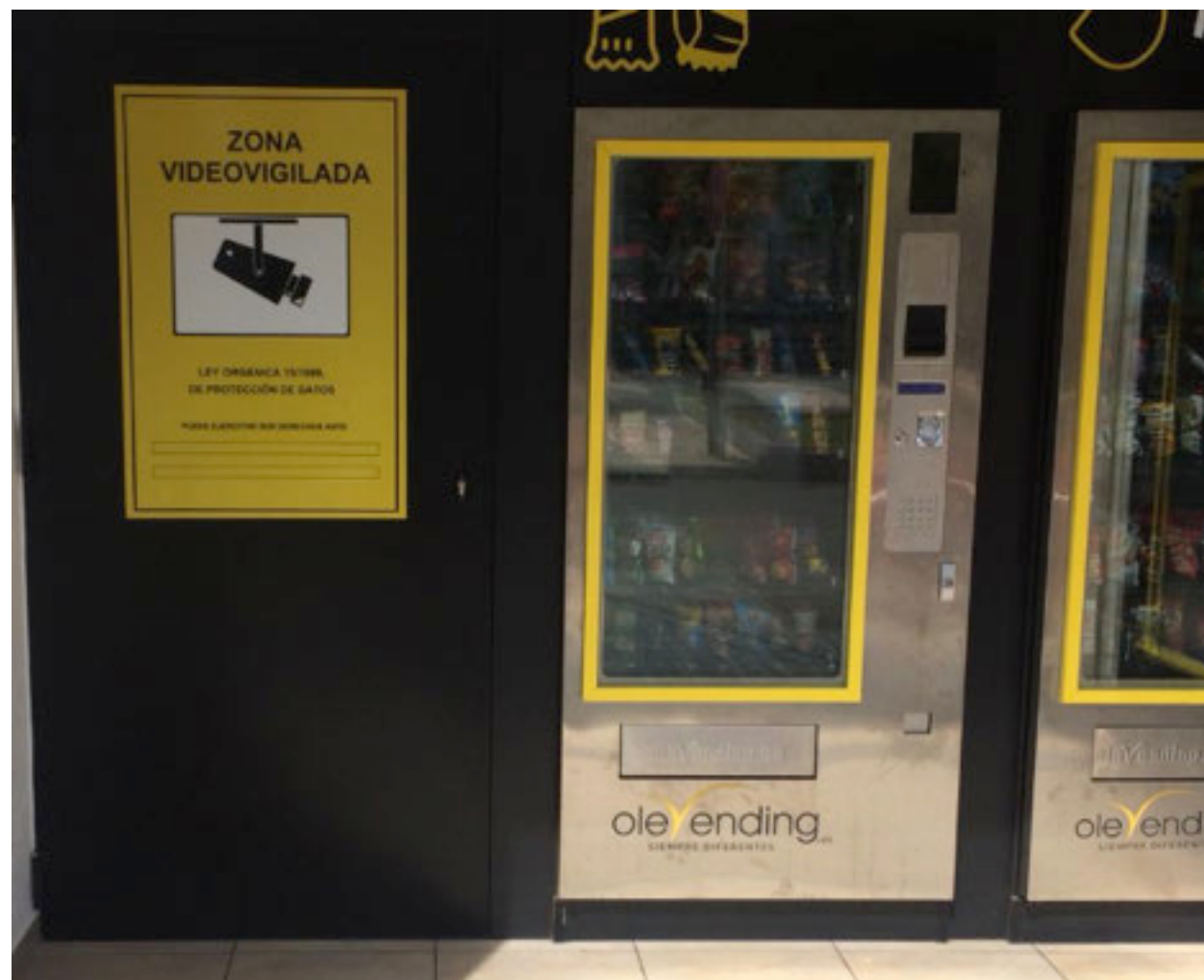
Una escola que col·loca la imatge de menors d'edat visibles des de la via pública. Caldria considerar si els representants legals dels menors han consentit aquest tractament i en quins termes han autoritzat el tractament de la imatge dels menors. També cal considerar fins a quin punt aquest tractament de dades respon a una finalitat educativa.



Problemes de videovigilància


■ Distintiu informatiu i deure d'informació prèvia

Cal col·locar un distintiu informatiu que indiqui que s'accedirà a una zona videovigilada. Aquest distintiu cal que sigui clarament visible, però també cal que indiqui la informació que exigeix la normativa: responsable del tractament, lloc d'exercici dels drets de protecció de dades i informació addicional (termini de conservació, finalitat del tractament i destinataris de les imatges, p. ex.). En aquest cas, s'incompleix el deure d'informació prèvia.



■ Contingut distintiu informatiu

Aquest cartell conté informació molt detallada sobre el tractament de les imatges, no obstant això, dona per fet el més important: indicar qui és el responsable del tractament i el lloc on es poden exercir els drets de protecció de dades. D'altra banda, tampoc són correctes alguns dels drets que s'hi mencionen perquè en aquest tractament no és possible revocar el consentiment (la base legal és l'interès públic) ni és possible la rectificació (les imatges captades no es poden rectificar).



PROTECCIÓN DE DATOS

Le informamos que sus datos serán tratados de conformidad con lo dispuesto en las normativas vigentes, por lo que se le facilita la siguiente información del tratamiento:

Finalidad del tratamiento: control de la actividad interna a través de un sistema de videovigilancia por motivos de seguridad.

Criterios de conservación de los datos: se conservarán un máximo de 30 días naturales.

Comunicación de los datos: No se comunicarán los datos a ningún destinatario excepto si lo solicita las FCSE. O autoridades judiciales.

Derechos que asisten al interesado:

- Derecho a retirar el consentimiento en cualquier momento.
- Derecho de acceso, rectificación y supresión de sus datos y a la limitación u oposición a su tratamiento.
- Derecho a presentar una reclamación ante la Autoridad de control (agpd.es) si considera que el tratamiento no se ajusta a la normativa vigente.

(UE) 2016/679 de 27 de Abril (GDPR)
Ley Orgánica (ES) 15/1999 de 13 de diciembre (LOPD)
Instrucción 1/2006 de 8 de noviembre de la AEPD.

Puede ejercer sus derechos ante el **RESPONSABLE DEL TRATAMIENTO:**

RESPONSABLE DE TRATAMIENTO.
C/ DIRECCION RESPONSABLE

■ Finalitat del sistema de videovigilància

El més rellevant d'aquest distintiu de videovigilància és que informa de finalitats diferents de les de seguretat de les instal·lacions, béns i persones. Indica que les imatges s'utilitzaran per a una finalitat diferent (publicació a pàgina web). Cal recordar que per aquesta finalitat és imprescindible el consentiment de l'afectat de forma expressa, informada, inequívoca, revocable, lliure i granular. D'altra banda, també s'ha de considerar allò que preveu la L.O. 1/1982 sobre el dret a la imatge.



■ Ubicació del distintiu informatiu

El cartell informatiu sobre videovigilància d'un establiment d'un centre comercial s'ha de col·locar a un lloc clarament visible. Preferiblement, a l'alçada dels ulls. En aquest cas, s'ha col·locat a la part inferior de l'aparador. El més adequat seria haver-lo col·locat a la porta d'entrada o als laterals d'aquesta.



■ Deure d'informació prèvia

El cartell informatiu sobre el tractament de videovigilància ha de contenir informació sobre qui és el responsable del tractament, lloc d'exercici dels drets de protecció de dades i informació addicional (termini de conservació, finalitat del tractament i destinataris de les imatges, p. ex.). En aquest cas, s'incompleix el deure d'informació prèvia.



■ Deure d'informació prèvia

Si es realitza un tractament de dades mitjançant un sistema de videovigilància, s'ha de complir el deure d'informació prèvia. Si bé és cert que és suficient amb un distintiu a l'efecte, aquest ha de contenir informació suficient que permeti conèixer qui és el responsable del tractament, el lloc d'exercici dels drets de protecció de dades i la informació addicional (termini de conservació, finalitat del tractament i destinataris de les imatges, p. ex.).



■ Deure de secret i ubicació dels monitors

En aquesta cerveseria han ubicat el monitor del sistema de videovigilància a dins el local de manera que els clients de l'interior poden veure el que ocorre a la terrassa del local. Això vulnera el deure de secret i el principi de confidencialitat de les dades que es tracten a través del sistema de videovigilància. Els monitors s'haurien d'ubicar en un lloc que no permeti l'accés de terceres persones.

