

xera

Acció social



LLEI ORGÀNICA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL (LOPD)

XERA 2024

Contenido

Objectiu	3
Normativa de protecció de dades per a associacions sense ànim de lucre.....	3
Compliment de la llei	3
Compromís de Confidencialitat XERA 2024	6
Contractes de protecció de dades a Encarregats externs	6
Protocol específic per a accessos protegits: digitals i físics	7
Anàlisi del Risc i mesures de Seguretat	8
Valoració anual de la protecció de dades.....	9
Annexes	10

Objectiu

L'objectiu del present protocol és informar que a XERA **garantim que el tractament de dades personals que gestiona l'empresa compleixi amb els requisits legalment establerts en l'ordenament jurídic.**

En aquest sentit, aquest protocol conté els principis necessaris que han de ser aplicats per a garantir que tots els sistemes d'informació, suports i equips emprats per al tractament de dades de caràcter personal siguin protegits d'acord amb el que estableix la llei.

Els principis i normes continguts en aquest protocol han estat confeccionats conforme als criteris d'ètica empresarial i de compliment normatiu que regeixen en l'empresa, que es compromet a gestionar les dades personals en els fitxers de la seva titularitat d'una forma responsable i de conformitat amb la normativa aplicable.

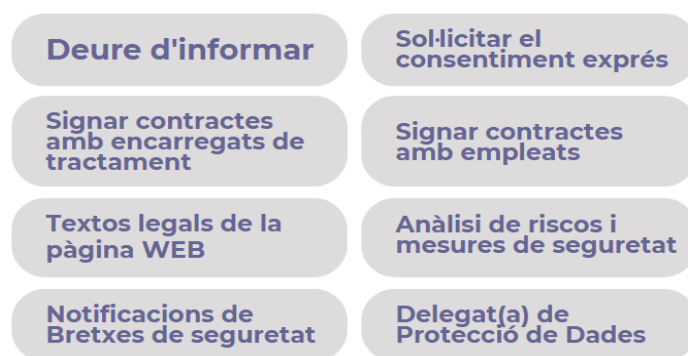
Normativa de protecció de dades per a associacions sense ànim de lucre

Les normes que regulen la protecció de dades en associacions sense ànim de lucre són:

- A nivell europeu, el *Reglament General de Protecció de Dades 2016/679*.
- A nivell nacional:
 - *Reial decret llei 5/2018, de 27 de juliol*, de mesures urgents per a l'adaptació del Dret espanyol a la normativa de la Unió Europea en matèria de protecció de dades.
 - LOPDGDD: Llei orgànica de Protecció de Dades de Caràcter Personal i Garantia de Drets Digitals.
 - Llei de Serveis de la Societat de la Informació i Comerç Electrònic (LSSI).
 - Llei 34/2002, d'11 de juliol que regula les transaccions mitjançant mitjans electrònics.

Compliment de la llei

Per a complir la llei de protecció de dades en associacions, a XERA seguim els següents requisits:



1.1 Deure d'informar: En el moment de la recollida de dades de caràcter personal, informem a les persones interessades (professionals, famílies, participants, proveïdors, altres...) de manera clara i concisa de:

- a) quines dades es tractaran
- b) durant quant temps
- c) base jurídica

A més d'això, no demanem més dades dels necessaris per a dur a terme la finalitat. I en el cas que es vagin a cedir les dades personals a altres professionals de l'equip o qualsevol altre tercer, ho informarem l'interessat.

1.2 Sol·licitar el consentiment exprés

Segons el RGPD, a XERA solament s'admet el **consentiment exprés**: aquell que s'atorga de manera concreta, explícita i directa, podent registrar-se d'una o diverses maneres que no deixin lloc a dubtes. El més habitual és donar-ho mitjançant la signatura d'algun document oficial o clàusula, perquè les parts puguin acudir a ell en el futur en cas de desacord.

1.3 Signar contractes amb l'encarregat de tractament

Totes les persones que conformen l'equip de XERA que tinguin accés a les dades d'usuaris (incloent les persones practicants/voluntàries, equip de socis, equip de comissions i altres col·laboradors de l'entitat) han de signar un **acord de gestió de tractament de dades**.

Totes les persones signaran un document on es reculli la confidencialitat en el tractament de les dades personals dels usuaris i beneficiaris.

(Veure apartat [Compromís de Confidencialitat i Annex I](#))

1.4 Signar contractes amb empleats

Les dades sensibles de l'entitat estan protegides:

- a) **A través de la limitació d'accés:** cada professional té accés a les carpetes de l'OneDrive que correspongui a les seves funcions. L'OneDrive és el

sistema que ens permet emmagatzemar i protegir els arxius, compartir-los amb altres usuaris i accedir a ells des de qualsevol lloc en tots els teus dispositius.

En aquestes carpetes estan incloses les informacions sobre dades d'identificació personal i dels/les usuaris/es vinculats/des als seus programes i projectes de XERA.

Exemple: la coordinació de RRHH té accés a la informació de les persones professionals; la coordinació de l'àrea administratiu, a la informació financera; la direcció té accés a totes les carpetes.

- b) A través de l'accés restret amb contrasenyes:** hi ha documents que contenen informació secreta amb contrasenyes segures que s'actualitzen a cada 12 mesos. És important protegir aquestes per a evitar accessos no autoritzats i possibles riscos de seguretat.

1.5 Textos legals de la pàgina WEB

La pàgina web de XERA compleix amb l'obligació d'actualitzar els seus textos legals al RGPD. Aquests són: l'**avís legal**, la **política de privacitat** i la **política de cookies**.

1.6 Anàlisi de riscos i mesures de seguretat

Amb caràcter previ a dur a terme qualsevol activitat de tractament de dades, és necessari realitzar una anàlisi de riscos per a determinar les amenaces a les quals podrien estar exposats les dades personals dels interessats derivades de fer aquest tractament i poder així aplicar les mesures de protecció més adequades per a garantir la seguretat les dades.

Sent així, a XERA fem un anàlisi de riscos i mesures de seguretat, i també comptem amb una avaluació d'impacte, amb l'objectiu d'avaluar de manera anticipada els potencials riscos als quals estan exposats les dades personals que es manegen. I determinar les mesures de seguretat més adequades per a ells.

(Veure apartat [Anàlisi de riscos i mesures de seguretat](#))

1.1 Notificacions de Bretxes de seguretat

Qualsevol bretxa de seguretat serà comunicada a l'AEPD (l'autoritat competent nacional) en un termini màxim de 72 hores des que es tingui coneixement. En els casos en què es vulnerin de manera greu els drets dels/les interessats, també informarem els/les interessats/des.

1.2 Delegat(a) de Protecció de Dades

A XERA tractem amb dades personals sensibles i, per això, estem obligats a tenir una persona Delegada de Protecció de Dades (DPO).

La persona Delegada de la Protecció de Dades de XERA es: Diego Sánchez.

Compromís de Confidencialitat XERA 2024

El contracte es un **consentiment exprés** i escrit que haurà de ser signat per totes les persones vinculades a l'entitat al moment de la contractació/vinculació, i s'haurà d'actualitzar una vegada a l'any.

En aquest contracte de confidencialitat, l'empresa i les persones vinculades acorden que la informació de tipus privada o sensible a la qual es tingui accés no serà posada a la disposició de tercers.

Serà la persona professional de Recursos Humans de l'entitat la responsable a enviar i recollir les signatures d'aquests documents.

(Veure Annex I)

Contractes de protecció de dades a Encarregats externs

El contracte de confidencialitat també s'aplica als agents externs que tinguin accés a la informació personal de les persones usuàries dels serveis de XERA i també dels seus treballadors. Així, es tracta d'un pacti bilateral entre empresa i col·laboradors (personis físiques i jurídiques), centris, institucions o altres empreses.

Tots les persones treballadores de XERA que necessitin vincular la informació personal de les persones usuàries del serveis de XERA a altres agents (Serveis Socials, Centres Educatius, Centres Terapèutics, Base de Dades u altres) hauran d'enviar el [COMPROMÍS DE CONFIDENCIALITAT I PROTECCIÓ DE DADES DE CARÀCTER PERSONAL DE XERA](#) i sol·licitar el document signat per una persona de referència d'aquest centre.

Veure Annex II

Protocol específic per a accessos protegits: digitals i físics

Tot el personal vinculat a XERA haurà de saber que hi ha documents de l'entitat que estan protegits per contrasenya: llistat de contrasenyes dels coreus

electrònics corporatius, xarxes socials, accés a la plataforma de base de dades (Midue), plataforma dels riscos laborals (Septra), serveis de difusió d'ofertes de treball/pràctiques de RRHH, Serveis de valoració dels centres de pràctiques, panel de control de pàgina web, accés bancari, entre altres.

Aquesta es una tècnica de control d'accés que ajuda a mantenir les dades protegides de hackers, garantint que només es pugui accedir amb les credencials correctes.

A XERA, gestionem les contrasenyes mitjançant la implementació d'una solució de protecció de contrasenyes dissenyades per a bloquejar contrasenyes dèbils, les variants repetitives i qualsevol característica que pugues ser fàcil d'avinar.

Tota informació protegida estarà especificada en un [Protocol Específic per a Accessos Protegits: digitals i físics](#), el qual tindrà accés només les persones treballadores que la direcció consideri que necessiten dicta informació per a la realització eficient de les seves funcions.

En aquest document es reunirà la informació sobre:

- Documents d'accés de contrasenyes de l'entitat;
- Documents específics d'on s'arxivaran els documents físics de les famílies i sobre com accedir-hi;
- Documents digitals antics dels últims 5 anys;
- Documents físics antics dels últims 5 anys;
- Distribució i criteri de l'accés dels documents digitals actuals;
- Distribució i criteri de l'accés dels documents físics actuals;
- Persones responsables per l'arxivament i accessos estrictes;
- Document dels criteris de permisos necessaris per a accedir a un arxiv. Exemple: sol·licitar a direcció la contrasenya, que s'enviarà mitjançant burofax;
- Accés a les claus i cadenats;
- Calendari de les actualitzacions de contrasenyes;
- Protocol a seguir en el cas que calgui accedir a aquestes dades;
- Com se'n va a produir la destrucció de les dades personals?

No obstant això, tant la direcció com les persones treballadores de XERA tenen la responsabilitat de desenvolupar el seu paper en la protecció de la informació confidencial de la empresa, el que inclou:

- a) Fer ús de contrasenyes segures;
- b) Seguir les polítiques i protocols establerts;
- c) Indicar qualsevol bretxa de seguretat digital i de documents físics a RH o direcció

Anàlisi del Risc i mesures de Seguretat

En les organitzacions més petites, la legislació vigent permet que l'anàlisi de les dades sigui el resultat d'una reflexió documentada sobre les implicacions dels tractaments, tenint en compte els drets i llibertats de les persones interessades.

A XERA, busquem mesures per a identificar i implementar accions que protegeixen les famílies, persones usuàries, persones treballadores, persones en pràctiques i voluntàries, agents externs i persones col·laboradores de amenaces com ara son:

- robatori d'identitat;
- accés no autoritzat;
- robatori/pèrdua de dispositives;
- fugides d'informació;
- robatori de documents físics;
- atacs de suplantació d'identitat;
- accés a través de xarxes Wi-Fi no segures;
- ús de contrasenyes febles;
- falta d'actualitzacions de seguretat;
- accés a través de dispositius no segurs.

Algunes de les mesures de seguretat utilitzades a XERA són:

- **Encriptació de dades:** les dades sensibles emmagatzemades en els nostres sistemes estan encriptats per a protegir-los d'accessos no autoritzats.
- **Polítiques d'accés i control d'usuaris:** comptem amb polítiques clares sobre qui té accés a les dades i quin tipus d'informació poden veure o modificar.
- **Actualitzacions i pegats de seguretat:** mantenim els nostres sistemes i programari actualitzat amb les últimes versions i pegats de seguretat per a protegir-los contra vulnerabilitats conegudes.
- **Auditories regulars:** realitza auditories periòdiques per a identificar possibles bretxes de seguretat i corregir-les a temps. Els professionals durant tot el seu període de vinculació amb XERA són part activa en la detecció dels problemes.
- **Capacitació del personal:** instruïm a les persones treballadores a través de la difusió de protocols sobre les bones pràctiques de seguretat informàtica, com l'ús de contrasenyes segures, la detecció de correus electrònics fraudulents (phishing) i la protecció de dispositius mòbils.
- **Còpies de seguretat:** realització de còpies de seguretat periòdiques de les dades crítiques per a poder recuperar la informació en cas de pèrdua o mal.
- **Compliment normatiu:** assegurem complir amb les lleis i regulacions vigents en matèria de protecció de dades.

La informació completa sobre l'Anàlisi del Risc i mesures de Seguretat estarà disponible a totes les persones vinculades a l'entitat en el conjunt de documentació Compliance.

Valoració anual de la protecció de dades

L'Article 32.1. del RGPD estableix que les mesures de seguretat tindran, a més d'un procés de verificació i avaluació de les dades i dels riscos, un procés de valoració regular.

És per això que a XERA farem anualment una Avaluació de les Proteccions de Dades, que pretén:

- a) Valorar el nombre de famílies que XERA ha atès l'any i el % de quantes famílies han signat documents de consentiment de l'ús de dades i d'imatges.
- b) Quantificar totes les fitxes dels diferents programes de l'entitat i qualificar/quantificar quines dades s'han sol·licitat enguany.
- c) Valorar si les dades sol·licitades són necessàries i compleixen amb una finalitat empresarial.
- d) Quantificar els/les proveïdors/es, i empreses externes que han tingut accessos a les dades dels NNA (nens, nenes i adolescents).
- e) Quantificar els consentiments expressos que s'han recollit d'empreses externes.
- f) Quantificar el nombre de professionals que han signat el document de gestió de tractaments de dades i confidencialitat.
- g) Quantificar els accessos protegits
- h) Valorar si s'ha actualitzat les contrasenyes dels accessos protegits.
- i) Crear un protocol sobre l'accés i destrucció de les dades;
- j) Verificar si s'ha actualitzat l'anàlisi de riscos anualment, actualitzant les mesures de seguretat i avaluació de l'impacte.
- k) Valorar si ha estat necessari fer notificacions de Bretxes de seguretat en un termini màxim de 72h;
- l) Valorar si s'ha indicat un delegat(a) de Protecció de Dades i realitzar valoració de les seves funcions.

Annexes

ANNEX 1: Compromís de Confidencialitat i Tractament de Dades 2024

ANNEX 2: Compromís de Confidencialitat i Protecció de Dades de Caràcter Personal de XERA.

COMPROMÍS DE CONFIDENCIALITAT I TRACTAMENT DE DADES 2024 Associació Educativa XERA	DATA __/__/__
---	-------------------------

Nom i cognoms: _____ **NI/NIE:** _____

En _____ a _____/_____/2024.

D'acord amb el *Reglament General de Protecció de Dades* relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i la lliure circulació d'aquestes dades (RGPD),

L'informem que **les seves dades passaran a formar part d'un fitxer titularitat d'ASSOCIACIÓ EDUCATIVA XERA**, amb domicili social en C/ Rambla de Badal 121, i CIF-G550741868.

Finalitat: L'empresa vol desenvolupar, mantenir, complir i controlar la seva activitat i donar compliment a les obligacions i funcions del departament de Recursos Humans, relatives a les activitats de formació, control d'assistència al treball, formalització de les nòmines, deures en matèria de prevenció de riscos laborals, així com la gestió de canals de comunicació/denúncies implementades per l'entitat de conformitat amb requisits previstos en les normatives en matèria de compliment vigents.

La legitimació per a la recollida de les seves dades es basa en el contracte laboral subscrit amb L'ASSOCIACIÓ EDUCATIVA XERA.

L'informem que per al compliment de les obligacions legals i laborals, les seves dades poden ser comunicats a Administracions Públiques (Seguretat Social, Agència Tributària, Subvencions); Mútues de protecció laboral i serveis de prevenció de riscos laborals o la preservació de la salut dels treballadors; Entitats o clients que exigeixin o davant les quals sigui necessari identificar als empleats: entitats bancàries per a pagaments de nòmines, asseguradores, projectes, formació, missatgeria, així com aquelles entitats o clients que requereixin dades identificatives i laborals del personal per a dur a terme el seu contractat i que acreditin la relació amb l'empresa; Comitès d'empresa, sindicats i delegats de prevenció; plataforma de base de dades.

Drets: Podrà sol·licitar la limitació o oposició al tractament de les seves dades quan es donin determinades circumstàncies i, en aquest cas, únicament seran conservats per al compliment de les obligacions legalment previstes. Per a exercitar els drets anteriorment descrits, haurà de dirigir-se a la persona Responsable del departament de Recursos Humans.

Amb la finalitat de mantenir actualitzats les dades, el/la signant haurà de comunicar qualsevol canvi que es produeixi sobre els mateixos.

Compromís de confidencialitat: en cap concepte, ha d'utilitzar-se ni incorporar-se als sistemes informàtics i arxius documentals d'aquesta entitat, quan això pugui implicar la vulneració de les legislacions anteriorment citades. En compliment de la legislació anteriorment esmentada, **vostè assumeix el compromís de guardar secret professional respecte a les dades personals, dades sobre els clients, estratègies comercials i organitzatives i industrials, i qualsevol altra informació a la qual tingui accés amb el motiu de les funcions assignades.** D'igual mode, l'informem que amb la finalitat de garantir el dret a la intimitat i privacitat del/la persona signant, per part de L'ASSOCIACIÓ EDUCATIVA XERA, en cap concepte vostè ha d'incorporar als sistemes informàtics i arxius documentals d'aquesta entitat, la seva informació de caràcter personal, com a fotos, vídeos o imatges.

Així mateix, de conformitat amb l'article 32 del RGPD, la persona signant es compromet a complir les normes internes de seguretat que afecten el desenvolupament de les seves funcions, així com a l'ús dels equips informàtics, correu electrònic i altres aplicacions a les quals tindrà accés.

Finalment, en relació a les noves implicacions i responsabilitats en matèria de *Responsabilitat Penal de l'Empresa (RPE)*, la persona signant es compromet a aplicar i tenir en consideració els protocols i procediments que estableixi l'entitat en aquesta matèria i que siguin aplicables en l'àmbit de protecció de dades de caràcter personal en els termes previstos en aquest document.

Davant qualsevol dubte, incident, o impossibilitat d'aplicació adequada dels procediments i normes ho comunicarà al responsable que se'l designi en cadascun dels supòsits tal com quedi establert a aquest efecte.

Signatura:

COMPROMÍS DE CONFIDENCIALITAT I PROTECCIÓ DE DADES DE CARÀCTER PERSONAL DE XERA

Data ____/____/____

Dades de l'ENTITAT/EMPRESA/CENTRE/INSTITUCIÓ que rebre els dades personals de XERA

Nom de l'ENTITAT/EMPRESA/CENTRE/INSTITUCIÓ

CIF

Responsable de la gestió de les dades personals

DNI/NIE

Correu electrònic

Telèfon de contacte

COMPROMÍS I CONFORMITAT DEL PROVEÏDOR/COL·LABORADOR

- Reduir l'ús d'informació confidencial a l'estrictament necessari per a la prestació dels Serveis.
- Comprometre's a mantenir i conservar de manera estrictament confidencial tota informació de les persones usuàries dels serveis de XERA.
- L'ús de la informació és restringit i únicament d'ús professional, no podent-se transmetre a persones no habilitades.
- Complir amb l'obligació de confidencialitat després de l'extinció de la seva relació amb XERA, respecte a qualsevol informació de caràcter reservat sobre l'empresa, els seus usuaris i usuàries, socis i sòcies, empleats i empleades, clients, projectes i assumptes als quals hagués tingut accés durant la vigència de la seva col·laboració amb XERA.
- Protegir la informació confidencial, establint mesures de control que garanteixin i impedeixin l'accés no autoritzat, incloent-hi la simple visualització.
- No transferir la informació sobre les persones usuàries de XERA a tercers, per qualsevol mitjà, excepte a les persones o entitats degudament autoritzades per raó del seu càrrec o competències.

Signatura i segell del/la responsable de la gestió de les dades personals