Autoritat Catalana de Protecció de Dades

Política de protecció de dades

Generalitat de Catalunya

Índex de continguts

1. Objecte, norma, abast, rols i responsabilitats

1.1. Objecte

L'objecte d'aquest document és definir la política de protecció de dades de l'Autoritat Catalana de Protecció de Dades (APDCAT) en el marc dels sistemes d'informació i les activitats de tractament de dades personals que duu a terme l'APDCAT.

1.2. Legislació

El marc regulador en el qual es desenvolupen les activitats de l'APDCAT es caracteritza per la normativa i legislació vigent que és d'aplicació.

1.3. Abast

És d'aplicació a tota la documentació i les activitats del sistema de gestió. Els usuaris d'aquest document són el personal de l'APDCAT, així com el personal extern amb qui es relaciona quan sigui d'aplicació. Està subjecte a revisió, aprovació, distribució, derogació i destrucció, seguint els procediments corresponents.

1.4. Rols i responsabilitats

S'han creat rols o perfils de seguretat del sistema i s'han designat els càrrecs o òrgans que els ocuparan, de la manera següent:

- Responsable/s d'informació.
- Responsable/s del servei.
- Responsable de seguretat.
- Comitè responsable del sistema.
- Responsable de contactes amb proveïdors.

2. Guies i marcs normatius

Les guies que afecten els controls determinats per l'ENS i la ISO27001 estan recollides al document de la declaració d'aplicabilitat del sistema**.**

Tot i això, atès que pel seu caràcter canviant el Centro Criptológico Nacional – Computer Emercengy Response Team (Equipo de Respuesta ante Emergencias Informáticas), en endavant CCN-CERT, les actualitza constantment, disposem de l'enllaç següent per consultar-ne l'última versió vigent: Guies CCN-CERT (per a consulta).

El marc normatiu per a les referències que s'han tingut en compte per redactar aquesta normativa és el següent:

- ISO 27001, en el seu domini "A5.1 Polítiques per la seguretat de la informació" i "A5.12 Classificació de la informació".

3. Aprovació i entrada en vigor

Text aprovat el dia 5 de juny de 2025 per resolució de l'Autoritat Catalana de Protecció de Dades (APDCAT).

Aquesta política és efectiva a partir de la data d'aprovació i fins que sigui reemplaçada per una nova política aprovada per la Direcció de l'APDCAT.

4. Objecte i àmbit d'aplicació

L'objecte d'aquest document és definir la política de protecció de dades, en el marc dels sistemes d'informació i les activitats de tractament de dades personals dutes a terme per l'APDCAT, d'acord amb el següent:

- És aplicable a tots els sistemes d'informació i totes les activitats de tractament de dades personals dels quals sigui responsable l'APDCAT, amb independència del suport en què es tractin.
- És de compliment obligat per a tots els empleats públics que presten serveis a totes les àrees i unitats en què s'organitza l'APDCAT. També l'han de complir la resta de tercers que accedeixin a la informació de la qual és responsable l'APDCAT, ja sigui en virtut d'una relació contractual o d'un altre acte jurídic conforme a dret.
- Estableix les bases per determinar el conjunt de mesures tècniques i organitzatives adequades per garantir que es compleix la normativa aplicable al tractament de les dades personals i a la seguretat de la informació.

5. Missió i funcions de l'APDCAT

D'acord amb el que estableix l'article 1 de la Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, l'APDCAT és l'organisme independent que té per objecte garantir, en l'àmbit de les competències de la Generalitat, els drets a la protecció de dades personals i d'accés a la informació que hi està vinculada.

L'àmbit d'actuació de l'Autoritat Catalana de Protecció de Dades comprèn els tractaments que duen a terme:

- Les institucions públiques.
- L'Administració de la Generalitat.
- Els ens locals.
- Les entitats autònomes, els consorcis i les altres entitats de dret públic vinculades a l'Administració de la Generalitat o als ens locals, o que en depenen.
- Les entitats de dret privat que compleixen, com a mínim, un dels tres requisits següents amb relació a la Generalitat, als ens locals o als ens que en depenen:
  - El seu capital pertany majoritàriament als ens públics esmentats.

  - Els seus ingressos pressupostaris provenen majoritàriament dels ens públics esmentats.
  - En els seus òrgans directius, els membres designats per aquests ens públics són majoria.

- Les altres entitats de dret privat que presten serveis públics per mitjà de qualsevol forma de gestió directa o indirecta, si es tracta de tractaments vinculats a la prestació d'aquests serveis.

- Les universitats públiques i privades que integren el sistema universitari català, i els ens que en depenen.

- Les persones físiques o jurídiques que compleixen funcions públiques amb relació a matèries que són competència de la Generalitat o dels ens locals, si es tracta de tractaments destinats a exercir aquestes funcions i el tractament es duu a terme a Catalunya.

- Les corporacions de dret públic que compleixen les seves funcions exclusivament en l'àmbit territorial de Catalunya.

6. Definicions

Dins el seu àmbit competencial, correspon a l'APDCAT desenvolupar el conjunt de funcions regulades a l'article 57 de l'RGPD, així com a l'article 5 de la Llei 32/2010.

Als efectes d'aquesta política, s'entén per:

a) **Dades personals**: qualsevol informació sobre una persona física identificada o identificable (l'interessat). S'ha de considerar persona física identificable qualsevol persona la identitat de la qual es pot determinar, directament o indirectament, en particular mitjançant un identificador, com per exemple un nom, un número d'identificació, dades de localització, un identificador en línia o un o diversos elements propis de la identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social d'aquesta persona.

b) **Tractament**: qualsevol operació o conjunt d'operacions realitzades sobre dades personals o conjunts de dades personals, ja sigui per procediments automatitzats o no, com la recollida, el registre, l'organització, l'estructuració, la conservació, l'adaptació o la modificació, l'extracció, la consulta, la utilització, la comunicació per transmissió, difusió o qualsevol altra forma d'habilitació d'accés, acarament o interconnexió, limitació, supressió o destrucció.

c) **Responsable del tractament**: la persona física o jurídica, autoritat pública, servei o un altre organisme que, sol o juntament amb altres, determina les finalitats i els mitjans del tractament; si el dret de la Unió o dels estats membres en determina les finalitats i els mitjans del tractament, el responsable del tractament o els criteris específics per nomenar-lo els pot establir el dret de la Unió o dels estats membres.

d) **Encarregat del tractament o encarregat**: la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme que tracta dades personals per compte del responsable del tractament.

e) **Destinatari**: la persona física o jurídica, autoritat pública, servei o qualsevol altre organisme al qual es comuniquen dades personals, tant si és un tercer com si no. Això no obstant, les autoritats públiques que poden rebre dades personals en el marc d'una investigació concreta no s'han de considerar com a destinataris, de conformitat amb el dret de la Unió o dels estats membres. El tractament d'aquestes dades efectuat per aquestes autoritats públiques és conforme a les normes en matèria de protecció de dades que són d'aplicació a les finalitats del tractament.

7. Principis

L'actuació de l'APDCAT parteix del principi de responsabilitat proactiva i l'enfocament en el risc. Assumeix que totes les accions involucrades amb la garantia efectiva de la protecció de dades i la seguretat de la informació se sustenten en el ferm compromís i suport de tots els nivells jeràrquics de l'Autoritat, representats per la Direcció de la institució. Així, l'APDCAT tracta la informació i les dades personals de manera coordinada i integrada amb la resta d'iniciatives estratègiques de l'Autoritat i d'acord amb els principis de protecció de dades, segons els quals les dades han de ser:

a) Tractades de manera lícita, lleial i transparent en relació amb l'interessat (licitud, lleialtat i transparència).

b) Recollides amb finalitats determinades, explícites i legítimes i posteriorment no s'han de tractar de manera incompatible amb aquestes finalitats. D'acord amb l'article 89, apartat 1 del Reglament General de Protecció de Dades (RGPD), el tractament posterior de les dades personals amb finalitats d'arxiu en interès públic, amb finalitats de recerca científica i històrica o amb finalitats estadístiques no es considera incompatible amb les finalitats inicials (limitació de la finalitat).

c) Adequades, pertinents i limitades al que és necessari en relació amb les finalitats per a les quals es tracten (minimització de dades).

d) Exactes i, si cal, actualitzades; s'han d'adoptar les mesures raonables perquè se suprimeixin o es rectifiquin sense dilació les dades personals que siguin inexactes pel que fa a les finalitats per a les quals es tracten ("exactitud").

e) Conservades de manera que permetin identificar els interessats durant un període no superior al necessari per a les finalitats del tractament de dades personals. Les dades personals es poden conservar durant períodes més llargs, sempre que es tractin exclusivament amb finalitats d'arxiu en interès públic, amb finalitats de recerca científica o històrica o amb finalitats estadístiques, de conformitat amb l'article 89, apartat 1 de l'RGPD. Això, sens perjudici de l'aplicació de les mesures tècniques i organitzatives adequades que imposa l'RGPD, amb la finalitat de protegir els drets i les llibertats de l'interessat ("limitació del termini de conservació").

f) Tractades de manera que se'n garanteixi una seguretat adequada, inclosa la protecció contra el tractament no autoritzat o il·lícit i contra la seva pèrdua, destrucció o dany accidental, mitjançant l'aplicació de les mesures tècniques o organitzatives adequades ("integritat i confidencialitat").

Alhora, també escau fer referència als principis de protecció de dades i seguretat des del disseny i per defecte. D'acord amb aquests principis, amb l'objectiu de complir els requisits definits a l'RGPD i garantir els drets de les persones, la protecció de dades ha de formar part de qualsevol actuació des de les primeres fases de concepció d'un projecte. En el mateix sentit, la seguretat de la informació s'ha d'aplicar des del disseny inicial dels sistemes d'informació. En aquest sentit, tots els tractaments de les dades personals s'han de dissenyar i configurar de manera que garanteixin la protecció de dades per defecte, especialment en el que fa referència a la minimització de les dades i l'accés a la informació.

També cal entendre aquests principis conjuntament amb els principis que estableix l'ENS:

a) **Seguretat integral**: la seguretat ha de tendir a preservar la confidencialitat, la integritat i la disponibilitat de la informació. La seguretat s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius relacionats amb el sistema i, llevat de casos d'urgència o necessitat, ha d'evitar qualsevol actuació puntual o tractament conjuntural.

b) **Gestió de riscos**: amb l'RGPD, l'enfocament en el risc s'ha convertit en un criteri a seguir de manera inexcusable per garantir els drets i llibertats de les persones. S'ha d'entendre en un sentit global i s'hi ha d'integrar la gestió de riscos dels sistemes d'informació, per aconseguir un únic sistema de gestió de riscos integral i coherent. L'anàlisi i la gestió de riscos són part essencial del procés de protecció de dades i de seguretat de la informació per permetre mantenir un entorn controlat i minimitzar els riscos fins a nivells acceptables. Aquests nivells s'han de reduir amb el desplegament de mesures de seguretat organitzatives i tècniques, que han d'establir un equilibri entre la naturalesa de les dades i els tractaments/serveis, l'impacte i la probabilitat dels riscos a què estiguin exposats i l'eficàcia i el cost de les mesures de seguretat.

c) **Prevenció, reacció i recuperació**: la seguretat del sistema ha de preveure'n la prevenció, detecció i correcció. Aquestes mesures són complementàries: la prevenció pretén reduir la probabilitat dels incidents de seguretat; la detecció persegueix una reacció que permeti tallar l'incident ràpidament; i la recuperació busca restaurar la informació i els serveis.

d) **Línies de defensa**: el sistema de defensa ha d'estar constituït per múltiples capes. Això permetrà guanyar temps de reacció en cas d'incident, minimitzar l'impacte dels incidents i reduir la probabilitat d'afectació total del sistema.

e) **Reavaluació periòdica:** les mesures de seguretat s'han de reavaluar i actualitzar periòdicament, per adequar-les a l'evolució dels riscos i dels sistemes de protecció.

f) **Responsabilitat diferenciada**: en els sistemes d'informació dels quals és responsable l'APDCAT s'ha d'observar el principi de responsabilitat diferenciada, de manera que les diferents responsabilitats i rols estiguin delimitats:

   - El responsable del tractament és l'APDCAT, que per mitjà de la Direcció determina les finalitats i els mitjans de tractament.
   - La persona delegada de protecció de dades informa i assessora el responsable del tractament.
   - La persona responsable de la informació determina els requisits de seguretat de la informació tractada.

- La persona responsable del servei determina els requisits de seguretat sobre els serveis prestats.
- La persona responsable de la seguretat determina les decisions a prendre per complir els requisits de seguretat.
- El comitè responsable del sistema s'encarrega del funcionament dels sistemes que gestionen la informació i presten els serveis, tant des del punt de vista del programari utilitzat com del maquinari sobre el qual funciona.

8. Registre de les activitats de tractament

L'APDCAT porta i manté actualitzat el registre de les activitats de tractament de dades personals de les quals és responsable, que inclou tota la informació a la qual es refereix l'article 30.1 de l'RGPD. Aquest registre es manté al dia i el seu inventari és accessible per mitjans electrònics.

La relació actualitzada de les activitats de tractament que duu a terme l'APDCAT està disponible a l'enllaç https://apdcat.gencat.cat/ca/autoritat/avis-proteccio-dades/.

9. Gestió de riscos i avaluació d'impacte sobre la protecció de dades

Periòdicament, cal dur a terme una anàlisi de riscos que permeti identificar i gestionar els riscos per als drets i llibertat de les persones, per minimitzar-los fins a nivells que es puguin considerar acceptables. Aquesta anàlisi s'integra en el sistema de gestió de riscos transversal de l'APDCAT i se centra en els riscos de probabilitat i gravetat variables per als drets i llibertats de les persones físiques. S'efectua 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 els riscos de probabilitat i gravetat variables per als drets i les llibertats de les persones físiques, amb l'objectiu d'aplicar les mesures tècniques i organitzatives adequades per garantir un nivell de seguretat adequat al risc. Per tant, s'efectua des d'un enfocament preventiu (anàlisi prèvia al tractament de dades personals, per aplicar les mesures tècniques i organitzatives adequades) i amb enfocament reactiu (per exemple, l'anàlisi i actualització, si s'ha patit un incident de seguretat no previst o difícilment previsible).

La gestió dels riscos comporta l'anàlisi contínua sobre el sistema d'informació, d'acord amb els principis de gestió de la seguretat basada en els riscos i en la reavaluació periòdica.

Les anàlisis de riscos són una tasca que involucra diferents actors. Els rols responsables d'executar-les són el/la responsable de la informació, el/la responsable del servei, el/la responsable del sistema i el/la responsable de seguretat, que poden delegar aquestes tasques i amb l'assessorament del delegat o de la delegada de protecció de dades.

Quan de l'anàlisi realitzada en resulti probable que el tractament comporti un alt risc per als drets i llibertats de les persones, caldrà fer també una avaluació d'impacte relativa a la protecció de les dades personals. Si l'avaluació d'impacte no és necessària, cal emetre un informe que justifiqui aquesta decisió.

10. Gestió de les violacions de seguretat

Les violacions de seguretat s'han de tramitar d'acord amb el protocol establert per a la gestió i resposta a les violacions de seguretat, en el qual s'han de preveure els requisits específics quan afectin dades de caràcter personal.

11. Revisió i auditoria

Dins el pla d'auditoria anual del sistema integrat de gestió ENS / ISO 27001, cal dur a terme una auditoria interna de protecció de dades amb l'objectiu de verificar, avaluar i valorar l'eficàcia de les mesures tècniques i organitzatives per garantir la seguretat dels tractaments i sistemes d'informació.

En tot cas, quan es facin modificacions substancials en el sistema d'informació que puguin repercutir en el compliment de les mesures de seguretat implantades, cal executar una auditoria específica i extraordinària.

El responsable de seguretat de la informació i el delegat o la delegada de protecció de dades han de revisar les auditories.

12. Estructura organitzativa

12.1. Responsable del tractament

Per mitjà de la Direcció, l'APDCAT té la condició de responsable dels tractaments de dades personals que duu a terme d'acord amb les competències que li atorga la normativa vigent.

Com a responsable del tractament, l'APDCAT determina les finalitats i els mitjans del tractament i vetlla pel compliment dels principis i obligacions que emanen de la normativa vigent de protecció de dades personals, en particular l'RGPD, l'LOPDGDD.

12.2. Delegat de protecció de dades

Correspon al responsable del tractament designar la persona que exerceix el càrrec de delegat de protecció de dades (DPD). Entre les seves funcions, d'acord amb el que estableix l'article 39 de l'RGPD, destaca la relativa a informar i assessorar de les obligacions de l'APDCAT i del seu personal, en relació amb tot el que afecta el compliment de la normativa de protecció de dades. També, té la funció de supervisar que es compleixi correctament aquesta normativa i de rebre i gestionar l'exercici dels drets a l'autodeterminació informativa, així com les consultes relatives al tractament de les dades personals efectuats per l'APDCAT.

Les persones interessades es poden posar en contacte amb el delegat de protecció de dades de l'APDCAT per exercir els drets d'accés, rectificació, supressió, oposició i limitació del tractament, així com per a qualsevol qüestió relacionada amb el tractament que l'APDCAT fa de les seves dades.

13. Obligacions del personal

Com a part dels deures que estableix la normativa relativa a la funció pública, el personal al servei de l'APDCAT té el deure de col·laborar en les actuacions d'implementació d'aquesta política.

En particular, el personal ha de conèixer i complir el que preveuen la política de protecció de dades personals i la política de seguretat de la informació, juntament amb les normes i procediments que les desenvolupen i la normativa d'ús de mitjans electrònics. Aquesta obligació també inclou col·laborar en la millora de l'aplicabilitat dels principis i obligacions que estableix la normativa sobre protecció de dades personals i seguretat de la informació, amb l'objectiu d'evitar, o si escau reduir, els riscos als quals estan exposades la informació i les dades personals de les quals l'APDCAT és responsable.

A aquest efecte, el personal ha de comunicar als òrgans responsables qualsevol proposta o suggeriment que ajudi a assolir amb més garanties els principis i obligacions a què fa referència la normativa de protecció de dades i a la confidencialitat, la integritat, la traçabilitat, l'autenticitat, la disponibilitat i la conservació de les dades, la informació i els serveis utilitzats per mitjans electrònics, en els termes als quals es refereix l'Esquema Nacional de Seguretat vigent.

14. Conscienciació i formació

Un dels pilars fonamentals de la implementació i la millora contínua de la seguretat de la informació, inclosa la protecció de dades personals, és la conscienciació i la formació del personal que participa en les operacions de tractament.

Per aquest motiu, periòdicament es desenvoluparan activitats formatives específiques orientades a conscienciar i formar el personal que presta els seus serveis a l'APDCAT. La difusió interna d'aquesta política forma part de l'activitat formativa. Es realitzaran com a mínim un cop cada any i correspon a la persona delegada de protecció de dades dur-les a terme i supervisar-les.

Cal habilitar els mitjans necessaris per informar totes les persones amb accés a la informació sobre els seus deures i obligacions, així com sobre els riscos existents en el tractament de la informació.

15. Drets a l'autodeterminació informativa

L'APDCAT ha de facilitar als interessats l'exercici dels seus drets, en virtut del que preveuen els articles 15 a 22 de l'RGPD. En resum, els interessats poden exercir els drets següents:

a) **Dret d'accés**: dret de la persona interessada a saber si el responsable del tractament tracta dades personals seves i, si és així, a accedir-hi i obtenir la informació sobre com s'estan tractant. L'interessat també té dret a obtenir una còpia gratuïta de les dades objecte del tractament.

b) **Dret de rectificació**: dret a rectificar les dades personals inexactes i que es completin les que siguin incompletes, fins i tot mitjançant una declaració addicional.

c) **Dret de supressió (dret a l'oblit)**: dret a obtenir la supressió de les dades personals ("dret a l'oblit") quan: ja no són necessàries per a la finalitat per a la qual es van recollir; es revoca el consentiment en el qual es basava el tractament; hi ha oposició al tractament; les dades s'han tractat il·lícitament; les dades s'han de suprimir per complir una obligació legal o s'han obtingut en relació amb l'oferta de serveis de la societat de la informació adreçada a menors.

Quan el/la responsable ha fet públiques les dades personals i s'han de suprimir, ha d'adoptar mesures raonables per informar de la supressió a altres responsables que estan tractant aquestes dades.

d) **Dret d'oposició**: dret a oposar-se al tractament de les dades personals quan el tractament es basa en una missió realitzada en interès públic o l'exercici de poders públics conferits a l'APDCAT, o en l'interès legítim perseguit. En aquest cas, l'oposició s'ha de fonamentar en motius relacionats amb la seva situació personal. El/la responsable del tractament ha de deixar de tractar-les, tret que acrediti motius legítims imperiosos per al tractament que prevalguin sobre els interessos, els drets i les llibertats de l'interessat, o per a la formulació, l'exercici o la defensa de reclamacions.

e) **Dret a la limitació del tractament**: dret consistent en el marcat de les dades personals conservades, amb la finalitat de limitar-ne el tractament en el futur. La limitació del tractament suposa que, a petició de la persona interessada, les seves dades personals es deixen de tractar. Situacions en què es pot sol·licitar la limitació:

- La persona interessada ha exercit els drets de rectificació o oposició i mentre el responsable determina si escau atendre la sol·licitud.
- El tractament és il·lícit, fet que determinaria l'esborrat de les dades, però l'interessat s'oposa a la supressió.
- Les dades ja no són necessàries per al tractament, fet que determinaria l'esborrat de les dades, però l'interessat s'oposa a la supressió perquè les necessita per formular, exercir o defensar reclamacions.
- Mentre dura la limitació, el responsable només pot tractar les dades afectades, més enllà de conservar-les, en els casos següents:
  - Amb el consentiment de la persona interessada.
  - Per formular, exercir o defensar reclamacions.
  - Per protegir els drets d'una altra persona física o jurídica.
  - Per raons d'interès públic importants, de la Unió o de l'estat membre corresponent.

El responsable ha de comunicar la limitació a cadascun dels destinataris, tret que sigui impossible o exigeixi esforços desproporcionats. Si l'interessat ho sol·licita, el responsable ha d'identificar els destinataris.

f) **Dret a la portabilitat de les dades**: no és d'aplicació als tractament de dades personals que duu a terme l'APDCAT.

g) **Dret a no ser objecte de decisions individuals automatitzades**: l'APDCAT no pren decisions individuals automatitzades.

Per exercir aquests drets i per a qualsevol qüestió relacionada amb el tractament que l'APDCAT fa de les dades, les persones interessades es poden posar en contacte amb el delegat o la delegada de protecció de dades de l'APDCAT.

L'exercici de drets en els tractaments de dades realitzats per l'APDCAT es pot formular des de la seva seu electrònica.

16. Desenvolupament i revisió de la política de protecció de dades

A proposta dels membres que integren l'estructura organitzativa descrita en aquesta política, la persona responsable del tractament ha de definir els procediments i les guies i instruccions necessàries per desplegar-la.

Aquesta política se sotmetrà a un procés de revisió permanent, per adaptar-se a les circumstàncies tècniques o organitzatives i evitar-ne l'obsolescència.

Autoritat Catalana de Protecció de Dades

Signat per:
Meritxell Borràs i Solé
Directora de l'Autoritat Catalana de Protecció de Dades

2025.07.10 23:14:55 +02'00'