DECRET 391/2022, DEL 28-9-2022 D'APROVACIÓ DEL REGLAMENT D'APLICACIÓ DE LA LLEI 29/2021, DEL 28 D'OCTUBRE, QUALIFICADA DE PROTECCIÓ DE DADES PERSONALS.

*(Nota: Aquest text està actualitzat d'acord amb les modificacions establertes al Decret 45/2023, del 25-1-2023, d'aprovació del Reglament de modificació del Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, del 14 de setembre del 2022.)

Decret 391/2022, del 28 de setembre del 2022

Decret 391/2022, del 28-9-2022 d'aprovació del Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

Exposició de motius

La Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals del Principat d'Andorra constitueix la base del procés d'adaptació del nostre ordenament jurídic als principis vigents en matèria de protecció de dades en l'àmbit internacional i, especialment, al marc de la Unió Europea –per exemple, el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, del 27 d'abril del 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 (RGPD).

D'acord amb l'article 5.3 de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, un dels principis rectors que regeixen la protecció de dades al nostre país és la responsabilitat proactiva dels responsables de tractament. Alhora, l'article 48.1 de la mateixa Llei disposa que l'Agència Andorrana de Protecció de Dades exerceix la seva autoritat de control sobre els tractaments de dades personals, i sobre qualsevol ús posterior d'aquestes dades, que duguin a terme al Principat d'Andorra els òrgans que constitueixen l'Administració pública, inclosos els organismes autònoms o les entitats parapúbliques, i les persones i les entitats privades que, d'acord amb el que estableix la Llei, són responsables del tractament i tenen el domicili al Principat d'Andorra o s'han constituït d'acord amb les lleis del Principat d'Andorra, així com els responsables no domiciliats al Principat que utilitzin mitjans de tractament de dades personals ubicats a Andorra. La Llei, doncs, estableix que l'Agència Andorrana de Protecció de Dades ha de supervisar els tractaments de dades personals que es duguin a terme a Andorra, però que seran els responsables del tractament els qui, en virtut de la seva responsabilitat proactiva, han de complir i estar en posició de poder demostrar que es compleixen els principis relatius a la protecció de dades.

Per tal de proporcionar seguretat jurídica a aquests responsables, aquest Decret aprova el Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, la finalitat principal del qual és establir un règim adaptat a les necessitats i peculiaritats del Principat d'Andorra i als responsables del tractament de les dades i que especifica, al mateix temps, els procediments i les obligacions concrets que es deriven dels preceptes de la mateixa Llei.

El Reglament desplega també altres conceptes previstos a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, com per

exemple el dret al testament digital, la transferència internacional de dades, l'exercici dels drets dels interessats o els tractaments amb finalitat de videovigilància.

El Reglament estableix un règim més adequat i eficient, i ho fa garantint, en tot moment, un nivell adequat de protecció de dades d'acord amb el risc i el context en què es produeixen determinats tractaments de dades, i regulant l'exercici efectiu, per part de l'Agència de Protecció de Dades, de les seves funcions de supervisió.

Aquest Reglament desenvolupa la previsió continguda en el primer punt de la disposició addicional de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

Un volta la publicació del Decret 367/2022, del 14-9-2022, d'aprovació del Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals s'han constatat diversos errors. A fi de donar compliment al principi constitucional de seguretat jurídica, promoure la claredat normativa i facilitar la consulta de la norma, s'aprova un nou text íntegre del Reglament, que substitueix l'anterior.

A proposta del ministre e Presidència, Economia i Empresa, en la sessió del 28 de setembre del 2022, el Govern aprova el Decret següent:

Article únic. Aprovació del Reglament

S'aprova el Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, que entra en vigor l'endemà de la seva publicació al Butlletí Oficial del Principat d'Andorra.

Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

Article 1. Objecte

Aquest Reglament té per objecte desplegar la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

Article 2. Àmbit d'aplicació

1. Aquest Reglament s'aplica a qualsevol tractament de dades personals totalment o parcialment automatitzat, i també al tractament no automatitzat de dades personals contingudes en un fitxer o destinades a ser-hi incloses, amb les excepcions previstes a la Llei qualificada de protecció de dades personals.

2. Aquest Reglament no s'aplica a les activitats exclusivament personals o domèstiques sense cap connexió amb l'activitat professional o comercial. L'excepció personal o domèstica és aplicable en sentit estricte a les activitats emmarcades en la vida privada o familiar. No s'inclouen en aquesta excepció les activitats particulars econòmiques que excedeixen aquest àmbit.

3. Aquest Reglament s'aplica a persones físiques i jurídiques quan es comparteixin o difonguin dades personals en plataformes digitals o xarxes socials obertes al públic, o tancades però amb accés a un alt nombre de contactes o bé a un nombre indeterminat de contactes.

Article 3. Definicions

A l'efecte d'aquest Reglament s'entén per:

a) Dades personals o de caràcter personal: tota informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus relativa a una persona física identificada o identificable ("persona interessada"); s'entén per persona física identificable qualsevol persona amb una identitat que

es pugui determinar, directament o indirectament, sense esforços desproporcionats, en particular mitjançant un identificador o un o diversos elements específics característics de la seva identitat física, fisiològica, genètica, psíquica, econòmica, cultural o social. A efectes d'aquest Reglament, no es considera dada de caràcter personal la que s'obté d'un tractament que comporti un mer mesurament, sense que el procés vagi acompanyat d'un registre ni una identificació dels interessats.

b) Metadades: tota informació secundària constituïda per dades que qualifiquen altres dades, que poden informar sobre la data, la ubicació des d'on s'ha demanat la dada, el moment, qui l'ha facilitat, el tipus de sensor, el seu factor de precisió, etc. Les metadades tenen la consideració de dades personals quan permeten identificar de forma directa o indirecta, sense esforços desproporcionats, una persona física.

c) Consentiment de la persona interessada: qualsevol manifestació de voluntat lliure, específica o granular, informada i inequívoca per la qual la persona accepta, mitjançant una declaració o una acció afirmativa clara, el tractament de les dades personals que l'afectin. En tot cas, el consentiment ha d'estar separat de la resta d'operacions del tractament o els termes i les condicions.

d) Elaboració de perfils: qualsevol forma de tractament automatitzat de dades personals consistent a utilitzar aquestes dades per avaluar determinats aspectes personals d'una persona física; en especial, per analitzar o predir aspectes relatius al rendiment professional, la situació econòmica, la salut, les preferències personals, els interessos, la fiabilitat, el comportament, la ubicació i els moviments d'aquesta persona, entre d'altres. Les decisions que no estan basades únicament en el tractament automatitzat, sinó que impliquen intervenció humana en alguna fase del tractament, poden incloure també l'elaboració de perfils.

e) Anonimització: procés que consisteix a eliminar tots els elements identificatius d'un conjunt de dades personals perquè ja no sigui possible identificar la persona interessada.

f) Seudonimització: tractament de dades personals que no permet atribuir-ne a una persona interessada sense utilitzar informació addicional, sempre que aquesta informació consti separadament i estigui subjecta a mesures tècniques i organitzatives destinades a garantir que les dades personals no s'atribueixen a una persona física identificada o identificable.

g) Violació de la seguretat de les dades personals: qualsevol violació de la seguretat que ocasiona, de manera accidental o il·lícita, en tot cas no autoritzada, la pèrdua, l'alteració o la divulgació de dades personals transmeses, conservades o tractades d'una altra manera, o la comunicació o l'accés no autoritzats a aquestes dades.

h) Interès vital: interès essencial per a la vida de la persona interessada.

i) Interès legítim: interès (lícit) del responsable del tractament o d'una tercera persona pel tractament de dades personals que prevalgui sobre els interessos, els drets o les llibertats fonamentals de l'interessat, tenint en compte les expectatives raonables dels interessats basades en la seva relació amb el responsable. Són exemples d'interès legítim tractaments efectuats en el marc d'una relació amb un client, quan es tracten dades personals per a finalitats de màrqueting directe, i tractaments per prevenir el frau o per garantir la seguretat de la xarxa i la informació dels seus sistemes informàtics, entre d'altres.

j) Dades biomètriques: dades personals obtingudes a partir d'un tractament tècnic específic, relatives a les

característiques físiques, fisiològiques o conductuals d'una persona física, que permeten o confirmen la identificació única d'aquesta persona, com imatges facials, dades dactiloscòpiques o patrons d'iris.

k) Dades relatives a la salut: dades personals relatives a la salut física o mental d'una persona física que revelen informació sobre el seu estat de salut, inclosa la prestació de serveis d'atenció sanitària. S'hi inclouen les dades relatives al codi d'identificació de la història clínica o la informació relativa al dopatge d'un esportista.

l) Dades economicofinanceres: dades que ofereixen informació sobre la situació econòmica o financera d'un individu. Tenen un grau de sensibilitat elevat, si bé no es consideren categories especials de dades personals.

m) Dades de menors o discapacitats: dades de col·lectius vulnerables. Tenen un grau de sensibilitat elevat, si bé no es consideren categories especials de dades personals.

n) Transferència internacional de dades: la comunicació de dades personals o la seva posada a disposició a favor d'un destinatari subjecte a la jurisdicció d'un tercer país, o quan el destinatari és una organització internacional.

o) Principi d'extraterritorialitat del tractament: aquest Reglament s'aplica a les entitats que tracten dades personals quan facin servir mitjans de tractament ubicats en territori andorrà, tant si aquestes entitats estan establertes al Principat d'Andorra com si no hi estan establertes, d'acord amb l'article 2.2 de la Llei qualificada de protecció de dades personals, i també a les entitats establertes fora del Principat d'Andorra quan les activitats del tractament tinguin per objecte el tractament de dades d'interessats andorrans o que resideixin al Principat d'Andorra o controlin el comportament d'aquests interessats.

p) Principi de responsabilitat proactiva: el responsable del tractament ha d'aplicar mesures tècniques i organitzatives apropiades per garantir i poder demostrar que el tractament és conforme amb la Llei qualificada de protecció de dades personals. Aquest principi exigeix una actitud conscient, diligent i proactiva per part de les organitzacions davant de tots els tractaments de dades personals que duguin a terme.

q) Coordinador de protecció de dades: persona física integrant del personal d'una entitat que dona assistència al delegat de protecció de dades en tasques organitzatives però que en cap cas n'assumeix funcions ni responsabilitats.

Article 4. Obligats

1. Són obligats per les disposicions d'aquest Reglament els responsables, corresponsables, encarregats de tractament i subencarregats andorrans o constituïts conforme a les lleis del Principat d'Andorra i els actors exteriors que facin servir mitjans de tractament, automatitzats o no, ubicats en territori andorrà. D'acord amb el principi d'extraterritorialitat del tractament, aquest Reglament també s'aplica al tractament de dades personals per part de responsables o encarregats de fora d'Andorra quan duguin a terme activitats de tractament relacionades amb els interessats andorrans, o que resideixin al Principat d'Andorra, o bé quan el tractament consisteixi a fer oferta de béns i serveis, inclòs el mer control del comportament, a interessats del Principat d'Andorra.

2. Els conceptes de responsable, corresponsable, encarregat del tractament, subencarregat i representant definits a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals són conceptes funcionals, ja que tenen per objectiu l'assignació de responsabilitats d'acord amb el rol real de cada part. L'estatus legal d'un actor,

doncs, es pot determinar mitjançant una norma amb rang legal i de compliment obligatori per als actors o per a les activitats reals d'aquests actors en un tractament de dades concret, més enllà de les designacions formals que puguin existir.

3. El règim de corresponsabilitat, que pot sorgir quan hi ha diversos participants en el tractament, es regeix per les condicions generals següents:

a) Els corresponsables determinen de forma conjunta la finalitat i els mitjans de tractament. Els criteris principals per determinar la corresponsabilitat són la participació conjunta de dos o més entitats en la determinació de finalitats i mitjans d'un o diversos tractaments i la impossibilitat del tractament sense la participació de l'altre o els altres corresponsables.

b) Si una activitat de tractament, una finalitat o un mitjà de tractament és determinat unilateralment per un dels corresponsables, s'entén que aquest darrer és el responsable únic d'aquell tractament de dades.

c) Quan hi ha corresponsabilitat, els corresponsables han de formalitzar transparentment i per escrit les funcions de cadascun i la seva relació amb els interessats. No obstant això, s'entén que el règim de responsabilitat és solidari davant els interessats, i per tant els interessats poden adreçar-se a i en contra de qualsevol dels responsables per exercir els seus drets.

d) En cas de vulneració de la normativa de protecció de dades, tots els corresponsables responen pels danys que hagin pogut ocasionar, independentment de les accions de repetició que es puguin exercir posteriorment entre corresponsables.

e) La distribució de les responsabilitats respectives entre corresponsables ha de determinar l'exercici dels drets dels interessats, el compliment del deure d'informació, l'aplicació de mesures de seguretat, la notificació de violacions de seguretat i les avaluacions d'impacte relatives a protecció de dades, entre altres aspectes.

f) En circumstàncies concretes determinades, com en el marc dels assajos clínics i altres investigacions clíniques, hi pot haver responsables independents dels seus tractaments respectius. En aquests casos correspon a cada responsable respondre per les obligacions derivades de la seva activitat, de manera que no es pot apreciar la responsabilitat solidària entre ells pels incompliments que hagi pogut cometre l'altra part o les altres parts.

4. Sense perjudici del que estableix l'article 15 d'aquest Reglament, es consideren encarregats de tractament les entitats de qualsevol naturalesa o les persones físiques que processin dades personals en nom del responsable del tractament. La qualificació d'encarregat de tractament depèn de dos condicions bàsiques: que sigui una entitat separada del responsable del tractament i que tracti dades personals en nom del responsable del tractament. D'acord amb la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, un responsable del tractament només ha d'utilitzar encarregats del tractament que proporcionin les garanties suficients per implementar adequadament mesures tècniques i organitzatives perquè el tractament compleixi els requisits de la normativa andorrana de protecció de dades. El grau de suficiència de les garanties depèn d'una anàlisi de risc del responsable que constati, entre altres aspectes, el coneixement expert de l'encarregat, la seva fiabilitat, els recursos de l'encarregat o la seva adhesió a un codi de conducta o mecanisme de certificació aprovat per Andorra que tingui validesa general dins d'Andorra. L'obligació del responsable d'escollir encarregats amb garanties suficients es manté durant tot el tractament, fet que requereix

mecanismes adequats per comprovar la vigència de les garanties demostrades.

5. D'acord amb les obligacions contingudes a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, i sense perjudici del que estableix l'article 16 d'aquest Reglament, els responsables o encarregats de tractament no domiciliats a Andorra o no constituïts conforme a les lleis del Principat però que facin servir mitjans de tractament, automatitzats o no, ubicats en territori andorrà, han de designar un representant prop de l'Agència Andorrana de Protecció de Dades establert al Principat d'Andorra, d'acord amb els criteris següents:

a) El representant pot ser una persona física o jurídica que pugui actuar en nom i representació del responsable.

b) El representant s'ha de designar tenint en compte les seves qualitats professionals i, especialment, els coneixements especialitzats en dret i la pràctica en matèria de protecció de dades. Alternativament, el representant pot no disposar d'aquests coneixements sempre que disposi d'un delegat de protecció de dades ja notificat davant l'Agència Andorrana de Protecció de Dades.

c) La designació s'ha de notificar a l'Agència Andorrana de Protecció de Dades de forma telemàtica mitjançant els formularis específics, i cal adjuntar-hi el contracte de representació i la documentació que permeti identificar el representant (passaport andorrà o targeta de registre del Registre de Societats Mercantils).

d) El responsable ha de mantenir actualitzada la informació sobre el representant davant l'Agència Andorrana de Protecció de Dades.

Article 5. Persona interessada

1. L'exercici dels drets continguts a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals és personalíssim, és a dir, correspon només a les persones interessades titulars de les dades o a un representant acreditat expressament i degudament. En el cas de menors de 16 anys o persones amb discapacitat, els drets els exerceixen els seus representants legals degudament acreditats.

2. Quan hi hagi dubtes raonables sobre la identitat de la persona que vol exercir els drets esmentats a l'article anterior, l'Agència Andorrana de Protecció de Dades pot instar la persona interessada a presentar el document oficial d'identitat. La signatura electrònica es pot utilitzar en lloc del document identificatiu com a mitjà per acreditar la identitat.

3. L'acreditació dels representants s'ha de fer mitjançant documents o instruments jurídics que identifiquin correctament la persona interessada i el representant i especifiquin l'encàrrec o el procediment per al qual es delega la representació.

4. Les accions i la legitimació activa per ser part en els procediments iniciats per l'Agència Andorrana de Protecció de Dades i en els procediments judicials que se'n puguin derivar són les que estableix el Codi de Procediment Civil vigent. A més, s'admet la representació feta per associacions i organitzacions constituïdes legalment que disposin del consentiment dels interessats per representar-los, sempre que aquestes associacions i organitzacions demostrin la seva representativitat del sector.

Article 6. Dret al testament digital *

1. L'accés a continguts gestionats per prestadors de serveis de la societat de la informació sobre persones difuntes es regeix per les regles següents:

a) Es reconeix a qualsevol persona el dret a preveure un règim de gestió i abast de les seves voluntats

digitals perquè en cas de pèrdua sobrevinguda de la seva capacitat, o en cas de mort, els seus hereus, o les persones o institucions designades expressament, actuïn davant dels prestadors de serveis digitals en els quals l'interessat tingui comptes actius, amb la finalitat de gestionar-los, donar-los instruccions sobre l'ús i la destinació de la informació o, fins i tot, demanar el tancament del compte i/o la supressió de les dades personals.

Els prestadors de serveis o el responsable del servei de contingut digital als quals es comuniqui la pretensió del causant han d'executar la sol·licitud sense dilacions.

b) El dret al testament digital comprèn el dret a preveure expressament la prohibició d'accés a continguts digitals, de manera total o parcial, a determinades persones mencionades expressament pel causant. Aquesta prohibició no afecta el dret dels hereus a accedir als continguts que puguin formar part del relicte.

c) En cas de difunts menors d'edat, aquestes facultats les poden exercir també els seus representants legals o, en el marc de les seves competències, el Ministeri Fiscal, que pot actuar d'ofici o a instància de qualsevol persona física o jurídica interessada.

d) En cas de mort de persones amb discapacitat, aquestes facultats les poden exercir també, a més de les persones esmentades a la lletra anterior, els tutors o els curadors i altres encàrrecs judicials o extrajudicials que supleixin o completin la capacitat d'altri, si aquestes facultats s'entenen compreses en les mesures de suport prestades per la persona designada.

2. Les voluntats digitals es poden ordenar per mitjà de testament, codicil o memòries testamentàries.

3. Les persones legitimades poden decidir sobre el manteniment o l'eliminació de perfils de persones difuntes, conforme a les indicacions del causant o, si no n'hi ha, conforme al seu bon criteri.

4. Si el causant no ha establert expressament l'accés de la persona legitimada per dur a terme la modificació o la supressió de les dades, la persona legitimada ha d'executar o dur a terme la petició del difunt sense tenir accés a comptes o arxius digitals, llevat que obtingui autorització judicial per fer-ho.

Article 7. (Suprimit) *

Article 8. Consentiment

1. D'acord amb l'article 7 de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, el consentiment ha de ser lliure, específic, informat i inequívoc, i s'ha de donar mitjançant un acte o una declaració afirmatius.

a) S'entén que el consentiment s'ha atorgat lliurement quan l'interessat ha disposat d'una elecció real i no condicionada a patir un perjudici si no s'atorgués.

b) El consentiment s'ha de vincular a una o a cadascuna de les finalitats especificades. Si el consentiment ha de legitimar el tractament de categories especials de dades personals, la informació de l'interessat hi ha de fer referència expressa.

c) Els mecanismes posats a disposició de l'interessat per part del responsable de retirar el consentiment han de ser tan intuïtius i accessibles com els que facilita per obtenir el consentiment.

d) El consentiment no pot ser implícit o tàcit, i s'ha de fer mitjançant una declaració o una acció activa. El silenci o la inacció de l'interessat no es poden considerar eines vàlides per atorgar el consentiment.

e) Tan sols és vàlid el consentiment que es pot revocar o denegar, de forma gratuïta, sense patir perjudicis o efectes negatius. També és vàlid el consentiment incentivat. No es considera un perjudici deixar de percebre un incentiu admissible sense que es disminueixi la prestació del servei.

f) El consentiment no pot legitimar un tractament quan sigui aplicable alguna altra base jurídica, com ara l'interès legítim, el compliment d'una obligació legal aplicable, la necessitat d'execució d'un contracte, la protecció d'interessos vitals o l'interès públic.

g) Si un responsable del tractament opta per basar el tractament o alguna part concreta o algunes parts concretes del tractament en el consentiment de l'interessat, ha d'estar preparat per respectar aquesta opció i aturar aquesta part del tractament si una persona retira el seu consentiment. El responsable no pot canviar de base legitimadora segons li convingui, sinó que ha de mantenir l'elecció original de la base jurídica.

h) El responsable ha de requerir el consentiment explícit en determinades situacions en què hi hagi un alt risc en relació amb la protecció de les dades i en què sigui adequat que hi hagi un nivell de control elevat sobre les dades personals, com ara en el cas de transferències internacionals de dades fora d'Andorra, en absència de garanties adequades, de conformitat amb l'article 45.1.a de la Llei qualificada de protecció de dades personals, o bé si el tractament inclou decisions individuals automatitzades, inclosa l'elaboració de perfils.

2. Les característiques i les condicions establertes als articles 7 i 8 de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals i en aquest article són el marc legal per redactar polítiques de privacitat de pàgines web i polítiques informatives de rastrejadors web.

Article 9. Anonimització i seudonimització

1. L'anonimització té lloc amb la dissociació definitiva i irreversible de les dades personals, sense esforços desproporcionats. L'anonimització correcta requereix implementar un procés o una tècnica que garanteixi la confidencialitat de la informació personal anonimitzada. A les dades anonimitzades no els és aplicable la normativa de protecció de dades, ja que no es consideren dades personals.

2. Quan la dissociació sigui reversible es considera seudonimització. A les dades seudonimitzades els és aplicable la normativa de protecció de dades.

Article 10. L'interès legítim

1. Perquè l'interès pugui considerar-se legítim, cal que sigui:

a) Lícit, és a dir, de conformitat amb la legislació andorrana.

b) Articulat amb la claredat suficient per permetre que la prova per examinar-lo o ponderar-lo es dugui a terme en contraposició als interessos i els drets fonamentals de l'interessat, és a dir, prou específic.

c) No especulatiu, és a dir, ha de representar un interès real i actual.

2. Poden emmarcar-se en l'interès legítim, amb caràcter enunciatiu, les situacions següents:

a) L'exercici del dret de llibertat d'expressió o informació, incloses les situacions en què s'exerceixi aquest dret als mitjans de comunicació i en les arts.

b) La prospecció convencional i altres formes de comercialització o publicitat.

c) Els missatges no comercials que no hagin estat sol·licitats, inclosos els pertanyents a campanyes

polítiques o de recaptació de fons per a organitzacions caritatives.

d) L'execució de drets reconeguts en procediments judicials, inclòs el cobrament de deutes mitjançant procediments extrajudicials.

e) La prevenció del frau, de l'ús indegut de serveis o del blanqueig de diners.

f) La supervisió dels empleats amb finalitat de seguretat o de gestió.

g) Els règims interns de denúncia d'irregularitats.

h) La seguretat física, la tecnologia de la informació i la seguretat a la xarxa.

i) El tractament amb finalitats històriques, científiques o estadístiques.

j) El tractament amb finalitats de recerca (inclosa la investigació de mercat).

3. L'interès és legítim quan el tractament es duu a terme en el marc de la relació amb un client, quan es tracten les dades personals per a finalitats de màrqueting directe, per prevenir el frau o per garantir la seguretat de la xarxa i la informació dels seus sistemes informàtics.

4. L'interès legítim no és una base jurídica idònia per a un tractament relacionat amb les categories especials de dades establertes a la Llei qualificada de protecció de dades personals.

Article 11. Transferència internacional de dades

1. Una transferència de dades personals a un estat membre de la Unió Europea, a un país de l'Espai Econòmic Europeu, a un país amb un nivell adequat de protecció d'acord amb la Comissió Europea, a un país que hagi ratificat el Conveni 108+, o bé a un tercer país declarat amb un nivell adequat per l'Agència Andorrana de Protecció de Dades, es pot fer mitjançant un instrument jurídic vinculant.

2. Es pot dur a terme una transferència internacional de dades fora dels països mencionats al punt anterior quan s'ofereixin garanties adequades.

3. En qualsevol cas, abans de fer una transferència internacional fora dels països mencionats a l'apartat 1 cal fer una anàlisi com a part del compliment del principi de responsabilitat proactiva. L'anàlisi ha d'incloure, com a mínim:

a) La comprovació d'on van les dades personals (país de destinació), i que les dades transferides són adequades i pertinents i es limiten al que és estrictament necessari en relació amb les finalitats per a les quals es transfereixen i es tracten al tercer país.

b) La verificació de l'instrument en què es basa la transferència, en particular els regulats a la Llei qualificada de protecció de dades personals. Si es transmeten dades a un tercer país amb un nivell adequat de protecció d'acord amb la Comissió Europea, o bé a un tercer país declarat amb un nivell adequat per l'Agència Andorrana de Protecció de Dades, tan sols cal verificar la vigència de la decisió d'adequació.

c) L'avaluació de si hi ha algun aspecte de la legislació o la pràctica del tercer país que pugui afectar l'eficàcia de les garanties adequades dels instruments de transferència en què es basa, en el context de la transferència específica. L'avaluació ha de centrar-se principalment en la legislació de tercers països que sigui pertinent per transferir les dades. En absència d'una legislació que reguli les circumstàncies en què les autoritats públiques poden accedir a les dades personals, s'han d'examinar altres elements pertinents i objectius, i no s'ha de confiar en factors subjectius com la probabilitat que

les autoritats públiques accedeixin a les dades de forma contrària a les normes de protecció de dades d'Andorra.

4. L'anàlisi sobre l'existència d'un nivell adequat de protecció de dades recau en el responsable o l'encarregat de tractament que pretén exportar dades, fet que té un impacte evident en les mesures que han de prendre ex ante aquests responsables, ja que, si el resultat de l'avaluació evidencia un risc que no es pot mitigar, cal adoptar mesures addicionals o complementàries. Les mesures addicionals o complementàries poden ser les següents, de manera independent o complementària, segons sigui necessari:

a) Mesures tècniques que puguin impedir o fer ineficaç l'accés de les autoritats públiques de tercers països a les dades personals, en particular amb finalitats de vigilància.

b) Mesures contractuals addicionals que puguin reforçar el nivell general de protecció de les dades, obstaculitzant, per exemple, els intents de les autoritats públiques d'accedir a les dades d'una manera no conforme amb les normes d'Andorra.

c) Mesures organitzatives, que poden consistir en polítiques internes, mètodes organitzatius i normes que els responsables i encarregats del tractament poden aplicar-se a si mateixos i imposar als importadors de dades a tercers països.

5. Si, malgrat implementar les mesures addicionals o complementàries, no s'aconsegueix mitigar el risc de la transferència internacional a un tercer país, cal formular una consulta davant l'Agència Andorrana de Protecció de Dades, que avalua la pertinència i l'efectivitat de les mesures adoptades i emet un informe favorable o desfavorable sobre les mateixes mesures i, en conseqüència, sobre la transferència internacional.

Article 12. Exercici dels drets dels interessats

1. El responsable de tractament ha d'establir dins la seva organització els protocols i els sistemes de resposta efectius per a l'exercici dels drets dels interessats. Aquests protocols han de ser coneguts per tots els membres de l'organització. Els protocols i la formació dels membres de l'organització han d'adaptar-se al tipus de dades tractades, als riscos inherents al tractament de dades efectuat i a la naturalesa de les funcions dels treballadors.

2. El cànon raonable definit a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals s'ha d'establir d'acord amb els costos administratius que s'han de satisfer i no pot suposar mai un desincentiu per a l'exercici dels drets de l'interessat. El cànon fixat pel responsable pot ser objecte de recurs davant l'Agència Andorrana de Protecció de Dades.

3. D'acord amb el que s'estableix a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, en la fase prèvia de la incoació d'un expedient administratiu, l'Agència Andorrana de Protecció de Dades pot decidir l'excepció de l'obligació de bloqueig si ho estima convenient tenint en compte l'anàlisi del cas concret.

4. La persona interessada exerceix el dret d'accés d'acord amb la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals. Quan el responsable tracti una gran quantitat de dades relatives a una mateixa persona interessada i aquesta persona exerceixi un dret d'accés genèric, sense especificar si es refereix a totes o a una part de les dades, el responsable li pot demanar, abans de facilitar la informació, que especifiqui les dades o les activitats de tractament a què fa referència la sol·licitud.

5. El dret d'accés s'entén atorgat si el responsable del tractament facilita a l'interessat un sistema d'accés remot, directe i segur a les dades personals que garanteixi de manera permanent l'accés a la totalitat de les dades. A aquest efecte, amb la comunicació del responsable a l'interessat sobre la manera com pot accedir al sistema n'hi ha prou per considerar atesa la sol·licitud d'exercici del dret.

Article 13. Tractaments amb finalitat de videovigilància

1. Les persones físiques o jurídiques, públiques o privades, poden dur a terme el tractament d'imatges mitjançant sistemes de càmeres o càmeres de vídeo amb la finalitat de preservar la seguretat de les persones i els béns, i també de les seves instal·lacions, en els termes que estableix la Llei qualificada de seguretat pública.

2. El deure d'informació establert a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals es considera complert mitjançant la col·locació d'un dispositiu informatiu en un lloc prou visible en què consti, almenys, l'existència del tractament, la identitat del responsable i la possibilitat d'exercir els drets regulats a la mateixa Llei. També es pot incloure al dispositiu informatiu un codi de connexió o una adreça d'Internet amb aquesta informació. En tot cas, el responsable del tractament ha de mantenir a disposició dels interessats la informació relativa al dret de transparència de la informació.

3. A l'empara de l'article 2.4 de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, es considera exclòs de l'àmbit d'aplicació d'aquest Reglament el tractament que faci una persona física d'imatges que només captin l'interior del seu domicili. També en queda exclosa la captació d'imatges amb sistemes de videoporter, sempre que s'activin només durant el període necessari per identificar les persones que volen accedir a l'immoble i no s'enregistrin les imatges, o bé la instal·lació de càmeres falses que no siguin aptes per captar imatges.

4. Només es pot fer un tractament amb sistemes de videovigilància d'acord amb el principi de minimització de les dades de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, és a dir, si la finalitat del tractament no es pot aconseguir raonablement amb altres mitjans que siguin menys intrusius per als drets i les llibertats fonamentals de l'interessat.

5. La utilització de la videovigilància, inclosa la funció de reconeixement biomètric instal·lada per entitats privades per a les seves finalitats pròpies (p. ex. màrqueting, estadístiques o fins i tot seguretat), requereix el consentiment explícit de tots els interessats, de conformitat amb l'article 9.2.a de la Llei 29/2021 del 28 d'octubre, qualificada de protecció de dades personals; no obstant això, també es pot aplicar una altra excepció de l'article 9.2, si escau.

6. Si l'interessat, mitjançant un dret d'accés, vol rebre una còpia del material audiovisual captat per les càmeres de videovigilància, cal que el responsable eviti afectar negativament els drets i les llibertats d'altres interessats sobre el material. Per evitar aquest efecte, el responsable del tractament, com a norma general, ha d'aplicar mesures tècniques per complir la sol·licitud d'accés; per exemple, editant les imatges amb emmascarament o codificació.

Article 14. Protecció de dades des del disseny i per defecte (privacy by design i by default)

1. La privacitat des del disseny és la que obliga a fer un enfocament metodològic orientat a la gestió del risc i de responsabilitat proactiva que permeti fixar ex

ante els requisits de privacitat que tot tractament de dades ha de complir. La implementació eficaç i eficient dels principis de privacitat exigeix que aquests requisits formin part integral de la naturalesa dels tractaments, els productes i els serveis, i per això s'han de tenir en compte des de la fase inicial de concepció, disseny i desenvolupament dels tractaments, els productes i els serveis com una part més del conjunt de les especificacions, funcionals i no funcionals.

2. A partir de l'anàlisi de risc en la fase de concepció, s'han d'establir tant els objectius específics de protecció de dades com els objectius de seguretat des de la perspectiva de la privacitat que garanteixin els principis bàsics de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals. Aquests objectius han de concretar-se en el disseny d'estratègies de privacitat que identifiquin els requisits de cada objectiu.

3. La configuració per defecte, que ha de garantir que només es tracten les dades personals necessàries per a cada finalitat del tractament, ha de quedar establerta des del disseny de manera que resulti tan respectuosa com sigui possible en termes de privacitat. Si l'interessat no fa cap acció de configuració, la seva privacitat ha d'estar garantida des de l'inici, ja que ha d'estar integrada al sistema i configurada per defecte. En qualsevol cas, cal:

a) Fixar criteris de recollida limitats a la finalitat que persegueix el tractament.

b) Limitar l'ús de les dades personals a les finalitats per a les quals han estat recollides i assegurar-se que hi ha una base legitimadora del tractament.

c) Restringir els accessos a les dades personals a les parts implicades en els tractaments, d'acord amb el principi de need to know (o «necessitat de saber») i segons la funció que facin mitjançant la creació de perfils d'accés diferenciats.

d) Definir terminis estrictes de conservació i establir mecanismes operatius que en garanteixin el compliment.

e) Crear barreres tecnològiques i procedimentals que impedeixin la vinculació no autoritzada de fonts de dades independents.

4. En la fase de disseny els objectius identificats en la fase de concepció s'han de desenvolupar i integrar mitjançant decisions de disseny que regulin procediments d'implementació efectiva i problemes comuns, repetibles i previsibles, i identifiquin i esmenin vulnerabilitats potencials del sistema. Les mesures tècniques i organitzatives de la fase de disseny es consideren ben implementades en termes de seguretat si aconsegueixen garantir:

a) La confidencialitat, perquè eviten els accessos no autoritzats als sistemes.

b) La integritat, perquè protegeixen les dades de modificacions o alteracions no autoritzades de la informació.

c) La disponibilitat, perquè garanteixen que les dades i els sistemes estan disponibles quan sigui necessari.

5. En la fase de desenvolupament s'han d'aplicar de manera concreta els patrons i s'ha de confirmar que els requisits de privacitat definits han estat implementats correctament i satisfan les expectatives i les necessitats de les parts interessades (verificació i validació de la privacitat).

6. Els responsables del tractament s'han de mantenir al dia dels avenços tecnològics relacionats amb el tractament, dels riscos i les oportunitats de la tecnologia, i de les mesures i les garanties aplicables tenint en compte l'evolució del panorama tecnològic.

7. Els usuaris tenen un paper actiu en la gestió i el control de la gestió de les seves dades. Per implementar configuracions per defecte robustes, el responsable del tractament ha d'informar els usuaris sobre les conseqüències que té la modificació dels paràmetres del servei prestat en la seva privadesa.

Article 15. Encarregat del tractament

1. La regulació de la relació entre el responsable i l'encarregat del tractament s'ha d'establir mitjançant un contracte que els vinculi jurídicament i defineixi la posició de l'encarregat del tractament. El contracte o l'acte jurídic ha de constar per escrit i pot ser en format electrònic.

2. D'acord amb la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, el contracte ha d'establir l'objecte, la durada, la naturalesa i la finalitat del tractament, el tipus de dades personals i les categories d'interessats, i les obligacions i els drets del responsable.

3. L'encàrrec ha de descriure de manera clara i concreta, amb instruccions precises, els tractaments de dades que ha de dur a terme l'encarregat del tractament, el tipus de servei i la manera de prestar-lo. Ha de determinar de forma clara les comunicacions a tercers que el responsable encomana a l'encarregat o que es deriven del servei prestat. La subjecció a les instruccions del responsable s'ha de produir, igualment, en el cas de les transferències internacionals de dades que tenen lloc com a conseqüència de la prestació del servei.

4. El responsable té una obligació especial de diligència en l'elecció i la supervisió de l'encarregat i no es pot limitar a una llista en què es marca si s'aplica o no una mesura. La diligència del responsable s'entén assolida amb l'acreditació d'una anàlisi o una valoració real de les mesures de seguretat.

5. 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, el responsable i l'encarregat del tractament han d'aplicar les mesures tècniques i organitzatives apropiades per garantir el nivell de seguretat adequat al risc existent. Les mesures de seguretat concretes es poden determinar amb una llista exhaustiva o amb una remissió a un estàndard o marc regulador reconegut. L'adhesió a codis de conducta o la possessió d'un certificat són elements que serveixen per demostrar el compliment d'aquests requisits.

6. El responsable i l'encarregat del tractament han de prendre mesures per garantir que qualsevol persona que actua sota la seva autoritat i té accés a dades personals només pot tractar aquestes dades seguint instruccions del responsable, tret que hi estigui obligada en virtut d'una norma legal.

7. El règim de subcontractació es pot establir en el contracte i es fonamenta en qualsevol cas en l'autorització prèvia del responsable del tractament. Aquesta autorització pot ser genèrica o específica, que identifiqui l'entitat concreta. Si l'autorització és de caràcter general, l'encarregat ha d'informar el responsable de la incorporació d'un subencarregat o de la substitució per altres subencarregats; d'aquesta manera, dona al responsable l'oportunitat d'oposar-se a aquests canvis. El subencarregat del tractament ha d'estar subjecte a les mateixes condicions i a les mateixes formalitats que l'encarregat del tractament, en relació amb el tractament adequat de les dades personals i la garantia dels drets de les persones afectades. Si el subencarregat les incompleix, l'encarregat inicial continua sent plenament responsable del compliment de les obligacions del

subencarregat davant del responsable del tractament.

8. Si una part o la totalitat de l'encàrrec es basa en la recollida de dades, correspon a l'encarregat del tractament complir amb el dret d'informació de les persones afectades en nom i per compte del responsable. El contracte de l'encarregat del tractament ha de fixar la forma i el moment en què s'ha de fer efectiva aquesta obligació.

9. Si una part o la totalitat de l'encàrrec es basa en les obligacions relatives a l'avaluació d'impacte, la consulta prèvia, la seguretat i confidencialitat del tractament o la notificació i comunicació d'una violació de seguretat de les dades personals a l'autoritat de control o a la persona interessada, el compliment d'aquestes obligacions queda supeditat a la naturalesa del tractament efectuat i a la informació que estigui a disposició de l'encarregat.

10. Quan s'apliqui la legislació de contractes del sector públic, també cal tenir en compte les disposicions específiques establertes en aquest Reglament.

11. El principi d'extraterritorialitat permet aplicar les obligacions d'aquest Reglament a encarregats del tractament que tractin dades personals en el context de les activitats d'un establiment de l'encarregat a Andorra, independentment que el tractament tingui lloc a Andorra o en un altre país. Si l'establiment es troba fora del territori andorrà, s'aplica el Reglament sempre que ofereixi béns o serveis a interessats que resideixin a Andorra, o bé controlin el comportament d'interessats que resideixin en territori andorrà. La transmissió de dades personals en el marc d'un acord d'encarregat del tractament a l'estranger es regeix per la regulació establerta a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals per a les transferències internacionals.

Article 16. Representant dels responsables o encarregats del tractament no domiciliats al Principat o no constituïts conforme a les lleis del Principat d'Andorra

1. El representant d'un responsable o encarregat del tractament no domiciliat al Principat o no constituït conforme a les lleis del Principat d'Andorra ha de ser designat expressament per mandat escrit del responsable del tractament o de l'encarregat, perquè actuï en nom seu respecte a les obligacions que li corresponen d'acord amb la normativa andorrana de protecció de dades. La designació del representant esmentat no afecta la responsabilitat del responsable o de l'encarregat en virtut de la Llei 29/2021 del 28 d'octubre, qualificada de protecció de dades personals i d'aquest Reglament ni la capacitat dels interessats d'exercir accions contra el responsable o l'encarregat.

2. El representant pot ser tant una persona física com una persona jurídica. En qualsevol cas, el mandat per escrit ha de designar un individu concret com a destinatari últim del mandat. Es prohibeix expressament que el representant pugui ser designat també com a delegat de protecció de dades, ja que no pot assumir les dos responsabilitats.

3. El representant ha d'exercir les seves funcions conforme al mandat rebut del responsable o de l'encarregat. En cas d'incompliment, el responsable o l'encarregat són competents per aplicar mesures coercitives al representant designat.

4. El mandat per escrit ha d'estipular, com a mínim, que el representant:

a) Actua en nom del responsable o de l'encarregat del tractament;

b) Pot atendre consultes dels interessats o de les autoritats de control juntament amb el responsable o l'encarregat, o en nom seu, i

c) Pot rebre i/o atendre o no els exercicis de drets dels interessats.

5. La designació del representant s'inclou en el contingut del deure d'informació. A més, el representant està obligat a portar un registre de les activitats de tractament i ha de col·laborar estretament amb l'encarregat o el responsable.

6. Mitjançant el formulari corresponent, el responsable o l'encarregat del tractament ha de comunicar a l'Agència Andorrana de Protecció de Dades la identitat del representant andorrà i dels seus substituts o els cessaments que es produeixin. És obligació del responsable o de l'encarregat del tractament mantenir aquesta informació actualitzada.

7. De conformitat amb el que estableix la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, es considera tractament ocasional, i, per tant, exempt de l'obligació de designar un representant, el tractament limitat en el temps o en nombre d'afectats. Perquè un tractament tingui la consideració d'ocasional el nombre d'afectats a Andorra no pot ser en cap cas superior a un terç del nombre d'interessats totals d'un tractament.

Article 17. Avaluació d'impacte

1. Quan sigui probable que un tipus de tractament, especialment si utilitza noves tecnologies, i tenint en compte la seva naturalesa, l'abast, el context o les finalitats, pugui comportar un alt risc per als drets i les llibertats de les persones físiques, abans del tractament el responsable, ja sigui públic o privat, ha d'avaluar l'impacte de les operacions de tractament en la protecció de dades personals. En el cas d'una operació de tractament que ja està en marxa, s'ha de fer una avaluació d'impacte tan aviat com es detecti un risc greu per als drets i les llibertats de les persones.

2. L'avaluació d'impacte no és una tasca puntual, sinó que cal actualitzar-la periòdicament.

3. Un tractament comporta un risc alt o bé quan es produeixen les tres situacions especificades a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals o bé quan dos o més dels criteris següents apareixen en una operació de tractament:

a) L'avaluació o puntuació dels interessats, inclosa l'elaboració de perfils.

b) La presa de decisions automatitzades amb efectes jurídics significatius per a les persones físiques o que les afectin significativament de manera similar.

c) L'observació sistemàtica d'interessats.

d) Dades sensibles (especialment protegides).

e) Un tractament de dades a gran escala.

f) L'associació o la combinació de conjunts de dades.

g) Dades relatives a interessats vulnerables, com ara menors, empleats o grups més vulnerables de la població que necessiten una protecció especial.

h) L'ús innovador o l'aplicació de noves solucions tecnològiques o organitzatives.

i) El tractament impedeix als interessats exercir un dret, utilitzar un servei o executar un contracte.

j) Tractaments de dades economicofinanceres per part d'entitats bancàries o establiments financers.

4. El delegat de protecció de dades pot suggerir en qualsevol moment la realització d'una avaluació d'impacte i, en cas de dubte, s'ha de pronunciar sobre si aquesta avaluació és necessària o no ho és.

5. El concepte de gran escala establert a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals depèn dels criteris següents:

a) El nombre de persones afectades, ja sigui en termes absoluts o com a proporció d'una població determinada.

b) El volum i la varietat de dades tractades. En qualsevol cas, el tractament de dades personals de més de cinc mil afectats implica la consideració de tractament a gran escala.

c) La durada o la permanència de l'activitat de tractament.

d) L'extensió geogràfica de l'activitat de tractament.

6. Sense perjudici dels tractaments esmentats, d'acord amb la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, l'Agència Andorrana de Protecció de Dades pot publicar en qualsevol moment una llista complementària d'activitats que requereixin una avaluació d'impacte.

7. Independentment del risc que pugui tenir una operació de tractament, no cal fer una avaluació d'impacte:

a) Si ja s'ha efectuat una avaluació d'impacte d'un altre tractament molt similar en naturalesa, abast, context i finalitats.

b) Quan el tractament està inclòs en una llista de tractaments (publicada per l'Agència Andorrana de Protecció de Dades) que no requereixen una avaluació d'impacte.

8. L'escala de riscos establerta a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals s'ha de fer tenint en compte els criteris d'impacte i de probabilitat d'amenaça. Per calcular el nivell de risc associat a un tractament de dades, el responsable del tractament ha de combinar la gravetat del possible impacte amb la probabilitat de l'amenaça, prenent sempre com a punt de vista i referència els interessats, d'acord amb la taula de valoració de riscos continguda a l'annex 1 d'aquest Reglament.

9. Quan, abans de començar un tractament, el responsable (o l'encarregat) del tractament constata que el risc de conseqüències per als drets i les llibertats de les persones és alt, ha de sotmetre a l'Agència Andorrana de Protecció de Dades la idoneïtat del tractament i les mesures que vol aplicar-hi.

10. La comunicació a l'Agència Andorrana de Protecció de Dades de les avaluacions d'impacte que suposin un alt risc establerta a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals es fa de forma telemàtica i s'hi adjunta la documentació definida a la mateixa Llei. L'Agència pot instar el responsable a aportar posteriorment qualsevol informació que consideri rellevant per donar resposta a la consulta feta.

Article 18. Mesures de seguretat i confidencialitat

1. Els responsables i encarregats del tractament tenen la responsabilitat activa de transmetre els coneixements necessaris en matèria de privacitat als seus treballadors i conscienciar tot el personal que tingui accés a dades personals de la importància de la seguretat i la confidencialitat i dels protocols interns sobre aquesta matèria. La informació s'ha d'adaptar al tipus de dades tractades, als riscos inherents al tractament de dades efectuat i a la naturalesa pròpia de les funcions del treballador.

2. El deure de confidencialitat que el responsable o l'encarregat del tractament ha d'imposar als treballadors ha de contenir, com a mínim, la informació i les obligacions següents:

a) Què s'entén per informació confidencial.

b) Els mitjans, els recursos o la informació que es posa a disposició del treballador.

c) L'obligació de secret i confidencialitat.

d) L'obligació de restituir al responsable o l'encarregat del tractament la informació confidencial a què s'ha tingut accés en ocasió de la relació laboral a la fi de la relació contractual.

e) El termini establert per les parts durant el qual l'obligació de secret i confidencialitat romandrà vigent un cop acabada la relació contractual.

f) Les conseqüències que pot tenir per al treballador l'incompliment de l'obligació de confidencialitat i secret.

Article 19. Notificació de violacions de seguretat

1. Una violació de la seguretat de les dades es produeix quan les dades personals que tracta un responsable o un encarregat del tractament pateixen un incident de seguretat que dona lloc a la violació de la confidencialitat, disponibilitat o integritat de les dades.

2. Si la violació posa en risc els drets i les llibertats d'una persona, tal com fixa la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, el responsable del tractament ho ha de notificar a l'autoritat de control tan aviat com sigui possible i, com a molt tard, 72 hores després –incloses les hores transcorregudes en caps de setmana i dies festius– que el responsable tingui constància que l'incident de seguretat ha afectat dades personals. Si la notificació no té lloc en aquest termini, s'han de justificar els motius de la dilació. L'encarregat del tractament ha de notificar cada violació de la seguretat de les dades al responsable del tractament.

3. Quan en el moment de la notificació no és possible facilitar tota la informació necessària, el responsable del tractament ha d'informar-ne de manera gradual, com més aviat millor i sense dilació.

4. D'acord amb la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, si la violació de la seguretat de les dades suposa un risc alt per a les persones afectades, aquestes persones també n'han de ser informades tan aviat com sigui raonablement possible.

5. Quan el responsable del tractament notifica una violació de seguretat a l'autoritat de control, d'acord amb la Llei 29/2021 del 28 d'octubre, qualificada de protecció de dades personals, com a mínim, ha de:

a) Descriure la naturalesa de la violació de la seguretat de les dades personals, incloent-hi, si és possible, les categories i el nombre aproximat de persones interessades afectades, i les categories i el nombre aproximat de registres de dades personals afectats.

b) Comunicar el nom i les dades de contacte del delegat de protecció de dades o d'un altre punt de contacte del qual es pot obtenir més informació.

c) Descriure les possibles conseqüències de la violació de la seguretat de les dades personals.

d) Descriure les mesures adoptades o proposades pel responsable del tractament per fer front a la violació de la seguretat de les dades personals, incloses, si escau, les mesures adoptades per mitigar-ne els possibles efectes negatius.

6. La notificació es fa amb el formulari corresponent de l'Agència Andorrana de Protecció de Dades. L'Agència pot requerir la informació addicional necessària i emetre l'ordre o la comunicació oportuns, i també establir el termini en què el responsable ha d'atendre el requeriment.

7. Si considera que no hi ha riscos per als drets i les llibertats de les persones físiques, el responsable ha de documentar qualsevol violació de la seguretat de les dades personals, inclosos els fets relacionats amb la violació de seguretat, els seus efectes i les mesures correctives adoptades, perquè l'autoritat de control pugui verificar el compliment del principi de responsabilitat proactiva.

Article 20. Tipus de violacions de seguretat

Les violacions de seguretat es classifiquen, d'acord amb els tres principis de la seguretat de la informació, de la manera següent:

a) Violació de la confidencialitat. Té lloc quan es produeix una revelació no autoritzada o accidental de les dades personals o l'accés a les dades personals.

b) Violació de la integritat. Té lloc quan es produeix una alteració no autoritzada o accidental de les dades personals.

c) Violació de la disponibilitat. Té lloc quan es produeix una pèrdua d'accés accidental o no autoritzada a les dades personals, o la destrucció de les dades personals.

Article 21. Delegat de protecció de dades

1. Correspon al responsable del tractament valorar si convé designar un sol delegat de protecció de dades o més d'un, i si ha de pertànyer o no a la seva estructura, per garantir-ne en tot moment la independència i la disponibilitat.

2 En grups empresarials o empreses de grans estructures, un sol delegat de protecció de dades pot ser suficient si és fàcilment accessible des de cada establiment.

3. Encara que hi hagi un sol delegat de protecció de dades, a l'Administració pública o a les organitzacions privades en què sigui necessari per la magnitud, l'estructura o la complexitat del tractament s'han de nomenar internament un o diversos coordinadors de protecció de dades, per donar suport a les tasques organitzatives del delegat de protecció de dades.

4. Qualsevol empresa o organització privada l'activitat principal de la qual es basi en el tractament de dades de subjectes vulnerables o en risc d'exclusió social o bé de menors de catorze anys ha de designar un delegat de protecció de dades tenint en compte la protecció específica que mereixen aquest tipus d'interessats.

5. Els responsables i encarregats del tractament han de comunicar a l'Agència Andorrana de Protecció de Dades, en el termini de deu dies, les designacions, els nomenaments i els cessaments dels delegats de protecció de dades, tant si estan obligats a designar-ne com si la designació del delegat de protecció de dades ha estat voluntària.

6. Si s'externalitza la funció, el delegat de protecció de dades té la condició d'encarregat del tractament.

Article 22. Coneixements del delegat de protecció de dades

1. L'Agència Andorrana de Protecció de Dades pot fixar o analitzar els coneixements i la capacitació suficient per ser delegat de protecció de dades en qualsevol moment.

2. Tant les persones físiques com les jurídiques poden demostrar la qualificació suficient com a delegat de protecció de dades mitjançant certificats voluntaris o títols universitaris que acreditin coneixements especialitzats en el dret i la pràctica de l'àmbit de la protecció de dades.

Article 23. L'exercici de les funcions del delegat de protecció de dades

1. El responsable del tractament o l'encarregat han de garantir que el delegat de protecció de dades

disposa del temps suficient per desenvolupar correctament les seves funcions i pot comptar amb els recursos financers, la infraestructura i el personal que siguin necessaris. També ha de garantir que el delegat de protecció de dades participa de manera adequada i en el moment oportú en totes les accions relatives a la protecció de dades personals i que té accés al nivell jeràrquic més alt.

2. Sense perjudici del que estableix la Llei 29/2021 del 28 d'octubre, qualificada de protecció de dades personals, el delegat de protecció de dades no pot exercir simultàniament altres funcions de responsabilitat o d'alta direcció dins l'organització que puguin generar un conflicte d'interès, com ara director general, director d'operacions, director financer, responsable legal, responsable de sistemes, responsable de compliment, cap de màrqueting o cap de recursos humans, entre altres càrrecs, ni tampoc altres responsabilitats inferiors que tinguin poder de decisió sobre les finalitats o els mitjans del tractament.

3. L'Agència Andorrana de Protecció de Dades posa a disposició dels responsables i els encarregats del tractament les eines telemàtiques i presencials necessàries per comunicar les designacions de delegats de protecció de dades i els canvis que es puguin produir. Les comunicacions han de contenir, com a mínim:

a) Les dades de la persona física que comunica la designació o el canvi.

b) Les dades del responsable o l'encarregat del tractament.

c) Les dades públiques de contacte del delegat de protecció de dades i, si escau, del delegat de protecció de dades de suport.

4. L'Agència Andorrana de Protecció de Dades publica al seu lloc web les dades públiques de contacte dels delegats declarats pels responsables o encarregats del tractament com a garantia jurídica dels interessats.

Article 24. Relació entre el delegat de protecció de dades i l'Agència Andorrana de Protecció de Dades

1. En compliment de la funció de cooperació amb l'autoritat de control que té atribuïda legalment, el delegat de protecció de dades li facilita l'accés als documents i la informació necessaris per dur a terme les seves funcions en l'exercici de les seves competències. L'obligació de secret i confidencialitat no suposa una incompatibilitat amb la possibilitat de consultar l'autoritat de control i contactar-hi.

2. El delegat de protecció de dades, amb ajuda d'un equip, si cal, també ha d'estar en condicions de comunicar-se eficaçment amb els interessats i cooperar amb les autoritats de control que corresponguin.

3. Abans de resoldre sobre l'admissió a tràmit d'una reclamació, l'Agència Andorrana de Protecció de Dades pot remetre-la al delegat de protecció de dades, si n'hi ha.

Article 25. Codis de conducta

1. Un codi de conducta és un instrument al qual es poden adherir responsables i encarregats del tractament i que recull les regles que ha de complir un sector d'activitats específic per aplicar adequadament la normativa sobre protecció de dades, tenint en compte les característiques i les necessitats del sector.

2. Les associacions i altres organismes que representen categories de responsables o d'encarregats del tractament poden elaborar codis de conducta, modificar-los o ampliar-los, per tal

d'especificar l'aplicació de la legislació sobre els aspectes establerts a la Llei 29/2021 del 28 d'octubre, qualificada de protecció de dades personals.

3. Aquestes associacions o organitzacions han de demostrar que són representatives del sector mitjançant, entre altres aspectes, índexs del nombre de membres representats o l'experiència de l'organització en el sector.

4. Els projectes de codis de conducta s'han de presentar a l'Agència Andorrana de Protecció de Dades de forma telemàtica mitjançant el procediment establert per l'Agència amb aquesta finalitat. Als projectes de codis de conducta s'hi ha d'adjuntar:

a) Una memòria justificativa clara i concisa, que descrigui detalladament l'objectiu del codi, el seu àmbit d'aplicació i com facilitarà l'aplicació efectiva de la normativa andorrana de protecció de dades.

b) Una memòria explicativa del govern del codi de conducta que estableixi, concretament i com a mínim, com s'organitzarà la relació entre els membres, el titular i l'òrgan regulador al llarg de la vida del codi de conducta, les condicions d'adhesió al codi de conducta, el mecanisme de sortida del codi, el procés d'actualització dels requisits del codi i els criteris de selecció de l'òrgan de control.

c) Documentació que acrediti la justificació de la legitimació del promotor.

d) Documentació que acrediti l'àmbit d'aplicació material i que especifiqui les operacions de tractament de dades personals que abasta, així com les categories de responsables o encarregats del tractament a què s'aplica.

e) Documentació que acrediti l'àmbit d'aplicació territorial.

f) Documentació que acrediti l'autoritat competent, si es tracta de codis transnacionals.

g) Documentació que estableixi els mecanismes de supervisió i l'organisme de supervisió, si escau.

h) Documentació que acrediti la consulta amb les parts interessades, o la justificació de la seva absència.

5. Per aprovar-los, l'Agència Andorrana de Protecció de Dades ha de valorar si els codis presentats:

a) Compleixen el contingut mínim disposat a la Llei 29/2021 del 28 d'octubre, qualificada de protecció de dades personals.

b) Compleixen els requisits formals de l'apartat anterior.

c) Satisfan una necessitat específica del sector o l'activitat de tractament de què es tracti.

d) Faciliten i especifiquen l'aplicació de la normativa de protecció de dades.

e) Aporten garanties suficients.

f) Disposen de mecanismes suficients per supervisar-ne el compliment.

6. D'acord amb la Llei 29/2021 del 28 d'octubre, qualificada de protecció de dades personals, la supervisió dels codis de conducta es pot confiar a un tercer la missió del qual no interfereix amb les de l'autoritat de control. Els organismes de supervisió del compliment dels codis han de ser acreditats per l'Agència Andorrana de Protecció de Dades. Els requisits generals del marc d'acreditació de l'Agència són:

a) Que tot el tractament que efectua l'òrgan supervisor com a part de les seves missions compleix la normativa andorrana de protecció de dades.

b) Que l'òrgan supervisor disposa de recursos humans, financers i materials d'acord amb l'abast del codi de conducta.

c) Que l'òrgan supervisor duu a terme les tasques previstes al codi de conducta i disposa de procediments de control regulars, complets i transparents.

d) Que l'òrgan supervisor conserva els documents relacionats amb l'exercici de les seves funcions, de manera que en preserva la confidencialitat o els destrueix de manera permanent i segura si resulten innecessaris.

e) Que l'òrgan supervisor respecta les mesures de seguretat establertes pels adherents al codi, en l'exercici de les seves funcions.

f) Que l'òrgan supervisor compleix els requisits de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

7. Les organitzacions que volen acreditar-se com a organismes supervisors de codis de conducta s'han d'adreçar primer al portador del codi per expressar el seu interès a ser identificades com a òrgan de control. En la fase d'aprovació definitiva dels codis de conducta davant l'Agència Andorrana de Protecció de Dades, li han de presentar la documentació necessària per acreditar el compliment dels requisits generals establerts en l'apartat anterior.

Article 26. Registre d'activitats de tractament

1. El Registre d'activitats de tractament (RAT) pot integrar-se en els catàlegs de processos que ja existeixin a l'entitat i formar-ne part, incloent-hi tota la informació que el responsable consideri necessària per protegir els drets i les llibertats de les persones físiques i per demostrar el compliment de la normativa tenint en compte la naturalesa, l'àmbit, el context i les finalitats del tractament, i també els possibles orígens dels riscos que aquest tractament pot suposar per als interessats.

2. El Registre d'activitats de tractament no s'ha de portar en empreses ni organitzacions que ocupin menys de cinquanta persones, llevat que hi concorri alguna de les circumstàncies següents:

a) Que sigui probable que hi hagi un risc per als drets i les llibertats dels subjectes.

b) Que el tractament no sigui ocasional.

c) Que el tractament inclogui categories especials de dades, d'acord amb la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, o infraccions i condemnes penals.

Els tractaments en què es produeixi alguna d'aquestes circumstàncies s'han d'incloure al Registre.

3. El Registre d'activitats de tractament inclou informació que facilita l'aplicació efectiva de la responsabilitat proactiva i és una eina que acredita que l'actuació del responsable del tractament és conforme a la normativa andorrana de protecció de dades. El responsable o l'encarregat del tractament i, si escau, el seu representant han de posar el Registre a disposició de l'Agència Andorrana de Protecció de Dades quan aquesta autoritat de control ho sol·liciti.

4. El Registre d'activitats de tractament també s'ha de posar a disposició de qualsevol interessat que ho sol·liciti, directament o mitjançant la seva publicació a la pàgina web del responsable o l'encarregat del tractament.

5. Si hi ha un delegat de protecció de dades designat, el responsable o l'encarregat del tractament li han de comunicar qualsevol addició, modificació o exclusió del contingut del Registre d'activitats de tractament.

6. Els subjectes enumerats a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals han de fer públic un inventari de les seves activitats de tractament, accessible per mitjans electrònics, en què consti la informació de la mateixa Llei.

Article 27. Sancions

En el cas de concórrer dos o més infraccions molt greus tipificades a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals, les sancions econòmiques poden incrementar-se fins al 2% de la facturació global anual de la companyia.

Disposició transitòria primera

S'estableix un termini de sis mesos d'adaptació per als obligats perquè adaptin els seus processos interns i desenvolupin les obligacions que s'hi regulen.

Disposició transitòria segona

Els responsables del tractament que tinguin declarats un o més fitxers al Registre públic d'inscripció de fitxers de dades personals disposen del termini de dos mesos des de la publicació d'aquest Reglament per suprimir els fitxers del registre esmentat i recollir la còpia original de l'expedient a les dependències de l'Agència Andorrana de Protecció de Dades. Passat aquest termini, l'Agència destrueix la documentació en suport paper i només en conserva una versió digitalitzada.

Disposició transitòria tercera

Els contractes d'encarregat del tractament subscrits abans del 17 de maig del 2022 d'acord amb la Llei 15/2003 mantenen la vigència fins a la data de venciment que s'hi assenyala i, en cas d'haver-se pactat de forma indefinida, fins al 17 de maig del 2024. Durant aquests terminis qualsevol de les parts pot exigir a l'altra la modificació del contracte a fi que resulti conforme al que disposa la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

Disposició derogatòria

Amb l'entrada en vigor d'aquest Decret queden derogades les disposicions de rang igual o inferior que s'hi oposin, i en concret el Decret 367/2022, del 14-9-2022, d'aprovació del Reglament d'aplicació de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

Andorra la Vella, 28 de setembre del 2022

Xavier Espot Zamora

Cap de Govern

Annex 1. Taula de valoració del risc en avaluacions d'impacte

L'escala de riscos establerta a l'article 32.10 de la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals s'ha de fer tenint en compte els criteris d'impacte i de probabilitat d'amenaça. Per calcular el nivell de risc associat a un tractament de dades, el responsable del tractament ha de combinar la gravetat del possible impacte amb la probabilitat de l'amenaça, prenent sempre com a punt de vista i referència els interessats.

Impacte	Descripció
Baix	Els interessats poden patir algunes molèsties menors, que poden reparar-se sense problemes.
Mitjà	Risc de patir inconvenients importants reparables.
Alt	Risc de patir conseqüències importants, reparables però amb moltes dificultats.
Molt alt	Risc de patir conseqüències greus

	irreparables.				
		Impacte			
		Baix	Mitjà	Alt	Molt alt
Probabilitat	Improbable	Risc baix	Risc baix	Risc mitjà	Risc alt
	Possible	Risc baix	Risc mitjà	Risc alt	Risc alt
	Probable	Risc mitjà	Risc alt	Risc alt	Risc alt

Quan, abans de començar un tractament, el responsable (o l'encarregat) del tractament constata que el risc de conseqüències per als drets i les llibertats de les persones és alt, ha de sotmetre a l'Agència Andorrana de Protecció de Dades la idoneïtat del tractament i les mesures que vol aplicar-hi.

Data de publicació en el BOPA: 05.10.2022 (núm. 118)
Data de publicació en el BOPA: 01.02.2023 (núm. 13)
www.bopa.ad