

Reglaments

Decret 170/2023, del 19 d'abril del 2023

Decret 170/2023, del 19-4-2023, d'aprovació del Reglament de videoidentificació

Exposició de motius

La Llei 35/2014, del 27 de novembre, de certificació i confiança electrònica indica a l'article 26.2 que el prestador de serveis de confiança electrònica qualificat ha de verificar de forma fefaent la identitat i, si escau, qualsevol altre atribut específic de la persona física o jurídica a la qual expedeix el certificat electrònic qualificat. Aquesta informació pot ser verificada pel prestador de serveis qualificat o per un tercer autoritzat que actuï sota la responsabilitat del prestador de serveis qualificat. En relació amb les possibilitats de verificar aquesta informació, l'apartat 2.e del mateix article indica que els sistemes de videoconferència també estaran admesos si es compleixen els requisits previstos i els que es puguin desenvolupar reglamentàriament, pel que fa als nivells de garantia necessaris.

Justament, aquest desenvolupament reglamentari es fa amb aquesta norma, la finalitat de la qual és regular la videoidentificació en la provisió de serveis dels prestadors de serveis de confiança, per habilitar i identificar de forma remota, per vídeo, els sol·licitants de certificats qualificats, en termes de seguretat jurídica dels operadors del servei i dels usuaris. Pel que fa a les mesures organitzatives procedimentals i de seguretat que és necessari implementar, es regulen de manera proporcional als riscos i són adequades a la naturalesa dels serveis.

Finalment, caldrà tenir present que aquestes previsions s'han de posar en relació amb el Decret pel qual s'aprova el Reglament de supervisió, control i servei públic de confiança electrònica, i el Decret 382/2021, pel qual s'aproven els números de referència de normes relatives a dispositius de signatura electrònica i de segell electrònic, i altres sistemes, mitjans i productes relacionats.

Aquest Reglament de videoidentificació consta de 8 articles i d'una disposició final.

A proposta del ministre de Presidència, Economia i Empresa en funcions, el Govern, en la sessió del dia 19 d'abril del 2023, aprova aquest Decret, amb el contingut següent:

Article únic

S'aprova el Reglament de videoidentificació, que entrarà en vigor l'endemà de ser publicat al *Butlletí Oficial del Principat d'Andorra*.

Reglament de videoidentificació

Article 1. *Objecte*

1. Aquest Reglament té per objecte regular les condicions i els requisits tècnics mínims aplicables a la verificació de la identitat i, si escau, altres atributs específics de la persona sol·licitant d'un certificat qualificat mitjançant mètodes de videoconferència, conforme al que disposa l'article 26.1.e de la Llei 35/2014, de 27 de novembre, de certificació i confiança electrònica (en endavant, LCCE).

2. El compliment dels requisits establerts en aquest Reglament es confirma per un organisme acreditat d'avaluació de la conformitat, conforme al que disposa el Decret de l'1 de juliol de 2015 pel qual s'aprova el Reglament de supervisió, control i servei públic de confiança electrònica.

Article 2. *Àmbit d'aplicació*

1. Aquest Reglament s'aplica:

- a) Als prestadors qualificats públics i privats de serveis electrònics de confiança establerts al Principat d'Andorra.
- b) Als prestadors qualificats residents o domiciliats a un altre Estat que tinguin un establiment permanent situat al Principat d'Andorra en els termes de l'article 2 de l'LCCE.

2. L'execució dels procediments d'identificació remota per vídeo pot ser externalitzada. En aquest cas, el prestador que expedeix el certificat qualificat manté la responsabilitat plena, en relació amb l'aplicació d'aquest Reglament.

Article 3. *Protecció de dades de caràcter personal*

Els tractaments de dades de caràcter personal de les persones físiques que es produeixin com a conseqüència de l'aplicació d'aquesta norma resten subjectes al que disposa la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals (en endavant, "LQPD"), així com la resta de la normativa sobre protecció de dades personals.

Article 4. *Modalitats admeses i documents d'identificació*

1. El procés de videoconferència es pot fer de forma assistida, amb la mediació síncrona d'un operador, o de manera no assistida, sense necessitat d'interacció en línia entre un operador i el sol·licitant, amb posterior revisió d'un operador.

2. La identitat d'un sol·licitant andorrà s'acredita mitjançant els documents d'identitat previstos a la legislació andorrana, singularment el passaport. La identitat d'un sol·licitant ciutadà de la Unió Europea i de l'Espai Econòmic Europeu s'acredita mitjançant els documents oficials d'identitat que corresponguin. La resta de sol·licitants acrediten la seva identitat mitjançant el seu passaport.

3. Els documents d'identitat utilitzats han d'incloure una fotografia i disposar de característiques de seguretat automàticament comprovables en el procés de videoconferència, de manera que es garanteixi la detecció de falsificacions i de manipulacions.

Article 5. *Requisits de procediment*

1. Cal informar el sol·licitant, de manera clara i comprensible, dels termes i de les condicions del procés d'identificació remota per vídeo, de les recomanacions de seguretat aplicables, així com del que preveu l'article 16 de l'LQPD.

2. S'ha de demanar el consentiment exprés del sol·licitant, incloent-hi el consentiment a l'enregistrament íntegre del vídeo i al tractament i conservació de categories especials de dades personals. En aquest sentit, cal informar el sol·licitant d'altres alternatives existents per a la identificació que no requereixin el tractament i la conservació de la seva imatge i de les seves dades biomètriques, incloses en tot cas les previstes a l'article 26 de l'LCCE.

3. Cal adoptar les mesures adequades que garanteixin la privadesa de tot el procés d'identificació del sol·licitant.

4. Cal verificar l'autenticitat, la vigència i la integritat física i lògica del document d'identificació utilitzat i la correspondència del titular del document amb el sol·licitant.

5. Cal adoptar mesures per reduir al mínim el risc que la identitat del sol·licitant no coincideixi amb la identitat reclamada, tenint en compte el risc de documents perduts, robats, suspesos, revocats o expirats.

6. Cal adoptar les mesures adequades per detectar una possible manipulació de la imatge de vídeo, del document d'identitat o del sol·licitant, garantint la seva prova de vida. Per això, cal implantar, com a mínim:

- a) Mesures procedimentals que facin palesa aquesta manipulació, amb la introducció d'un codi únic, aleatori i impredecible i d'un sol ús, generat a aquest efecte i tramès al sol·licitant. El codi consta d'un mínim

de sis caràcters o d'un sistema amb entropia equivalent. El prestador comprova que el dispositiu mòbil al qual es remet el codi es troba en possessió de l'usuari durant el procés d'identificació.

b) En el cas de la videoconferència assistida, mesures organitzatives que facin palesa aquesta manipulació a través de la interacció amb el document d'identitat utilitzat i amb el sol·licitant, segons les indicacions de l'operador, a través d'interaccions i actuacions físiques que figuren en un protocol que inclou accions tant comunes com aleatòries i diferenciades.

c) En cas de la videoconferència no assistida, el sistema requereix al sol·licitant la realització activa d'interaccions i actuacions físiques, les quals consten d'un protocol que inclou accions tant comunes com aleatòries i diferenciades.

7. El procés d'identificació s'interromp o no es considera vàlid quan concorri alguna de les circumstàncies següents:

a) Hi ha indicis de falsedat, manipulació o manca de validesa del document d'identificació.

b) Hi ha indicis de falta de correspondència entre el titular del document i el sol·licitant.

c) La qualitat de la imatge o el so impedeixen o dificulten verificar l'autenticitat i la integritat del document d'identificació i la correspondència entre el titular del document i el sol·licitant.

d) Les condicions, la seguretat o la qualitat de la comunicació impedeixen o dificulten completar el procés amb la fiabilitat adequada.

e) Hi ha indicis d'ús d'arxius prèviament enregistrats.

f) Hi ha indicis que per a la transmissió de vídeo no s'ha utilitzat un únic dispositiu.

g) Hi ha indicis que la transmissió de vídeo no s'ha fet en temps real o que el procés no s'ha fet en unitat d'acte.

h) Hi ha indicis que el sol·licitant està sent coaccionat o intimidat.

i) Qualsevol altra en què existeixi un dubte raonable sobre la seguretat del procés d'identificació que s'està fent.

En cas que l'operador interrompi o no consideri vàlid el procés d'identificació, s'ha d'indicar la causa deixant-ne constància fefaent al sistema.

8. Si el procés d'identificació es fa de forma assistida, el prestador ha de disposar d'un procediment per dur a terme l'entrevista d'identificació del sol·licitant del certificat i una guia de diàleg per als operadors.

9. Si el procés d'identificació es fa de manera no assistida, un operador supervisa a posteriori el procés d'identificació gravat i comprova les proves i les imatges generades pel sistema per acceptar o rebutjar la validesa del procés d'identificació.

10. L'operador de registre basa la decisió d'aprovació o denegació de la sol·licitud d'emissió del certificat en la revisió de totes les proves obtingudes en el procés d'identificació, incloent-hi, almenys, el vídeo, la comprovació de caràcters aleatoris enviats al sol·licitant, l'existència d'elements de seguretat del document d'identitat extrets durant el procés d'identificació i la comparació biomètrica efectuada.

11. En el cas de les persones físiques que actuïn a través de representant, així com de les persones jurídiques, es comproven les dades relatives a la constitució i personalitat jurídica, o a la persona o entitat representada, així com l'extensió i vigència de les facultats de representació del sol·licitant d'un certificat qualificat, d'acord amb la legislació aplicable. Aquesta comprovació es pot fer en un procés diferent de la identificació del sol·licitant, si bé en qualsevol cas s'ha de fer de forma prèvia a l'expedició del certificat.

Article 6. Requisits de personal

1. L'operador encarregat de la verificació de la identitat del sol·licitant d'un certificat qualificat mitjançant videoconferència ha de disposar de:

- a) Formació específica sobre les característiques verificables pel mètode d'identificació, els seus procediments, mètodes de prova i mètodes comuns de falsificació, per tal d'assegurar que disposa de la capacitat suficient per detectar potencials frauds en el procés d'identificació i en els documents d'identitat.
- b) Formació sobre la normativa vigent en matèria de protecció de dades personals i serveis de confiança.
- c) Formació en l'ús de l'eina i la interpretació de la informació i les dades que subministra.

2. El prestador qualificat de serveis electrònics de confiança disposa d'un pla de formació que es revisa sempre que es produeixi un canvi tecnològic o normatiu i, com a mínim, anualment quant als continguts i l'eficàcia.

La formació prevista a l'apartat anterior, la durada del qual no pot ser inferior a quinze hores, es rep de forma periòdica i com a mínim una vegada a l'any.

Article 7. Requisits de seguretat

1. Cal disposar d'un model de gestió contínua del risc que inclogui una anàlisi de riscos específica, que es revisa amb una periodicitat mínima anual i, en tot cas, sempre que es produeixi un canvi en el sistema, en els procediments organitzatius, en l'estat de la tecnologia, o en qualsevol altre aspecte que pugui influir en el perfil de risc del procediment d'identificació.

Aquesta anàlisi té en compte la naturalesa, l'àmbit, el context i les finalitats del tractament de les dades personals, així com els riscos de diversa probabilitat i gravetat per als drets i les llibertats de les persones físiques, d'acord amb el que exigeix la normativa de protecció de dades personals.

2. Cal fer una avaluació d'impacte en la protecció de dades personals quan de l'anàlisi realitzada resulti probable que el tractament suposa un alt risc per als drets i les llibertats de les persones, d'acord amb el que preveu la normativa esmentada.

3. Cal adoptar mesures tècniques i organitzatives addicionals a les indicades en aquest Reglament quan el resultat de l'anàlisi de riscos efectuada així ho requereixi. En tot cas, en relació amb les dades de caràcter personal, cal adoptar les mesures tècniques i organitzatives apropiades, segons el que estableix l'LQDP, així com a la resta de la normativa sobre protecció de dades personals.

Aquestes mesures s'actualitzen immediatament quan es tingui coneixement de vulnerabilitats que puguin donar lloc a bretxes de seguretat.

4. Cal avaluar i documentar les característiques de seguretat del conjunt del sistema, incloent-hi tots els elements substantius de la plataforma d'identificació, els canals de comunicació i la generació i conservació de proves produïdes durant el procés d'identificació.

5. Cal ubicar els servidors i l'equipament que formin part dels sistemes d'informació que suporten el procés d'identificació en llocs protegits, amb accés restringit al personal autoritzat. S'han de controlar els accessos de manera que només es pugui accedir per les entrades previstes i vigilades, i s'ha d'identificar tot el personal que accedeixi a aquestes estades, i registrar les entrades i les sortides.

Si els servidors es troben ubicats en un país tercer, cal garantir que es compleixin els requisits establerts al capítol cinquè de l'LQDP, així com a la resta de la normativa sobre protecció de dades personals.

6. Es pot emprar, indistintament, un producte d'identificació remota per vídeo que compleixi:

- a) Els requisits mínims de seguretat indicats a l'annex F.11 de la Guia de seguretat de les TIC CCNSTIC-140, del Centre Criptològic Nacional de l'Estat espanyol, de categoria alta. El prestador qualificat ha de seguir les indicacions de configuració i ús segur del producte.
- b) El conjunt de requisits per a proveïdors de serveis de verificació d'identitat remota (PVID) publicat per l'ANSSI de l'Estat francès.

7. En cas que el personal involucrat en el procés de videoconferència desenvolupi la seva activitat en la modalitat de treball a distància, cal garantir de la mateixa manera la seguretat del procés, de la informació i la protecció de dades de conformitat amb la normativa aplicable.

Article 8. *Requisits de l'enregistrament i de conservació de proves*

1. El vídeo realitzat, de forma assistida o sense assistència, s'ha d'enregistrar íntegrament i sense interrupcions.
2. S'ha de constatar de manera fefaent la data i l'hora de l'enregistrament mitjançant l'ús d'un segell qualificat de temps.
3. Es conserva una còpia de l'enregistrament del vídeo durant un període mínim de temps de quinze anys des de l'extinció de la vigència del certificat obtingut per aquest mitjà.
4. Cal conservar, per un període mínim de temps de quinze anys, fotos o captures de pantalla del sol·licitant i del document d'identitat utilitzat, en les quals seran clarament reconeixibles tant la persona com l'anvers i el revers del document d'identitat.
5. Es conserva, per un període mínim de temps de quinze anys, el resultat automàtic de la verificació efectuada per l'aplicació, així com l'avaluació i les observacions efectuades per l'operador, juntament amb la seva decisió d'aprovació o rebuig de la identificació.
6. Es conserven totes les proves dels processos d'identificació incomplets que no hagin arribat a terme per sospita d'intent de frau durant un termini de cinc anys des de l'execució del procés d'identificació, i s'especifica la causa per la qual no es van completar, de conformitat amb la política establerta a aquest efecte.
7. Cal garantir la integritat i l'autenticitat de l'enregistrament, així com de les altres proves obtingudes durant el procés d'identificació remota, mitjançant la utilització de serveis de confiança qualificats, i també la seva confidencialitat. La conservació es fa mitjançant el bloqueig de les dades, d'acord amb el que preveu l'article 30.2 de l'LQDP.
8. L'enregistrament i les imatges obtingudes durant el procés d'identificació han de reunir les condicions de qualitat i nitidesa suficients per garantir-ne l'ús en investigacions o en anàlisis posteriors.

Cosa que es fa pública per a coneixement general.

Andorra la Vella, 19 d'abril del 2023

Xavier Espot Zamora
Cap de Govern en funcions