PÍNDOLA 31.- COVID-19: CONSELLS SOBRE L'ÚS D'EINES DE VIDEOCONFERÈNCIA

El desenvolupament i l'ús de solucions tecnològiques per lluitar o per adaptar-se davant les noves circumstàncies que ha comportat la pandèmia generada pel Covid-19 han de garantir la protecció de dades des del primer moment aplicant la protecció de dades des del disseny i per defecte.

En aquest cas, les aplicacions de videoconferència es basen en la tecnologia VoIP (veu sobre IP) que permet als usuaris establir comunicacions a través del seu micròfon i/o càmera web per finalitats professionals i/o personals.

QÚESTIONS PRÈVIES

En relació amb l'àmbit professional, cal que qualsevol eina que impliqui el tractament de dades personals estigui prèviament validada per la institució i, en concret, incorporant les garanties suficients i salvaguardes contractuals corresponents.

En general, es recomana en relació amb les aplicacions utilitzades:

- Llegir les condicions d'ús del servei abans de la seva contractació i, en el seu cas, renegociar-ne els termes. L'adhesió a condicions i clàusules estàndards comporta riscos i no és una bona pràctica des de la perspectiva de protecció de dades ni de contractació pública.

- No utilitzar aplicacions que no garanteixin la confidencialitat de les comunicacions ni que utilitzin les dades amb d'altres finalitats. Disposar de contractes d'encarregat, que ofereixen les mínimes garanties i salvaguardes contractuals, és sempre clau.

IMPORTANT: Quan s'ha de fer un tractament per compte d'un responsable del tractament, s'ha d'escollir únicament un proveïdor que ofereixi garanties suficients per aplicar les mesures tècniques i organitzatives adequades, de manera que el tractament sigui conforme als requisits de la normativa de protecció de dades i garanteixi la protecció dels drets dels usuaris.

LA GRATUÏTAT APARENT

Les aplicacions de videoconferència gratuïtes o a uns costos ajustats sovint només són aparents i poden rendibilitzar el seu servei processant informació sobre els seus usuaris. Aquesta informació no està necessàriament limitada a la que s'ha proporcionat directament i es pot estendre altres dades tècniques o de diagnòstic (adreça IP, identificador del dispositiu, metadades, cookies o tecnologies similars). Així, aquestes eines poden basar el seu preu en multitud de models econòmics, entre ells:

- Publicitat (que pot ser, integrada a l'aplicació o fora de l'aplicació)
- Una subscripció opcional a un servei que ofereix una funcionalitat addicional o desbloqueja determinades funcionalitats bàsiques (com el nombre màxim d'usuaris simultanis en un servidor).
- Anàlisi de patrons i estadístiques de les nostres interaccions per a la seva posterior comercialització.

PER EFECTUAR LA SELECCIÓ

- Afavorir solucions que garanteixin la protecció de dades, ja sigui certificades[1] o que disposin d'una Avaluació d'Impacte de Protecció de Dades per un tercer independent;
- Avaluar el risc en atenció al tipus de servei, no és el mateix el seu ús per desconges-tionar l'atenció assistencial que l'organització de reunions de l'àrea d'administració.
- Només valorar aplicacions per a les quals l'editor us indiqui clarament com es reutilit-zen les vostres dades (a les condicions de l'aplicació mateixa o al seu lloc web, per exemple);
- Comprovar que l'editor hagi implementat mesures de seguretat essencials, com ara el xifrat de comunicacions punt a punt. Cal recordar que en els casos en què un tercer presti un servei, les mesures de seguretat s'ha de correspondre amb les de l'Adminis-tració i, per tant, s'han d'ajustar a l'Esquema Nacional de Seguretat.[2]

ABANS D'INSTAL·LAR

- Evitar descarregar l'aplicació des d'un lloc web o una font desconeguda;
- Assegurar la vostra xarxa Wi-Fi amb una contrasenya forta, activant el xifrat WPA2 o WPA3;
- Assegurar que els vostres antivirus i tallafocs estiguin actualitzats.
- Utilitzar una contrasenya diferent de la que s'utilitza en altres serveis en línia.

Text de referència

MILLORA CONTINUA

- Si escau, aprofitar per renegociar les condicions d'ús de l'aplicació, en particular pel que fa al tractament de dades i a la relació Responsable-Encarregat.
- Recomanar als usuaris tant a l'ordinador com al telèfon, tancar l'aplicació quan ja no es faci servir, sobretot si s'activa el micròfon o la càmera web;
- Recomanar silenciar el micròfon i la càmera web quan no estiguin en ús. També es pot amagar físicament la càmera web, per exemple amb un tros de cinta o una funda.

Per a més informació:

- Nota de l'Agència de Ciberseguretat de Catalunya en relació a l'ús d'aplicacions de videoconferència
  https://ciberseguretat.gencat.cat/ca/detalls/noticia/Nota-de-lAgencia-de-Ciberseguretat-de-Catalunya-en-relacio-a-lus-daplicacions-de-videoconferencia
- COVID-19: consells de la CNIL (Agència Francesa de Protecció de Dades) sobre l'ús d'eines de videoconferència
  https://www.cnil.fr/fr/covid-19-les-conseils-de-la-cnil-pour-utiliser-les-outils-de-visioconference

Per qualsevol dubte o aclariment addicional podeu adreçar-vos al DPD de Salut:
dpd@ticsalutsocial.cat
https://ticsalutsocial.cat/oficina-dpd/
Tel.: 93 553 26 42 (9:00 a 14:00 h.) – *TEMPORALMENT INACTIU*

[1] Un exemple que ens informa la CNIL seria l'eina TIXEO:
https://www.ssi.gouv.fr/entreprise/certification_cspn/tixeoserver-version-11-5-2-0/

[2] Disposició addicional primera, Mesures de seguretat en l'àmbit del sector públic, de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.