

INFORMACIÓ SOBRE L'ENTRADA EN VIGOR DEL NOU REGLAMENT GENERAL DE PROTECCIÓ DE DADES

El proper 25 de maig de 2018 entra en vigor el nou Reglament (UE) 2016/679, 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 (Reglament general de protecció de dades), i per tant es derogarà tant la LOPD 15/1999 i el RD 1720/2007.

El nou RGPD conté molts conceptes, principis i mecanismes similars als que estableixen la Directiva 95/46 i les normes nacionals que l'apliquen. Per això, les organitzacions que actualment compleixen adequadament la LOPD 15/1999 tenen una bona base de partida per evolucionar cap a una correcta aplicació del nou Reglament. No obstant això, el RGPD modifica alguns aspectes del règim actual i conté noves obligacions que cada organització ha d'analitzar i aplicar tenint en compte les seves pròpies circumstàncies.

La innovació més gran de l'RGPD per als responsables la constitueixen dos elements de caràcter general: El principi de "responsabilitat proactiva". El RGPD descriu aquest principi com la necessitat que el responsable del tractament apliqui mesures tècniques i organitzatives apropiades, a fi de garantir i poder demostrar que el tractament és conforme al Reglament. En termes pràctics, aquest principi requereix que les organitzacions analitzin quines dades tracten, amb quines finalitats ho fan i quin tipus d'operacions de tractament duen a terme. A partir d'aquest coneixement, han de determinar de manera explícita com aplicaran les mesures que preveu l'RGPD. Així mateix, s'han d'assegurar que aquestes mesures són les adequades per complir-lo i que poden demostrar-ne el compliment davant les persones interessades i davant les autoritats de supervisió. Per tot això prenen especial importància les implicacions del nou Reglament relacionades amb els conceptes de privacitat en el disseny, seguretat en el disseny i privacitat per defecte, així com la inclusió de nous drets als ARCO actuals, com el d'informació (amb noves i importants implicacions), la portabilitat de les dades i la limitació del tractament.

Es farà molt prim en tot el relacionat amb la legitimació del tractament de dades personals, amb especial interès en el principi de consentiment (el RGPD requereix que l'interessat presti el consentiment mitjançant una declaració inequívoca o una acció afirmativa clara. Als efectes del nou Reglament, les caselles ja marcades, el consentiment tàcit o la inacció no constitueixen un consentiment vàlid) i la legitimació basada en interès legítim. Per tant, els responsables que efectuen tractaments basats en aquest consentiment per omissió haurien d'evitar continuar obtenint aquesta modalitat de consentiment i revisar aquests tractaments de manera que, a partir de maig de 2018, s'hagin adequat a les previsions del RGPD. Aquest consentiment haurà de ser explícit quan es realitzin tractaments de categories especials de dades (per exemple de salut).

S'haurà de tenir molt en compte també el principi de qualitat de les dades, on s'ha de considerar el principi d'exactitud, minimització i limitació del termini de conservació de les dades.

Nous requeriments: l'anàlisi de riscos, l'avaluació d'impacte i el delegat en protecció de dades.

Nota important: el requeriment de l'avaluació d'impacte no serà obligatori quan un tractament de dades d'historial del pacient el realitzi un únic professional de la salut (professional autònom), tal com indica el considerant 91 del RGPD.

Per a tractaments de salut on hi pugui intervenir més d'un professional, i a l'espera del que clarifiqui la nova legislació espanyola, serà necessari realitzar una avaluació d'impacte quan:

"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas."

"El tratamiento a gran escala de las denominadas categorías especiales de datos"

Per a realitzar aquesta avaluació caldrà obtenir de cada usuari que participi en algun tractament de dades, quines dades es tractaran (facilitades directament per l'interessat, facilitades per tercers, dades ja disponibles (reutilització), dades capturades, dades calculades, etc.), la descripció de les operacions de tractament (recollida, registre, estructuració, emmagatzemament, adaptació, modificació, extracció, consulta, utilització, comunicació per transmissió, difusió, comparació, combinació, restricció, supressió o destrucció).

S'hauran de detallar i definir les persones que participin en aquestes operacions de tractaments, quines tecnologies s'utilitzen, com s'obtenen les dades, com es registre, com s'emmagatzemen, quins documents s'utilitzen per recopilar la informació, encarregats de tractament, etc.

Per últim, s'haurà de nomenar un DPD (Delegat en Protecció de Dades) en aquells casos que:

"a) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

b) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales"

Per a qualsevol consulta, quedo a la vostra disposició a protecciondades@fisioterapeutes.cat