DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Butlletí protecció de dades

Butlletí del Departament de protecció de dades i Seguretat de la Informació de la Diputació Provincial de València

Butlletí N.º 25| Juliol 2022

ACTUALITZACIÓ DE L'ESQUEMA NACIONAL DE SEGURETAT DES DE LA PERSPECTIVA DE PROTECCIÓ DE DADES

ÍNDEX

NOCIONS BÀSIQUES DE LA VIDEOVIGILÀNCIA

Us convidem a traslladar-nos aquelles temàtiques que resulten del vostre interés per als pròxims butlletins informatius. Aquestes peticions hauran de dirigir-se a:

Diputació de València

Dpt. De Protecció de Dades i Seguretat de la Informació

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUBSCRIPCIONS

Si desitges subscriure's al nostre Butlletí informatiu accedeix al següent enllaç.

INTRODUCCIÓ

El passat 4 de maig es va publicar en el Butlletí Oficial de l'Estat el nou Esquema Nacional de Seguretat (Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, d'ara en avant "ENS"). L'ENS ofereix un catàleg de mesures de seguretat aplicables en funció de si el sistema s'ha valorat com a categoria BÀSICA, MITJANA o ALTA.

La Llei Orgànica 2/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (d'ara en avant, "LOPDGDD"), exigeix en la seua disposició adicional primera que les mesures de seguretat de l'ENS s'implanten en cas de tractament de dades personals per a evitar la seua pèrdua, alteració o accés no autoritzat, adaptant els criteris de determinació del risc en el tractament de les dades al que s'estableix en l'article 32 del Reglament (UE) 2016/679, del Parlament Europei i del Consell, de 27 d'abril de 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 (Reglament general de protecció de dades, d'ara en avant, "RGPD"). Aquesta obligació d'aplicar l'ENS s'esten, no sols a entitats del sector públic, sinó també a entitats del sector privat que col·laboren amb aquelles en la prestació de serveis públics que involucren el tractament de dades personals.

En aquest mateix sentit es pronuncia el legislador en la Llei Orgànica 7/2021, de 26 de maig, de protecció de dades personals tractats per a fins de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals. En concret, el seu artícle 37 incorpora l'obligació d'aplicar les mesures de l'ENS en els tractaments de dades personals per part de les autoritats públiques competents.

En la present publicació analitzarem els principals canvis de l'ENS després de la seua última actualització des de la perspectiva de protecció de dades.

"LA LOPDGDD EXIGE EN SU DISPOSICIÓN ADICIONAL PRIMERA QUE LAS MEDIDAS DE SEGURIDAD DEL ENS SE IMPLANTEN EN CASO DE TRATAMIENTOS DE DATOS PERSONALES PARA EVITAR SU PÉRDIDA, ALTERACIÓN O ACCESO NO AUTORIZADO".

PRINCIPALS CANVIS DE L'ESQUEMA NACIONAL DE SEGURETAT DES DE LA PERSPECTIVA DE PROTECCIÓ DE DADES

En l'article 3 de l'ENS s'estableix que quan un sistema d'informació tracte dades personals li serà aplicable el que es disposa en el RGPD i en la LOPDGDD, així com els criteris que s'establisquen per l'Agència Espanyola de Protecció de Dades (d'ara en avant, "AEPD") o, en el seu àmbit competencial, per les autoritats autonòmiques de protecció de dades, sense perjudici dels requisits establis a l'ENS.

Per tant, en aplicació del que es disposa en l'article 3 ENS, serà d'obligat compliment no sols la normativa de protecció de dades, sinó també els criteris de l'AEPD.

Els apartats 2 i 3 de l'article 3 ENS estableixen que, quan un sistema d'informació tracte dades personals, el responsable o l'encarregat del tractament, assessorat pel Delegat de Protecció de Dades, realitzaren una Anàlisi de Riscos conforme al que s'estableix en l'article 24 RGPD i, en els supòsits del seu article 35, una Avaluació d'Impacte en la Protecció de Dades. **En tot cas, prevaldran les mesures a implantar a conseqüència de l'anàlisi de riscos i, en el seu cas, de l'avaluació d'impacte** als quals es refereix l'apartat anterior, **en cas de resultar agreujades respecte de les previstes en l'ENS.**

Conforme al que es disposa en l'article 12 ENS, **la Política de Seguretat** de la informació és *"el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta*". Afig que, a aquest efecte, l'instrument que aprove aquesta política de seguretat **haurà d'incloure**, entre altres extrems, **els riscos que deriven de les dades personals**.

D'acord amb el que s'estableix en l'article 32.2 RGPD *"se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

En el **control ENS [op.exp.7.2]**, aplicable a totes les categories (bàsica, mitjana i alta), inclou modificacions en la gestió d'incidents respecte a la regulació anterior.

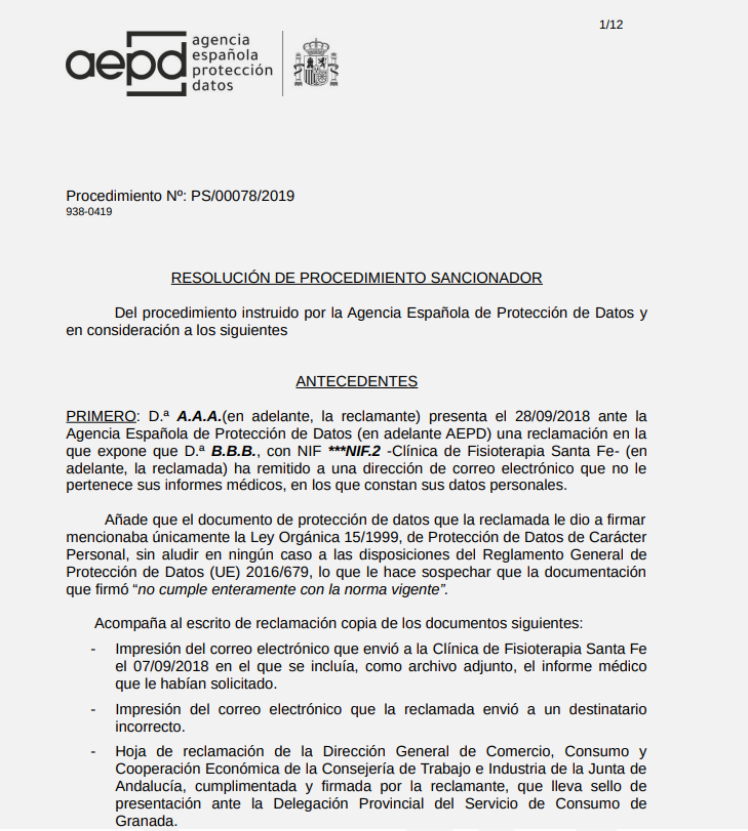
En particular, exigeix que *"la gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto."*

Això és, **en el procediment de gestió d'incidents s'haurà de tindre en compte la valoració de l'incident com a possible violació de la seguretat de les dades personals**, així com la possible notificació a l'autoritat de control i als interessats.

Què es considera "interconnexión"? Es denomina interconnexió a l'establiment d'enllaços amb altres sistemes d'informació per a l'intercanvi d'informació i serveis. En aquest sentit el **control ENS [op.ext.4.2]** (aplicable a categoria mitjana i alta) exigeix que **per a cada interconnexió es documente explícitament**: les característiques de la interfície, els **requisits de seguretat i protecció de dades** i la naturalesa de la informació intercanviada.

En el **control ENS [mp.info.1.1]**, aplicable a totes les categories (bàsica, mitjana i alta), s'exigeix el següent: "*Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.*"

SANCIÓ PER INCOMPLIMENT DE LA SEGURETAT DE LES DADES



1/12

agencia española protección datos

Procedimiento Nº: PS/00078/2019
938-0419

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en consideración a los siguientes

ANTECEDENTES

PRIMERO: D.ª ***A.A.A.***(en adelante, la reclamante) presenta el 28/09/2018 ante la Agencia Española de Protección de Datos (en adelante AEPD) una reclamación en la que expone que D.ª ***B.B.B.***, con NIF ******NIF.2*** -Clínica de Fisioterapia Santa Fe- (en adelante, la reclamada) ha remitido a una dirección de correo electrónico que no le pertenece sus informes médicos, en los que constan sus datos personales.

Añade que el documento de protección de datos que la reclamada le dio a firmar mencionaba únicamente la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, sin aludir en ningún caso a las disposiciones del Reglamento General de Protección de Datos (UE) 2016/679, lo que le hace sospechar que la documentación que firmó *"no cumple enteramente con la norma vigente"*.

Acompaña al escrito de reclamación copia de los documentos siguientes:

- Impresión del correo electrónico que envió a la Clínica de Fisioterapia Santa Fe el 07/09/2018 en el que se incluía, como archivo adjunto, el informe médico que le habían solicitado.
- Impresión del correo electrónico que la reclamada envió a un destinatario incorrecto.
- Hoja de reclamación de la Dirección General de Comercio, Consumo y Cooperación Económica de la Consejería de Trabajo e Industria de la Junta de Andalucía, cumplimentada y firmada por la reclamante, que lleva sello de presentación ante la Delegación Provincial del Servicio de Consumo de Granada.

La clínica de Fisioterapia Santa Fe va ser sancionada per l'Agència Espanyola de Protecció de Dades (Procediment Núm.: PS/00078/2019) per infracció de l'article 32 RGPD relatiu a la "seguridad de los datos", entre altres infraccions que també es reflecteixen en la citada resolució. Concretament, es va imposar una sanció d'advertència.

El reclamant trasllada a l'AEPD que la clínica havia remés a una adreça de correu electrònic que no li pertany els seus informes mèdics, en els quals consten dades personals.

Després de l'anàlisi de la documentació aportada, l'AEPD conclou que la clínica ha omés les mesures de seguretat que estava obligada a adoptar, a l'empara de l'article 32 RGPD, quan va remetre per correu electrònic un informe mèdic de la reclamant amb dades de salut a una adreça que va resultar ser errònia. L'AEPD es pronuncia en el procediment establint el següent:

"Los documentos que obran en el expediente y las declaraciones de la reclamada evidencian que ésta ***no había adoptado ninguna medida que garantizara la integridad de los datos personales*** *que trata, en particular con ocasión de su comunicación a través de medios electrónicos.*

La reclamada, en respuesta a la solicitud que le hizo la AEPD antes de la apertura del acuerdo de inicio del expediente para que informara sobre las medidas había adoptado para evitar que en el futuro se produzcan hechos análogos, informó en escrito de 13/02/2019 que "Desde la detección del error se ha tomado la decisión de enviar los informes médicos de los pacientes que lo soliciten por medios electrónicos sin incluir sus datos personales identificativos".

A propósito de la medida que dice haber adoptado hemos de advertir que ***no parece que tal decisión signifique una auténtica garantía de la integridad de los datos objeto de tratamiento****.*

Por una parte, porque, aunque en el email no se identifique al destinatario por su nombre, apellidos y NIF, en muchas ocasiones las direcciones de correo incorporan alguno o algunos de esos datos.

Por otra, porque, además de que los documentos del informe médico suelen incluir esos datos, el concepto de dato personal no se circunscribe a nombre, apellidos y NIF. El artículo 4.1) del RGPD entiende por dato personal "toda información sobre una persona física identificada o identificable ("el interesado"); se considera persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona". Por tanto, en relación a la infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de esa norma, de la que es responsable la reclamada, ***ésta no ha acreditado haber adoptado medida alguna con virtualidad para garantizar el cumplimiento de las obligaciones que le impone el precepto vulnerado.****"*

En conclusió, tal com es desprén del procediment, tot responsable del tractament ha d'estar en condicions de demostrar que ha implementat les mesures de seguretat adequades per a protegir les dades personals. En aquests casos, una declaració de conformitat amb l'ENS per als sistemes de categoria bàsica, o bé una certificació en l'ENS per als sistemes de categoria mitjana o alta, pot constituir una prova adequada de disposar controls de seguretat necessaris per a la correcta protecció de les dades personals.

MATERIAL COMPLEMENTARI

- Guia per a la notificació de bretxes de dades personals. Consulta la Guía en aquest enllaç.
- Guia de gestió del risc i avaluació d'impacte. Consulta la Guia en aquest enllaç.
- 10 malentesos relacionats amb l'anonimització. Consulta la publicació en aquest enllaç.
- Guia tecnologies i protecció de dades en les Administracions Públiques. Consulta la Guia en aquest enllaç.
- Guia de protecció de dades per defecte. Consulta la Guia en aquest enllaç.

NOTÍCIES

- **L'AEPD imposa una sanció d'advertència al servei andalús de salut per una infracció de l'article 32. 1b RGPD.** La part reclamada va incorporar informació de tercers a la història clínica del reclamant. Aquesta circumstància suposa una vulneració del principi de confidencialitat, atés que el reclamant ha tingut accés a informació de dades de salut d'altres pacients que resultaven identificables. En aquest sentit, l'AEPD conclou que *"el reclamado, en su condición de responsable de dicho tratamiento, debería de haber adoptado e implementado, en forma proactiva, las medidas técnicas y organizativas que resultasen apropiadas para evaluar y garantizar un nivel de seguridad adecuado a los probables riesgos de diversa naturaleza y gravedad vinculados a los tratamientos de datos de salud realizados que pudieran afectar, entre otros, a los principios de exactitud y confidencialidad"*. Consulta la resolució en aquest enllaç.

- **L'AEPD imposa una sanció d'advertència a la Conselleria d'educació (Junta d'Andalusia) per infracció de l'article 5.1.c RGPD -principi minimització de dades- i una altra infracció de l'article 5.1.f RGPD -principi d'integritat i confidencialitat.** Els motius en què basa la reclamació són que, després de realitzar les proves d'accés al cos de professors d'educació secundària, la publicació de les corresponents qualificacions obtingudes detallava el nom, cognoms i DNI complets de cadascun dels aspirants. L'AEPD conclou que "*La información no aparece segura si se impone como criterio de consulta el DNI, cuando previamente se han publicado los mismos, posibilitando la consulta por terceros al ser el dato DNI un medio de acceso débil, considerando además que la reclamada lo ha estado publicando en distintos procesos selectivos. El dato de consulta NIF en dicha casilla no ofrece seguridad al poder ser un dato que hoy por hoy puede ser conocido con no mucha dificultad"*. Consulta la resolució en aquest enllaç.