DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Quaderns DivalData

Quaderns dirigits a delegats, responsables i especialistes en protecció de dades personals

Quadern nº 2 | Agost 2020

COMPATIBILITAT DE LES FIGURES DEL DELEGAT DE PROTECCIÓ DE DADES I RESPONSABLES DE SEGURETAT

Í N D E X

Vos invitem a traslladar-nos aquelles temàtiques que resulten del vostre interès per als pròxims butlletins informatius. Estes peticions hauran de dirigir-se a:

Diputació de València

Dpt. de Protecció de Dades y Seguretat de la Informació

Pl. de Manises, 4 46003 València

Correu electrònic: dpdssi@dival.es

SUBSCRIPCIONS

Si desitges subscriure't a la nostra publicació accedix al següent

enllaç

COMPATIBILITAT DE LES FIGURES DEL DELEGAT DE PROTECCIÓ DE DADES I RESPONSABLES DE SEGURETAT

"EL PAPER DEL RESPONSABLE DE SEGURETAT ÉS GARANTIR LA SEGURETAT DE LA INFORMACIÓ DE LES ADMINISTRACIONS PÚBLIQUES. EL DPD, PER LA SEUA BANDA, GARAMTIX ELS DRETS I LLIBERTATS DE LES PERSONES LES DADES DELS QUALS SÓN TRATADES"

DIFERENCIACIÓ ENTRE L'ÀMBIT DE LA SEGURETAT DE LA INFORMACIÓ I EL DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

Les figures del Responsable de Seguretat (RSEG) i del Delegat de Protecció de Dades (DPD) es regulen en normes diferenciades, amb objectius i àmbits d'aplicació distints.

El paper del RSEG, que es regula en el **Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica (ENS)** , és garantir la **seguretat de la informació** de les Administracions Públiques, ja siguen dades personals o una altra informació de les Administracions Públiques.

El paper del DPD, per la seua banda, es regula en **el Reglament (UE) 2016/679, General de Protecció de Dades (RGPD)** i la **Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD)**, i consistix a garantir els **drets i llibertats de les persones** les dades dels quals són tractats.

A pesar de tractar-se d'àmbits d'actuació distints, es poden apreciar certes similituds en part de les funcions d'ambdós figures, motiu pel qual nombroses Administracions Públiques s'han qüestionat la possibilitat que ambdós confluïsquen en una mateixa persona.

En el present quadern analitzarem el règim jurídic d'ambdós figures i la seua compatibilitat, basant-se en la interpretació realitzada per l'Agència Espanyola de Protecció de Dades (AEPD).

"EL DPD HA ADQUIRIT UNA IMPORTÀNCIA ESSENCIAL EN EL MODEL DE PROTECCIÓ DE DADES ACTUALS. ESTE TINDRÀ, COM A MÍNIM, FUNCIONS D'INFORMACIÓ I ASSESSORAMENT PEL QUE FA A LES OBLIGACIONS DE LA NORMATIVA DE PROTECCIÓ DE DADES I DE COOPERACIÓ I PUNT DE CONTACTE AMB L'AUTORITAT DE CONTROL"

EL DELEGAT DE PROTECCIÓ DE DADES

El DPD és una figura que ha adquirit una importància essencial en el model de protecció de dades actuals, sent la seua designació obligatòria en determinats supòsits, com el cas en què el tractament de dades ho duga a terme una autoritat o organisme públic. Pel que es referix a les seues **FUNCIONS**, l'article 39 RGPD establix les següents:

Article 39. Funcions del delegat de protecció de dades.

1. El delegat de protecció de dades tindrà com a mínim les funcions següents

*a) **informar i assessorar** el responsable o a l'encarregat del tractament i als empleats que s'ocupen del tractament de les obligacions que els incumbixen en virtut del present Reglament i d'altres disposicions de protecció de dades de la Unió o dels Estats membres;*

*b) **supervisar** el compliment del que disposa el present Reglament, d'altres disposicions de protecció de dades de la Unió o dels Estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents;*

c) oferir l'assessorament que se li sol·licite sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar la seua aplicació de conformitat amb l'article 35;

d) cooperar amb l'autoritat de control;

e) actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36, i realitzar consultes, en el seu cas, sobre qualsevol altre assumpte.

Així mateix, la LOPDGDD preveu en el seu art. 36 que el DPD puga inspeccionar els procediments i emetre recomanacions, i en l'art. 37, la possibilitat que el mateix puga atendre les reclamacions que li plantejaren els afectats amb caràcter previ al fet que aquests acudisquen a l'autoritat de protecció de dades. Igualment, es preveu la possibilitat que plantejada una reclamació davant aquesta autoritat aquesta puga consultar al delegat de protecció de dades sobre la mateixa amb caràcter previ a la tramitació de la reclamació.

"EL DPD NO POT REBRE CAP INSTRUCCIÓ PEL QUE FA A L'EXERCICI DE LES SEUES FUNCIONS. ESTE PODRÀ EXERCIR ALTRES FUNCIONS I COMESES SEMPRE QUE NO DONEN LLOC A CONFLICTE D'INTERESSOS".

L'article 38.3 RGPD, en regular la POSICIÓ DEL DPD, subratlla la seua independència en assenyalar que: "el responsable i l'encarregat del tractament garantiran que el delegat de protecció de dades no reba cap instrucció pel que fa a l'acompliment d'aquestes funcions. No serà destituït ni sancionat pel responsable o l'encarregat per exercir les seues funcions. El delegat de protecció de dades rendirà comptes directament al més alt nivell jeràrquic del responsable o encarregat" i el seu apartat 6 afig que: "el delegat de protecció de dades podrà exercir altres funcions i comeses. El responsable o encarregat del tractament garantirà que aquestes funcions i comeses no donen lloc a conflicte d'interessos".

En aquest mateix sentit, l'article 36.2 del LOPDGDD especifica que: "Es garantirà la independència del delegat de protecció de dades dins de l'organització, havent d'evitar-se qualsevol conflicte d'interessos".

Precisament, en relació amb el possible conflicte d'interessos, el Grup de Treball de l'Article 29 (ara Comitè Europeu de Protecció de Dades) va assenyalar en el seu document de 'Directrius sobre els delegats de protecció de dades' el següent:

"Encara que els DPD puguen tindre altres funcions, solament podran confiar-se'ls altres tasques i comeses si aquestes no donen lloc a conflictes d'interessos. Això suposa, especialment, que el DPD no pot ocupar un càrrec en l'organització que li porte a determinar les finalitats i mitjans del tractament de dades personals. A causa de l'estructura organitzativa específica de cada organització, això haurà de considerar-se cas per cas. Com a norma general, els càrrecs en conflicte dins d'una organització poden incloure els llocs d'alta direcció (com ara director general, director d'operacions, director financer, director mèdic, cap del departament de màrqueting, cap de recursos humans o director del departament de TU) però també altres càrrecs inferiors en l'estructura organitzativa si tals càrrecs o llocs porten a la determinació de les finalitats i mitjans del tractament".

"EL RESPONSABLE DE SEGURETAT DETERMINARÀ LES DECISIONS PER A SATISFER ELS REQUISITS DE SEGURETAT DE LA INFORMACIÓ I DELS SERVICIS. A DIFERÈNCIA DEL DPD, QUE NO POT REBRE INSTRUCCIONS EN L'EXERCICI DE LES SEUES FUNCIONS, EL RESPONSABLE DE SEGURETAT SÍ POT REBRE INSTRUCCIONS DEL RESPONSABLE DE LA INFORMACIÓ".

Per part seua, l'AEPD, en el seu document de 'El delegat de protecció de dades en les Administracions Públiques' va assenyalar que: "En entitats de menor grandària serà possible que el DPD compagine les seues funcions amb unes altres. Si aquest és el cas, ha de tindre's en compte la necessitat d'evitar conflictes d'interessos entre les diverses ocupacions. El DPD actua com a assessor i supervisor intern, per la qual cosa aqueix lloc no pot ser ocupat per persones que, alhora, tinguen tasques que impliquen decisions sobre l'existència de tractaments de dades o sobre la manera en què seran tractats les dades (p. ex.: responsables de ITC, o responsables de seguretat de la informació)."

RESPONSABLE DE SEGURETAT

L' ENS regula esta figura en el seu article 10:

Article 10. La seguretat como a funció diferenciada.

En els sistemes d'informació es diferenciarà el responsable de la informació, el responsable del servei i el responsable de la seguretat.

El responsable de la informació determinarà els requisits de la informació tractada; el responsable del servei determinarà els requisits dels serveis prestats; i el responsable de seguretat determinarà les decisions per a satisfer els requisits de seguretat de la informació i dels serveis.

La responsabilitat de la seguretat dels sistemes d'informació estarà diferenciada de la responsabilitat sobre la prestació dels serveis. La política de seguretat de l'organització detallarà les atribucions de cada responsable i els mecanismes de coordinació i resolució de conflictes.

L'RSEG, a diferència del DPD, que no pot rebre instruccions en l'acompliment de les seues funcions, sí que pot rebre instruccions del Responsable de la Informació.

"AMB CARÀCTER GENERAL, HA D'EXISTIR LA NECESSÀRIA SEPARACIÓ ENTRE EL DPD I L'RSEG, SENSE QUE LES SEUES FUNCIONS PUGUEN RECAURE EN LA MATEIXA PERSONA O ÒRGAN COL·LEGIAT".

COMPATIBILITAT DE TOTES DUES FIGURES

1. L'AEPD va tractar la qüestió en l'Informe núm. 170/2018, interpretant que ha d'existir la necessària separació entre el DPD i l'RSEG, sense que les seues funcions puguen recaure en la mateixa persona. Algunes de les raons que esgrimeix són: A diferència de les figures que defineix l'article 10 de l'ENS, que reben ordres del responsable de la informació, el DPD no pot rebre instruccions de cap de les figures ja esmentades i obra amb total independència d'aquestes. Qüestió que, lògicament, impedeix que les funcions del DPD puguen ser dutes a terme per part de qualsevol dels rols implicats en el compliment de l'ENS els qui poden rebre instruccions del responsable de la informació. El nomenament del DPD sobre la mateixa persona o entitat que ostenta la condició d'RSEG suposaria negar el principi d'independència i segregació de funcions del ENS (art. 10) i, una negació del principi d'independència que determina el RGPD (art. 38.3).

2. Encara que podrien apreciar-se similituds en part de les funcions de totes dues figures, reitera l'AEPD que es tracta d'àmbits d'actuació diferents, amb objectius que haurien de ser diferenciats. Concretament el RSEG actua amb la finalitat de garantir la seguretat de la informació i les funcions del DPD han d'encaminar-se a garantir els drets i llibertats de les persones en els tractaments que duu a terme el responsable.

   En definitiva, amb **caràcter general, ha d'existir la necessària separació entre el DPD regulat en l'RGPD i l''RSEG de l'ENS, sense que les seues funcions puguen recaure en la mateixa persona o òrgan col·legiat**. Només seria admissible, excepcionalment, en aquelles organitzacions que, per la seua grandària i recursos, no pogueren observar aquesta separació, sempre que en la persona concorregueren els requisits de formació i capacitació previstos en l'RGPD i s'adoptaren totes les mesures organitzatives que garantiren la necessària independència i l'absència de conflicte d'interessos. En tot cas, aquesta circumstància haurà d'avaluar-se cas per cas, i haurà de motivar-se i documentar-se aquesta designació.

MATERIAL COMPLEMENTARI

- Informe núm. 170/2018, sobre la possible compatibilitat entre la figura del DPD i RSEG (AEPD). Consulta l'informe en aquest enllaç..
- Directrius sobre els Delegats de Protecció de Dades (Grup de Treball de l'Article 29). Consulta el document en aquest enllaç.
- Guia de Seguretat de les TIC – CCN-STIC 801 – Esquema Nacional de Seguretat. Responsabilitats i funcions (CCN). Consulta la Guia en aquest enllaç.
- El Delegat de Protecció de Dades en les Administracions Públiques (AEPD). Consulta el document en aquest enllaç.

NOTÍCIES

- **L'Agència Espanyola de Protecció de Dades publica un informe sobre l'accés a Fons Documentals i Obres d'una Administració Pública. En l'Informe N/REF: 0046/2019, l'AEPD dona resposta a la qüestió relativa a l'adequació a la normativa de protecció de dades de la posada en marxa d'un programa d'accés a fons documentals i obres per part d'una Administració. Consulta la resolució** en aquest enllaç.

- **L' Autoritat Catalana de Protecció de Dades publica un Dictamen sobre la consideració de determinades dades biomètriques com a dades de categoria especial. En el Dictamen CNS 21/2020, la APDCAT dona resposta a la consulta d'una Administració Pública sobre la consideració de determinades dades biomètriques tractats amb mitjans tècnics per a autenticar una persona física, com a dades de categoria especial. Consulta el Dictamen en** aquest enllaç.

- **La Agència Espanyola de Protecció de Dades publica un article sobre el xifrat homomòrfic. El xifrat homomòrfic és una tècnica de privacitat per defecte adequada per a aquells casos en què un responsable subcontracta una part d'una activitat a un encarregat, i vol garantir tècnicament que aquest no accedirà a les dades. L'AEPD ens mostra alguns conceptes, esquemes i possibles usos. Consulta l'article** en aquest enllaç.

- **La Agència Espanyola de Protecció de Dades publica un article sobre els escorçadors d'URLs i la protecció de dades. Quan fem clic en un enllaç escurçat no podem estar segurs d'on ens portarà, i això pot posar en risc la nostra privacitat. L'AEPD ens parla dels seus riscos per a la privacitat i mesures a tindre en compte. Consulta l'article** en aquest enllaç.

- **El Tribunal de Justícia de la Unió Europea declara invàlid l'Escut de Privacitat per a la realització de transferències internacionals de dades als EUA. La sentència, estableix, al seu torn, la validesa de les clàusules contractuals estàndard adoptades per la Comissió Europea. Consulta la Sentència** en aquest enllaç.