Dictamen en relació amb la consulta d'un Departament de la Generalitat, sobre les funcions del DPD en relació amb altres perfils, en concret, el Responsable de Seguretat de la Informació i Protecció de Dades del mateix Departament

Ref. CNS 17/2024

Antecedents

1. La consulta demana a aquesta Autoritat que emeti dictamen respecte de la figura i funcions del delegat de protecció de dades (en endavant, DPD), en relació amb "els referents en protecció de dades", que segons la consulta exerceixen funcions relatives a les actuacions del diferents departaments o ens del sector públic en l'àmbit de la protecció de dades, com seria el cas del Responsable de Seguretat de la Informació i Protecció de Dades d'un Departament de la Generalitat, al que es refereix la consulta.

Així, la consulta demana avaluar l'encaix de la figura d'aquests referents en relació amb el DPD, tenint en compte les previsions recollides a la normativa de protecció de dades personals, així com al Decret 148/2023, d'1 d'agost, sobre les persones delegades de protecció de dades de l'Administració de la Generalitat i el seu sector públic (article 4), i les previsions del Decret de reestructuració del Departament, a les que es refereix la consulta.

La consulta s'acompanya de còpia de diversa normativa, entre d'altres, la Resolució de concurs específic per a la provisió del lloc de responsable de Seguretat de la Informació i Protecció de Dades de la Secretaria General del Departament; i còpia dels documents "Directrices sobre los delegados de protección de datos (5.05.2017), del Grup de treball de l'article 29 (GT 29), i *"2023 Coordinated Enforcement Action. Designation and position of Data Protection Officers"* (16.01.2024), del Comitè Europeu de Protecció de Dades (EDPB).

2. Analitzada la consulta, vista la normativa vigent aplicable, i d'acord amb l'informe de l'Assessoria Jurídica, s'informa del següent:

Fonaments de dret

I

(...)

II

La consulta es refereix a la figura i funcions del delegat de protecció de dades (en endavant, DPD), tenint en compte la normativa de protecció de dades, i el seu encaix, en quant a les funcions desenvolupades, amb altres "referents en protecció de dades."

Respecte d'aquests referents de protecció de dades, la consulta explica que *"exerceixen funcions relatives a les actuacions dels diferents departaments o ens del sector públic en*

l'àmbit de la protecció de dades, com és el cas del Responsable de Seguretat de la Informació i Protecció de Dades del Departament" que formula la consulta.

Fem notar, d'entrada, que no hi ha previsions normatives que hagin configurat la figura, el rol o les funcions dels "referents en protecció de dades", ja sigui en el Decret 148/2023, d'1 d'agost, sobre les persones delegades de protecció de dades de l'Administració de la Generalitat i el seu sector públic, o en d'altra normativa.

En qualsevol cas, als efectes d'aquest dictamen cal partir de la premissa que, des de la perspectiva de la normativa de protecció de dades, la figura que l'RGPD configura i dota de funcions específiques als efectes d'assessorar els responsables i encarregats del tractament de dades personals (art. 4, apartats 7 i 8 RGPD, respectivament), en relació amb la correcta aplicació de dita normativa, i per supervisar les activitats del tractament dels responsables -o encarregats del tractament-, és, específicament, el DPD.

Dit això, la consulta es refereix específicament al rol del Responsable de Seguretat de la Informació i Protecció de Dades del propi Departament (en endavant, RS), i aporta normativa relativa al dit Departament i a les funcions que el Departament hauria assignat al lloc de treball esmentat (RS).

Situada la consulta en aquests termes, cal concretar d'entrada quin és el rol i les funcions de la figura del DPD, segons la normativa aplicable, això és, el Reglament (UE) 2016/679, del Parlament i del Consell Europeu, de 27 d'abril de 2016, General de Protecció de Dades (RGPD), que és la norma que crea aquesta figura que en aquest cas el Departament hauria nomenat atesa la previsió de l'article 37.1.a) de l'RGPD.

L'article 38 RGPD estableix la posició que ha de tenir el DPD dins l'organització, en aquest cas, el Departament que formula la consulta, en els següents termes:

> *"1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.*
>
> *2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.*
>
> *3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.*
>
> *4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.*

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses."

I l'article 39 de l'RGPD estableix les funcions dels DPD, de les quals es desprèn el paper fonamental que desenvolupa en el model de responsabilitat proactiva implantat pel RGPD, si bé ajustat a les funcions de naturalesa assessora i supervisora que li corresponen, en els següents termes:

"1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2.El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento."

Sobre la figura del DPD cal tenir en compte les previsions dels articles 34 a 37 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD).

En concret, i segons l'article 36 LOPDGDD:

"1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir

recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento."

Per tant, es desprèn de la normativa aplicable que el DPD ha de tenir un coneixement adequat i suficient dels procediments relacionats amb el tractament de dades personals que es duen a terme, que li permeti donar compliment de forma independent a les funcions que la normativa li assigna. En qualsevol cas, l'article 38.1 RGPD defineix l'abast de la intervenció del DPD en uns termes força amplis.

Afegim que el Decret 148/2023, esmentat, explicita a l'article 2.3 que:

"(...).
3. Les persones delegades de protecció de dades en els departaments de l'Administració de la Generalitat s'adscriuen orgànicament a la secretaria general. Aquesta adscripció en cap cas afecta el règim d'independència funcional de la figura de la persona delegada de protecció de dades.

4. La persona delegada de protecció de dades actua, en l'exercici de les seves funcions, amb plena independència funcional i no està subjecte a instruccions, ordres de servei i recomanacions del responsable del tractament ni de cap altre òrgan de l'organització."

Per tant, el rol del DPD dins el Departament que formula la consulta és el que ve determinat per l'RGPD, sense que la seva adscripció orgànica o la coexistència amb d'altres figures o d'altres òrgans als que farem referència més endavant (singularment, el RS al que es refereix la consulta), pugui desvirtuar les funcions que la normativa atribueix al DPD, i la independència funcional amb la que necessàriament ha d'actuar el DPD, tal i com explicita la normativa estudiada.

III

Més en concret, la normativa conté previsions específiques relatives a la participació del DPD, entre d'altres, en relació amb el registre d'activitats del tractament (RAT), al que es refereix l'article 30 RGPD.

Així, l'article 31.1 de l'LOPDGDD, *in fine*, disposa el següent, en relació amb el RAT:
"Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro."

Així mateix, en relació amb la notificació de violacions de seguretat (NVS) que el responsable ha de dur a terme, si escau, a l'Autoritat competent (art. 33 RGPD), la normativa estableix que el responsable ha de comunicar, entre d'altres, el nom i dades de contacte del DPD (art.33.3.b) RGPD). Aquesta comunicació respon a que el DPD és l'interlocutor de l'organització amb les Autoritats de protecció de dades i, per tant, en lògica conseqüència, el DPD haurà d'estar informat d'allò que afecta els dits incidents o violacions de seguretat que es puguin produir a l'organització.

En aquestes i altres previsions de l'RGPD (per exemple, art. 36 RGPD), és clar que la normativa de protecció de dades atribueix al DPD un paper específic com a interlocutor entre l'organització responsable del tractament i l'Autoritat de control, atesa la seva implicació i participació en totes aquelles qüestions que afecten al tractament de dades personals dins l'organització.

I en relació amb les avaluacions d'impacte en la protecció de dades (AIPD), cal recordar també que el DPD té un rol específic, tal i com preveu la normativa (art. 35.1 RGPD), segons la qual el responsable comptarà amb l'assessorament del DPD (art. 35.2 RGPD).

Amb tot això, als efectes de la consulta, cal recordar que, segons el GT 29 (apartat 4.2 de les Directrius sobre el DPD):

"El Grupo de Trabajo del artículo 29 recomienda que el responsable del tratamiento busque el asesoramiento del DPD en las siguientes cuestiones, entre otras:

- si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos;
- qué metodología debe seguirse al llevar a cabo una evaluación de impacto;
- si debe realizarse la evaluación de impacto en la propia organización o subcontratarse;
- qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados;
- si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD."

Com també fa avinent el GT 29 al mateix document (apartat 2.5):

"La capacidad del DPD para desempeñar sus funciones debe interpretarse tanto en referencia a sus cualidades personales y conocimientos como a su puesto dentro de la organización. Las cualidades personales deben incluir, por ejemplo, la integridad y un nivel elevado de ética profesional; la principal preocupación del DPD debe ser posibilitar el cumplimiento del RGPD. El DPD desempeña un papel fundamental en la promoción de una cultura de protección de datos dentro de la organización y contribuye a la aplicación de elementos esenciales del RGPD, como los principios relativos al tratamiento de datos, los derechos de los interesados, la protección de los datos desde el diseño y por defecto, el registro de las actividades de tratamiento, la seguridad del tratamiento y la notificación y comunicación de las violaciones de la seguridad de los datos."

El mateix document estableix el següent (apartat 3.1):

"Es fundamental que el DPD, o su equipo, participen desde la etapa más temprana posible en todas las cuestiones relativas a la protección de los datos. En cuanto a las evaluaciones de impacto relativas a la protección de datos, el RGPD dispone expresamente la implicación temprana del DPD y especifica que el responsable del tratamiento recabará el asesoramiento del DPD al realizar dicha evaluación de impacto. Garantizar que se informa y consulta al DPD desde el principio facilitará el cumplimiento del RGPD, fomentará un enfoque de privacidad desde el diseño y, por lo tanto, debería ser un procedimiento estándar en la gobernanza de la organización. Asimismo, es importante que el DPD sea considerado como un interlocutor dentro de la organización y que forme parte de los correspondientes grupos de trabajo que se ocupan de las actividades de tratamiento de datos dentro de la organización.

En consecuencia, la organización debe garantizar, por ejemplo, que:

- Se invita al DPD a participar con regularidad en reuniones con los cuadros directivos altos y medios.
- Se recomienda que esté presente cuando se toman decisiones con implicaciones para la protección de datos. Toda la información pertinente debe transmitirse al DPD a su debido tiempo con el fin de que pueda prestar un asesoramiento adecuado.
- La opinión del DPD se tiene siempre debidamente en cuenta. En caso de desacuerdo, el Grupo de Trabajo recomienda, como buena práctica, documentar los motivos por los que no se sigue el consejo del DPD.
- Se consulta al DPD con prontitud una vez que se haya producido una violación de la seguridad de los datos o cualquier otro incidente."

Finalment, en l'àmbit de Catalunya, el Decret 148/2023, d'1 d'agost, sobre les persones delegades de protecció de dades de l'Administració de la Generalitat i el seu sector públic, que resulta d'aplicació al cas que ens ocupa, té per objecte establir el règim jurídic de les persones delegades de protecció de dades de l'Administració de la Generalitat i el seu sector públic institucional, així com la regulació de la Comissió de Coordinació de Protecció de Dades (art. 1).

L'article 2 del Decret 148/2023 reitera la plena independència funcional dels DPDs, i que aquests no es troben subjectes a instruccions, ordres de servei i recomanacions del responsable del tractament ni de cap altre òrgan de la organització (art. 2.4 Decret).

I l'article 4 de la mateixa norma concreta les funcions dels DPDs en l'àmbit de l'Administració de la Generalitat, en els següents termes:

"1. La persona delegada de protecció de dades té les funcions següents:

a) Informar, assessorar i col·laborar amb les persones responsables o encarregades del tractament de dades.
b) Inspeccionar procediments, comunicar l'existència de vulneracions en matèria de protecció de dades i emetre recomanacions.
c) Supervisar el compliment correcte del Reglament UE 2016/679, així com d'altres disposicions normatives sobre protecció de dades.

d) Assessorar en les avaluacions d'impacte sobre la protecció de dades i supervisar-ne l'aplicació.
e) Cooperar amb l'Autoritat Catalana de Protecció de Dades i les altres autoritats de control.
f) Actuar com a punt de contacte de les autoritats de control per a qüestions relatives al tractament, inclosa la consulta prèvia a l'autoritat de control.
g) Atendre les reclamacions de les persones interessades o les que li derivi l'Autoritat Catalana de Protecció de Dades.
h) Lliurar al responsable del tractament una memòria anual en què es recullin les activitats desenvolupades amb una menció expressa de les incidències que s'hagin pogut observar en l'exercici de les funcions assignades.
i) Retre comptes de la seva activitat i resultats, quan se li requereixi, davant la persona titular de la secretaria general del departament, o de la direcció de l'entitat del sector públic corresponent.
j) Qualsevol altra funció que li assigni la normativa vigent.

2. La persona delegada de protecció de dades ha d'exercir les funcions observant la deguda atenció als riscos associats a les operacions de tractament i considerant, així mateix, la naturalesa, l'abast, el context i les finalitats del tractament.

3. Els òrgans i unitats departamentals, i també les entitats del sector públic, han de prestar el suport i la col·laboració necessaris a la persona delegada de protecció de dades per garantir el desenvolupament correcte de les funcions assignades, incloent-hi els recursos formatius, la disposició de mitjans tècnics i la disponibilitat d'espais."

Fem avinent que aquesta Autoritat va emetre l'Informe PD 10/2022, en relació amb el Projecte de Decret sobre les persones delegades de protecció de dades de l'Administració de la Generalitat i el seu sector públic, que es troba disponible al web www.apdcat.cat.

En definitiva, la normativa de protecció de dades configura el rol del DPD com un element de garantia del dret fonamental a la protecció de dades personals dins l'organització. Així, el DPD informa i assessora al responsable del tractament pel que fa a tot allò que tingui incidència en la protecció del dret fonamental a la protecció de dades personals dins l'organització, en els termes que preveu la normativa, amb plena independència en l'exercici de les seves funcions respecte de la resta d'òrgans o d'altres figures de l'organització, en garantia del dret a la protecció de dades personals.

En qualsevol cas, vista la normativa aplicable, resulta recomanable que el responsable del tractament defineixi amb claredat les funcions que hagi de dur a terme el DPD en el marc de la normativa de protecció de dades, per tal que aquest pugui actuar amb independència dins l'organització i que s'evitin, així mateix, possibles conflictes d'interessos en relació amb l'exercici de les seves funcions (considerant 97 RGPD, art. 38.6 RGPD i art. 36.2 LOPDGDD).

En aquest sentit, en les Directrius del GT 29, esmentades, es proposa el següent (apartat 3.1):

"Cuando sea pertinente, el responsable o el encargado del tratamiento podría elaborar directrices o programas sobre la protección de datos que determinen cuándo debe consultarse al DPD."

Així, sens perjudici de les consideracions que es faran més endavant, ja avancem que, atesos els termes de la consulta, podria ser recomanable que el Departament, en compliment del principi de responsabilitat proactiva (art. 5.2 RGPD), estableixi els casos en què l'organització ha de consultar al DPD, a efectes de claredat.

IV

Dit això, cal diferenciar entre la figura del DPD, a la que ja ens hem referit, d'altres figures que també preveu la normativa, com ara l'anomenat "responsable de seguretat" (en endavant, RS) que, en principi, i per la informació de què es disposa, sembla que seria la figura a la que específicament es refereix la consulta.

D'entrada, l'article 156.2 de la Llei 40/2015, d'1 d'octubre, del règim jurídic del sector públic, disposa que:

"2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de Seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada."

En desenvolupament d'aquesta previsió, el Reial Decret 311/2022, de 3 de maig, que regula l'Esquema Nacional de Seguretat (ENS), estableix els mecanismes i mesures de seguretat que caldrà aplicar amb la finalitat de protegir els sistemes d'informació de l'entitat, així com els serveis vinculats als sistemes d'informació.

En aquest context, i en relació amb la seguretat dels sistemes d'informació, l'article 11 del Reial Decret 311/2022, de 3 de maig, que regula l'Esquema Nacional de Seguretat (ENS), estableix els rols de diferents intervinents, entre d'altres, el responsable de seguretat:

"1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el ***responsable de la seguridad*** *y el responsable del sistema.*
2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.
3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos."

Segons l'article 12.1 de l'RD 311/2022, la normativa defineix la política de seguretat de la informació com el conjunt de directrius que regeixen la forma en què una organització gestiona i protegeix la informació que tracta i els serveis que presta, i preveu que l'instrument que aprovi la política de seguretat d'una organització ha de tenir un contingut mínim en el que s'inclou, entre d'altres, *"els riscos que es deriven del tractament de les dades personals"* (art. 12.1, apartar f) RD 311/2022).

I segons l'article 13 del mateix RD 311/2022 :

"(…)
2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e

identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El responsable de la información determinará los requisitos de la información tratada.
b) El responsable del servicio determinará los requisitos de los servicios prestados.
c) ***El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.***
d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. (…).
4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.
(…).”

Així, la normativa estudiada estableix que la política de seguretat ha d'aplicar una sèrie de requisits mínims (art. 12.6 RD 311/2022), en relació amb els quals la mateixa normativa especifica diferents àmbits d'intervenció del RS (art. 28 RD 311/2022, al que ens remetem, en relació amb les mesures de seguretat a aplicar, detallades a l'annex II de la mateixa norma).

D'una banda, com hem vist, el DPD informa i assessora el responsable en tot allò que afecta el dret a la protecció de dades de les persones titulars de la informació que és objecte de tractament per part del responsable, i a l'assegurament de l'exercici dels drets *d'habeas data* per part dels afectats, i ho fa amb plena independència respecte d'altres intervinents, com puguin ser les figures que, en l'àmbit de la seguretat de la informació, crea la normativa reguladora de l'ENS. A més, el DPD és l'interlocutor amb l'Autoritat de control en matèria de protecció de dades.

D'altra banda, correspondria al RS vetllar per totes aquelles qüestions que afectin la seguretat dels sistemes d'informació de l'organització, en aquest cas, al Departament. En definitiva, pel que es desprèn de la normativa aplicable, l'ENS limita el rol i les funcions del RS a l'àmbit específic de la seguretat de la informació.

Òbviament dins el concepte d'informació s'inclou la informació personal sotmesa als principis i garanties de l'RGPD. I també pot entendre's que la política de seguretat que estableix una organització en la utilització de mitjans electrònics en el context de l'ENS, en la que hauran de participar les diferents figures que estableix l'ENS (entre d'altres, el RS), pot tenir un impacte en el tractament del conjunt de la informació que tracta la organització, per tant, també en la informació personal sotmesa als principis i garanties de l'RGPD.

Ara bé, la diferenciació o segregació de funcions que estableix l'ENS en relació amb diferents responsables (art. 11.3 RD 311/2022), també s'ha d'entendre que opera necessàriament, per exigència de l'RGPD, respecte d'aquests en relació amb el DPD. I això, no només per la diferenciació d'àmbits en els que s'actua (l'àmbit de la seguretat de la

informació pel que fa al RS, i l'àmbit de la protecció del dret fonamental a la protecció de dades pel que fa al DPD), sinó perquè altrament es podria condicionar l'actuació amb plena independència d'aquest DPD.

Així, tenint en compte que el DPD té dependència orgànica però no funcional dins l'organització, no pot rebre ordres ni indicacions sobre l'assessorament que li correspon donar al responsable o encarregat per part d'altres òrgans, els quals sí tenen aquesta dependència funcional dins l'organització.

Aquesta segregació de funcions deriva de l'article 38.3 RGPD, esmentat, segons el qual el responsable ha de garantir que el DPD no rep instruccions de cap altre òrgan de l'organització en l'exercici de les seves funcions per tant, en aquest cas, no pot rebre instruccions dels òrgans esmentats a què es refereix el RD 311/2022.

Com ha quedat dit, seguint les Directrius del GT 29, i vistos els termes de la consulta, i a efectes del compliment del principi de transparència (art. 5.1.a) RGPD), i del principi de responsabilitat proactiva (art. 5.2 RGPD), sembla pertinent que l'organització responsable, en aquest cas, el Departament, diferenciï de forma clara els àmbits respectius en els que les dues figures a què es refereix la consulta (DPD i RS), operen.

Això, sens perjudici que, atesos els àmbits d'actuació d'ambdues figures (DPD i RS), es pugui donar una col·laboració, o que hi hagi actuacions en les que intervenen ambdós i que es poden arribar a relacionar.

A tall d'exemple, recordem les previsions de la normativa respecte la intervenció del DPD en relació amb les avaluacions d'impacte relatives a la protecció de dades (AIPD), prevista en l'article 35.2 RGPD i delimitada, en quant a les recomanacions que caldria seguir en relació amb aquesta intervenció, per les Directrius del GT 29 (apartat 4.2, esmentat).

I pel que fa a l'àmbit de l'ENS, la taula de mesures de Seguretat prevista a l'RD 311/2022, preveu, entre d'altres, que (apartat # [mp.info.1.1]): *"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."*

En qualsevol cas, l'article 3 del mateix RD 311/2022, explicita que, en el cas que els sistemes d'informació tractin dades personals, resulta d'aplicació la normativa de protecció de dades (RGPD i LOPDGDD o, si escau, Llei orgànica 7/2021), així com els criteris de les Autoritats de protecció de dades, sens perjudici dels requisits establerts al dit RD 311/2022 (art. 3.1), i afegeix (apartats 2 i 3), que:

> *"2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.*

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto."

Per tant, en aquest cas les normatives estudiades estableixen clarament el rol dels dos intervinents a què es refereix la consulta. Precisament perquè en d'altres casos la distinció podria no ser tan clara, resulta recomanable, com hem apuntat, que el responsable estableixi, com apunta el GT 29, com ha de ser aquesta intervenció, i adopti les mesures necessàries per garantir d'una banda, la independència del DPD i, d'altra banda, la salvaguarda de les seves funcions d'assessorament i supervisió, que no es poden veure afectades per disposicions autoorganitzatives que, en la pràctica, puguin suposar el buidatge o desconeixement de les seves funcions.

V

Com apunta la consulta, el Decret de reestructuració preveu que diferents òrgans del Departament tenen la funció, entre d'altres, de *"Vetllar pel compliment de la normativa de protecció de dades i ciberseguretat dels tractaments del Departament* (...), *amb l'assistència del Gabinet Tècnic i amb l'assessorament i la supervisió del delegat o delegada de protecció de dades."*

I segons l'article 43.1.k) del mateix Decret, correspon al Gabinet Tècnic:

"k) Assegurar l'existència de les mesures organitzatives que garanteixin la seguretat de la informació i la protecció de les dades personals, i coordinar l'organització interna per a la ciberseguretat i la protecció de les dades de caràcter personal del Departament."

La normativa de protecció de dades exigeix al responsable establir mesures tècniques i organitzatives adequades per tal de garantir un nivell de seguretat adequat al risc i el correcte compliment del principi d'integritat i confidencialitat (art. 32 i art. 5.1.f) RGPD) i, en definitiva, el compliment del conjunt de principis establerts a l'RGPD. Així, la previsió esmentada sembla indicar que el Departament articula el compliment de les seves obligacions de compliment de l'RGPD, a nivell intern, a través del dit Gabinet Tècnic.

Aquesta menció, des de la perspectiva de la protecció de dades, resulta adequada, si bé no sembla imprescindible fer-ne esment, atès que l'RGPD ja preveu i explicita les obligacions del responsable.

Qüestió diferent és que es pugui interpretar la "coordinació" a la que es refereix l'article 43.1.k) del Decret de reestructuració, com una limitació de les funcions i de l'assessorament que correspon al DPD (en els termes als que ens hem referit abastament).

Que el Departament coordini a través del dit òrgan la manera com s'ha d'assegurar la protecció de dades (el compliment dels principis, mesures i garanties que ha d'aplicar el responsable) no resulta problemàtic des de la perspectiva de la protecció de dades, sempre que això no suposi un impediment per al compliment de les funcions del DPD, o de l'execució d'aquestes funcions amb plena independència, com s'ha indicat, o que la

utilització el terme “coordinació” es vulgui interpretar d’una manera extensiva, afecten funcions exclusives del DPD.

És a dir, la “coordinació” prevista en la norma esmentada, no ha d’interpretar-se en el sentit que pugui condicionar o limitar l’assessorament i l’actuació independent del DPD de l’organització, ni pot suposar que aquest rebi indicacions del dit Gabinet Tècnic pel que fa al desenvolupament de les dites funcions.

En línia amb el que va apuntar aquesta Autoritat en l’Informe PD 10/2022, citat, en relació amb la creació de la Comissió de Coordinació de Protecció de Dades (art. 8 Decret 148/2023), fem esment de la definició dels principis de col·laboració, cooperació i coordinació de l’article 140 de la Llei 40/2015, de l’ú d’octubre, de règim jurídic del sector públic, LRJSP, (art. 140.1, apartats c), d) i e) respectivament).

Segons la LRJSP, el principi de coordinació implica que l’Administració pública *“tiene la obligación de garantizar la coherencia de las actuaciones de las diferentes “administraciones públicas (...).”*

Per tant, el principi de coordinació comporta un element d’obligatorietat, a diferència dels principis de cooperació i de col·laboració, segons la LRJSP.

Als efectes que interessen, la dita previsió normativa (art. 43.1.k) citat), en concret, la dita “coordinació”, no s’hauria d’interpretar en el sentit que el DPD pugui rebre indicacions pel que fa al seu assessorament o al desenvolupament de les seves funcions des del dit òrgan (Gabinet Tècnic), ja que això posaria en risc la independència que l’RGPD atribueix a l’actuació del DPD.

Fem notar que, segons la Resolució de convocatòria de concurs específic, entre d’altres, del lloc de responsable de seguretat de la informació i protecció de dades, al que es refereix la consulta, el lloc de treball de responsable de Seguretat de la Informació i Protecció de Dades té per missió: *“Proposar l'adopció dels requeriments i les mesures organitzatives que garanteixin la seguretat de la informació i la protecció de les dades personals, i coordinar-ne la implementació al Departament* (...), *d'acord amb la normativa vigent, els procediments establerts i les directrius dels superiors jeràrquics, amb la finalitat de complir amb els objectius del Departament en l'àmbit de la protecció de dades personals i seguretat de la informació.”*

També aquest apartat s’hauria d’interpretar, pels motius exposats, en el sentit que la missió del RS es desenvolupa sens perjudici de les funcions d’assessorament que corresponen al DPD i de la necessària col·laboració amb el DPD en tot allò que es refereixi a la protecció de dades de caràcter personal.

En aquesta línia, i pel que fa a les finalitats/funcions del lloc de treball esmentat (apartat 4 de la Resolució esmentada), fem avinent que, a criteri d’aquesta Autoritat, hi ha diverses previsions que, vista la seva redacció, podrien no ser prou aclaridores en el sentit indicat.

Així, segons aquest apartat:

“Finalitats/funcions:

a) Proposar als òrgans que tinguin assignada la responsabilitat directiva sobre la seguretat de la informació i la protecció de dades personals la valoració i els requeriments de seguretat dels sistemes d'informació i dels tractaments de dades personals, així com l'acceptació del risc residual resultant de les anàlisis de risc i de les mesures de seguretat que, per mitigar els riscos identificats, puguin ser raonablement aplicades en termes de tecnologia disponible i cost, en coordinació amb la persona designada per l'Agència de Ciberseguretat de Catalunya (...).
b) Fer els tractaments de dades personals proporcionals i necessaris per comprovar la seguretat de la xarxa, de la informació i dels serveis vinculats.
c) Fer les avaluacions d'impacte dels tractaments de dades per determinar-ne el risc per als drets i les llibertats de les persones físiques, demostrar-ne l'ajust normatiu i decidir si és necessari consultar o demanar autorització a l'autoritat de control abans de realitzar el tractament, en coordinació amb la persona designada per l'ACC en l'àmbit del Departament.
d) Analitzar els tractaments de dades personals per verificar el compliment de les obligacions legals, els principis normatius i els requisits específics de la base jurídica del tractament.
e) Proposar l'adopció de les polítiques internes i les mesures tècniques i organitzatives que permetin el compliment normatiu, i coordinar-ne l'aplicació d'acord amb les directrius dels superiors jeràrquics.
f) Mantenir el registre de les activitats de tractament executades sota la seva responsabilitat d'acord amb les prescripcions legals, i posar-lo a disposició de les autoritats de control que el sol·licitin.
g) Assessorar les unitats del Departament en les matèries pròpies del seu àmbit competencial, i promoure el respecte i les bones pràctiques de l'organització en matèria de seguretat i protecció de dades personals.
h) Arbitrar fórmules per facilitar l'exercici dels drets dels interessats respecte de les seves dades personals, i elaborar les propostes de resposta a les peticions presentades i les que s'han de trametre a l'Autoritat Catalana de Protecció de Dades (ACPD) a conseqüència de la iniciació d'un procediment de tutela de drets o la presentació d'una denúncia.
i) Fer la valoració de compliment normatiu de les propostes d'encàrrecs de tractament i cessió de dades i, quan s'escaigui, elaborar la documentació necessària per formalitzar-los.

(...).”

Ateses les previsions normatives (arts. 38 i 39 RGPD i 36 LOPDGDD), i les consideracions fetes en aquest dictamen, fem notar que alguns d’aquests apartats, en la seva redacció actual, tampoc no recullen de forma clara la necessària intervenció del DPD, i podrien derivar en una afectació a les seves funcions.

En definitiva, aquestes previsions, referides a la missió i les funcions atribuïdes al RS del Departament, des de la perspectiva de la protecció de dades, s’haurien d’entendre sens perjudici del compliment de les funcions atribuïdes al DPD, i de la necessària col·laboració amb el DPD en tot allò que es refereixi a la protecció de dades de caràcter personal, i sens perjudici de les funcions que l’RGPD atribueix específicament al DPD.

Aquesta consideració es fa amb caràcter general i, especialment, en relació amb les previsions dels apartats c), d), f), g), h) i i), esmentats, en els quals es troba a faltar una menció o aclariment en aquest sentit.

En conclusió, atès que el Departament ha de garantir la participació del DPD en totes les qüestions relatives a la protecció de dades de forma adequada i en el temps oportú, en els termes de la normativa aplicable i com apunta el GT 29, que el DPD és l'interlocutor amb les Autoritats de protecció de dades en relació amb les qüestions relatives a la protecció de dades, i que té atribuïdes funcions específiques, en relació amb l'assessorament al responsable, les avaluacions d'impacte en la protecció de dades o en relació amb l'exercici dels drets ARSOPOL, entre d'altres, sembla recomanable interpretar la dita Resolució en els termes apuntats.

Conclusions

El rol del DPD dins l'organització del responsable (art. 4.7 RGPD) ve determinat per l'RGPD, sense que la seva adscripció orgànica o la coexistència i col·laboració amb d'altres figures, com ara la dels "referents en protecció de dades", o d'altres òrgans (singularment, el responsable de seguretat), pugui desvirtuar les funcions que la normativa li atribueix o la seva independència funcional.

Tenint en compte la normativa aplicable, i seguint les Directrius del Grup de Treball de l'Article 29, podria ser recomanable que el Departament, en compliment del principi de responsabilitat proactiva (art. 5.2 RGPD), estableixi els casos en què cal consultar al DPD, a efectes de claredat i en els termes que s'exposen en aquest dictamen, als efectes de garantir les funcions assessores i supervisores pròpies del DPD.

Atès que el Departament ha de garantir la participació del DPD en totes les qüestions relatives a la protecció de dades de forma adequada i en el temps oportú, en els termes de la normativa aplicable i com apunta el GT 29, que el DPD és l'interlocutor amb les Autoritats de protecció de dades en relació amb les qüestions relatives a la protecció de dades, i que té atribuïdes funcions específiques en relació amb l'assessorament al responsable, amb les AIPD o amb l'exercici dels drets ARSOPOL, entre d'altres, s'hauria d'interpretar la Resolució de concurs específic en els termes apuntats en el Fonament Jurídic V d'aquest dictamen.

Barcelona, 15 de juliol de 2024