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 Núm. 8 | Febrer 2021

TRANSFERÈNCIES INTERNACIONALS DE DADES. PRINCIPALS CONSEQÜÈNCIES DESPRÉS DE L'ANUL·LACIÓ DEL PRIVACY SHIELD

Í N D E X

TRANSFERÈNCIES INTERNACIONALS DE DADES. PRINCIPALS CONSEQÜÈNCIES DESPRÉS DE L'ANUL·LACIÓ DEL PRIVACY SHIELD

Vos 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 València

email: dpdssi@dival.es

SUSCRIPCIONS

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

enllaç

"DESPRÉS DE L'ANUL·LACIÓ DEL PRIVACY SHIELD, TOTES AQUELLES TRANSFERÈNCIES DE DADES EMPARADES EN AQUEST, DEIXEN D'OFERIR GARANTIES I, PER TANT, HAN DE DEIXAR DE TRANSFERIR-SE DADES SOBRE LA BASE D'AQUEST ESCUT O, EN EL SEU CAS, HAN DE BUSCAR-SE ALTRES MECANISMES QUE OFERISQUEN UN NIVELL DE GARANTIA ADEQUAT".

INTRODUCCIÓ

En el marc de la normativa de protecció de dades, s'entén per «transferència internacional» el flux de dades personals des del territori espanyol a destinataris establits en països fora de l'Espai Econòmic Europeu – EEE (a més dels països de la Unió Europea, Liechtenstein, Islàndia i Noruega).

Per a que una transferència internacional siga vàlida, s'ha de complir alguna de les condicions establides en el Capítol V del Reglament General de Protecció de Dades (d'ara en avant, RGPD). Entre aquestes, s'inclou la Declaració de nivell de protecció adequat per la Comissió Europea.

En aquesta situació es trobaven algunes entitats estatunidenques que, en el marc de la 'Decisió d'Execució (UE) 2016/1250 de la Comissió, sobre l'adequació de la protecció conferida per l'Escut de la privacitat UE-EUA' es comprometien a complir una sèrie de principis de protecció de la vida privada, establits pel Departament de Comerç dels Estats Units, que permetien el flux de dades personals entre els països de l'EEE i els Estats Units (d'ara en avant, els EUA).

No obstant això, el 16 de juliol de 2020, el Tribunal Superior de Justícia de la Unió Europea (d'ara en avant, TSJUE) dictava Sentència en l'assumpte C-311/18 (Schrems contra Facebook Ireland), invalidant la citada Decisió 2016/1250 («Privacy Shield» o «Escut de Privacitat»). Aquesta Sentència va tindre el seu origen en la reclamació interposada per Max Schrems, usuari de Facebook, per la transferència internacional de dades des de Facebook Ireland a Facebook Inc., als EUA. Aquest va alegar que el Dret i les pràctiques dels EUA no oferien suficient protecció enfront de l'accés, per part de les autoritats públiques, a les dades transferides.

L'anul·lació del «Privacy Shield» va suposar que totes les transferències de dades emparades en el mateix deixaren d'oferir garanties i, per tant, la necessitat de deixar de transferir dades personals sobre la base d'aquest Escut o, en el seu cas, de buscar altres mecanismes que oferisquen un nivell de garantia adequat.

"LES ORGANITZACIONS HAN DE REVISAR DETALLADAMENT LES TRANSFERÈNCIES INTERNACIONALS DE DADES CAP ALS ESTATS UNITS, SOVINT DERIVADES DE CONTRACTACIÓ ADMINISTRATIVA DE SERVEIS TECNOLÒGICS I L'ÚS D'APLICATIUS DE PROVEÏDORS ESTATUNIDENCS."

Aquesta qüestió revist especial complexitat des del punt de vista de la contractació administrativa de serveis tecnològics i l'ús d'aplicatius de proveïdors estatunidencs d'enorme profusió i popularitat, que fins ara feien ús del «Privacy Shield» per a legitimar les transferències de dades dels països de l'EEE als EUA.

MOTIUS DE L'ANUL·LACIÓ

El TSJUE va considerar que els requisits del Dret nacional estatunidenc i, en particular, alguns programes que permetien a les autoritats públiques dels EUA accedir a les dades personals transferides des de la UE als EUA amb finalitats de seguretat nacional, imposaven limitacions a la protecció de les dades personals i no oferien garanties substancialment equivalents a les exigides en el Dret de la Unió.

A més, no es proporcionava cap via de recurs judicial contra les autoritats dels EUA als titulars de les dades.

A conseqüència de tal interferència amb els drets fonamentals de les persones les dades de les quals es transfereixen a aqueix país tercer, el TSJUE va declarar invàlida la Decisió d'adequació del «Escut de Privacitat».

CONSEQÜÈNCIES DE L'ANUL·LACIÓ

El TSJUE va invalidar el «Privacy Shield» sense mantindre els seus efectes i sense concedir cap període de gràcia, ja que la legislació estatunidenca avaluada pel Tribunal no proporciona un nivell de protecció substancialment equivalent al garantit a la UE.

Això obliga les organitzacions a revisar detalladament les transferències internacionals de dades cap als EUA, sovint derivades de la contractació administrativa de serveis tecnològics i l'ús d'aplicatius de proveïdors estatunidencs.

Per a continuar transferint dades personals als EUA, les organitzacions hauran de donar compliment a

alguna de les condicions de l'art. 46 o següents del RGPD, que examinarem a continuació.

ALTRES EINES DE TRANSFERÈNCIA

A falta de Decisió d'adequació, es poden efectuar transferències internacionals de dades als EUA fent ús d'altres eines establides en els articles 46 a 49 del RGPD. Com quines?

1. CLÀUSULES CONTRACTUALS TIPUS (CCT)

Les Clàusules Contractuals Tipus (d'ara en avant, CCT), contemplades en l'art. 46 RGPD, són aquelles clàusules estandarditzades que han sigut adoptades per la Comissió Europea o una autoritat de control.

Són una manera de permetre la transferència de dades entre països de la Unió Europea i un tercer país, ja que suposen el compliment de determinades garanties en la protecció de les dades de l'interessat.

En la citada Sentència C-311/18 (Maximillian Schrems contra Facebook Ireland), a més de la validesa del «Privacy Shield», el TSJUE també va examinar la 'Decisió 2010/87/UE de la Comissió, de 5 de febrer de 2010, relativa a les clàusules contractuals tipus per a la transferència de dades personals als encarregats del tractament establits en tercers països, de conformitat amb la Directiva 95/46/CE', mantenint la seua validesa, encara que supeditant-la a l'avaluació del nivell de protecció exigit per la legislació de la UE al país tercer i, en cas que aquest no fora adequat, a l'avaluació de la necessitat d'adoptar mesures complementàries per a garantir un nivell de protecció equivalent a l'establit en l'Espai Econòmic Europeu (EEE).

Per tant, la possibilitat de transferir dades personals sobre la base de les CCT dependrà del resultat d'aquesta avaluació, tenint en compte les circumstàncies de cada transferència i les mesures complementàries que haja pogut aplicar l'entitat estatunidenca en qüestió.

"LES CLÀUSULES CONTRACTUALS TIPUS (CCT) MANTENEN LA SEUA VALIDESA, ENCARA QUE SUPEDITADES A L'AVALUACIÓ DEL NIVELL DE PROTECCIÓ EXIGIT PER LA LEGISLACIÓ DE LA UE EN EL PAÍS TERCER I, EN CAS QUE AQUEST NO FORA ADEQUAT, A L'AVALUACIÓ DE LA NECESSITAT D'ADOPTAR MESURES COMPLEMENTÀRIES PER A GARANTIR UN NIVELL DE PROTECCIÓ EQUIVALENT A L'ESTABLIT EN L'EEE".

"SI S'ARRIBA A LA CONCLUSIÓ QUE, TENINT EN COMPTE LES CIRCUMSTÀNCIES DE LA TRANSFERÈNCIA I LES POSSIBLES MESURES COMPLEMENTÀRIES, NO S'OFERIRIEN GARANTIES ADEQUADES, SERIA NECESSARI SUSPENDRE O POSAR FI A LA TRANSFERÈNCIA DE DADES PERSONALS".

Les CCT, després d'una anàlisi cas per cas de les circumstàncies de la transferència, juntament amb les mesures complementàries que, en el seu cas, foren necessàries, haurien de garantir que la legislació estatunidenca no afecte el nivell de protecció adequat.

Si s'arriba a la conclusió que, tenint en compte les circumstàncies de la transferència i les possibles mesures complementàries, no s'oferirien garanties adequades, seria necessari suspendre o posar fi a la transferència de dades personals.

En relació amb les mesures addicionals, el Comité Europeu de Protecció de Dades (CEPD) ha fet públic un document de recomanacions sobre mesures que complementarien les eines de transferència per a garantir el compliment del nivell de protecció de dades personals de la UE. Aquest conté una llista no exhaustiva d'exemples de mesures complementàries i algunes de les condicions que necessitarien per a ser eficaces. Per exemple:

a) MESURES TÈCNIQUES

Quines mesures tècniques podria adoptar un proveïdor de serveis de hosting estatunidenc per a emmagatzemar dades personals, per exemple, amb finalitats de mantindre una còpia de seguretat?

1. Fort encriptació de les dades abans de la seua transmissió;
2. L'algorisme de xifratge i la seua parametrització (per exemple, la longitud de la clau, la manera de funcionament, si escau) s'ajusten a l'estat de la tècnica i poden considerar-se robustos enfront de la criptoanàlisi realitzada per les autoritats públiques del país receptor, tenint en compte els recursos i les tècniques (per exemple, potència de computació per a atacs de força bruta) disponibles per a ells;
3. La força del xifratge té en compte el període de temps específic durant el qual ha de preservar-se la confidencialitat de les dades personals codificades;

"LES MESURES ADDICIONALS HAURAN DE DECIDIR-SE CAS PER CAS, TENINT EN COMPTE TOTES LES CIRCUMSTÀNCIES DE LA TRANSFERÈNCIA".

4. L'algorisme d'encriptació s'implementa sense problemes mitjançant un programari de manteniment adequat, la conformitat del qual haja sigut verificada, per exemple, per una certificació;
5. Les claus es gestionen de manera fiable;
6. Les claus es conserven únicament sota el control de l'exportador de dades o altres entitats a les quals s'haja confiat aquesta tasca que resideixen en l'EEE o en un tercer país, territori o un o més sectors específics dins d'un tercer país, o en una organització internacional per a la qual la Comissió ha establit en de conformitat amb l'article 45 del Reglament sobre l'aplicació de la llei, que es garanteix un nivell de protecció adequat.

   En aquest cas, el CEPD considera que l'encriptació realitzada seria una mesura complementària efectiva.

b) MESURES ORGANITZATIVES

El CEPD recomana mètodes d'organització i mesures de minimització de dades. Encara que els requisits organitzatius ja existeixen en virtut del principi de responsabilitat proactiva, supervisats amb auditories periòdiques i aplicant també mesures disciplinàries, podrien ser útils en un context de les transferències. Així mateix, ha de considerar-se especialment la minimització de les dades; per exemple, quan la prestació d'un servei només requerisca la transferència d'un conjunt limitat de dades, no s'ha de facilitar la base de dades completa. Però estableix com a condició la realització d'auditories periòdiques i l'aplicació de mesures disciplinàries estrictes per a vigilar i fer complir les mesures de minimització de dades en el context de les transferències. A més, també exigeix per a considerar vàlida aquesta mesura complementària, que les mesures de minimització de dades vagen acompanyades de mesures tècniques.

De totes maneres, hem de tindre en compte que les mesures addicionals hauran de decidir-se cas per cas, tenint en compte totes les circumstàncies de la transferència.

"QUAN LES TRANSFERÈNCIES ES BASEN EN EL CONSENTIMENT DEL TITULAR DE LES DADES, HAURAN DE SER: EXPLÍCITES; ESPECÍFIQUES PER A LA TRANSFERÈNCIA O CONJUNT DE TRANSFERÈNCIES DE DADES CONCRETA; I INFORMADES.

2. CONSENTIMENT

Encara és possible transferir dades als EUA sobre la base de les excepcions previstes en l'article 49 del RGPD, sempre que s'apliquen les condicions establides en aquest article. En particular, ha de recordar-se que quan les transferències es basen en el consentiment del titular de les dades, hauran de ser: explícites; específiques per a la transferència o conjunt de transferències de dades concreta (cosa que significa que l'exportador de les dades ha d'assegurar-se d'obtindre una autorització específica abans que es pose en marxa la transferència, fins i tot si això ocorre després d'efectuar-se la recollida de les dades); informades, en particular sobre els possibles riscos de la transferència (és a dir, que el titular de les dades també hauria de ser informat dels riscos específics derivats del fet que les seues dades seran transferides a un país que no ofereix una protecció adequada i que no s'apliquen garanties adequades destinades a garantir la protecció de les dades).

No obstant això, l'elevat llindar que estableix el RGPD per a l'ús d'aquesta excepció, combinat amb el fet que el consentiment prestat per un interessat pot retirar-se en qualsevol moment, fan que el consentiment no siga una solució viable a llarg termini per a les transferències internacionals de dades.

3. EXECUCIÓ D'UN CONTRACTE ENTRE EL TITULAR DE LES DADES I EL RESPONSABLE DEL TRACTAMENT

En aquest supòsit, ha de tindre's en compte que les dades personals només podran transferir-se quan la transferència siga ocasional. Haurà d'establir-se cas per cas si les transferències de dades es determinarien com a «ocasionals» o «no ocasionals». En qualsevol cas, aquesta excepció només podrà invocar-se quan la transferència siga objectivament necessària per a l'execució del contracte.

“PROVEÏDORS DE SERVEIS TECNOLÒGICS ESTATUNIDENCS COM GOOGLE, MICROSOFT, AMAZON, MAILCHIMP O ZOOM, LES EINES DEL QUAL SÓN SOVINT UTILITZADES PER ENTITATS PÚBLIQUES I PRIVADES, I LES TRANSFERÈNCIES INTERNACIONALS DE LES QUALS DE DADES QUEDAVEN LEGITIMADES FINS AL MOMENT PEL «PRIVACY SHIELD», HAN OPTAT PER ADOPTAR CLÀUSULES CONTRACTUALS TIPUS (CCT) PER A REGULARITZAR LES TRANSFERÈNCIES DE DADES PERSONALS ENTRE PAÏSOS DE LA UE I ELS EUA”.

4. RAONS IMPORTANTS D'INTERÉS PÚBLIC

El CEPD recorda que el requisit substancial per a l'aplicabilitat d'aquesta excepció és la constatació d'un interés públic important i no la naturalesa de l'organització, i que, encara que aquesta excepció no es limita a les transferències de dades que són «ocasionals», això no significa que les transferències de dades sobre la base de l'excepció per raons importants d'interés públic puguen tindre lloc a gran escala i de manera sistemàtica. Per contra, ha de respectar-se el principi general segons el qual les excepcions establides en l'article 49 del RGPD no han de convertir-se en «norma» en la pràctica, sinó que han de limitar-se a situacions específiques i cada exportador de dades ha de garantir que la transferència complisca la prova de necessitat estricta.

PER QUINA EINA HAN OPTAT ELS PROVEÏDORS DE SERVEIS TECNOLÒGICS ESTATUNIDENCS?

Proveïdors de serveis tecnològics estatunidencs com Google, Microsoft, Amazon, Mailchimp o Zoom, les eines del qual són sovint utilitzades per entitats públiques i privades, i les transferències internacionals de les quals de dades quedaven legitimades fins al moment pel «Privacy Shield», han optat per adoptar Clàusules Contractuals Tipus (CCT) per a regularitzar les transferències de dades personals entre països de l’EEE i els EUA. Com hem assenyalat, les CCT continuen mantenint la seua validesa, encara que supeditades a una avaluació que tinga en compte les circumstàncies de les transferències i a l'adopció de mesures complementàries que oferisquen garanties adequades.

"SI L'ORGANITZACIÓ A LA QUAL PERTANYS TRANSFEREIX DADES PERSONALS FORA DE L'ESPAI ECONÒMIC EUROPEU (A MÉS DE LA UE, NORUEGA, ISLÀNDIA I LIECHTENSTEIN), S'HA DE REVISAR EL GRAU DE COMPLIMENT D'AQUESTES A LA NORMATIVA DE PROTECCIÓ DE DADES."

PROCEDIMENT PER A LA REVISIÓ DE LES TRANSFERÈNCIES INTERNACIONALS DE DADES

Si l'organització a la qual pertanys transfereix dades personals fora de l'Espai Econòmic Europeu, s'ha de revisar el grau de compliment d'aquestes a la normativa de protecció de dades.

Quin procediment podem seguir per a la revisió?

1. Per a detectar **les transferències internacionals de dades,** pot ser d'utilitat el Registre d'Activitats de Tractament (RAT) de la nostra organització. En aquest, haurien de constar les transferències de dades personals a un tercer país o una organització internacional, inclosa la identificació de dita tercera país o organització internacional -art. 30 1.e) RGPD-.
2. Comprova si el país al qual es transfereixen les dades, és un **destinatari declarat de nivell adequat per la Comissió Europea** (art. 45 RGPD). Fins hui, els països i territoris declarats com a adequats són: Suïssa, el Canadà, l'Argentina, Guernsey, Illa de Man, Jersey, Illes Fèroe, Andorra, Israel, l'Uruguai, Nova Zelanda i el Japó. Com indicàvem supra, les entitats estatunidenques certificades en el marc de l'Escut de Privacitat UE-EUA ja no es consideren destinatàries de nivell adequat.
3. A falta de decisió d'adequació, verifica si compleix amb alguna de les **garanties que estableix l'art. 46 RGPD.** Especialment, comprova l'existència de Clàusules **Contractuals** Tipus aprovades per la Comissió. Encara que després de la Sentència del TSJUE aquestes Clàusules mantenen la seua validesa, la supediten a l'avaluació del nivell de protecció exigit per la legislació de la UE al país tercer i, en cas que aquest no fora suficient, a l'avaluació de la necessitat d'adoptar mesures complementàries per a garantir un nivell de protecció equivalent a l'establit en l'Espai Econòmic Europeu (EEE). En aquests casos, hauríem de revisar o instar el proveïdor que justifique que en el tercer país:

"ENCARA QUE S'HAGUEREN SUBSCRIT CLÀUSULES CONTRACTUALS TIPUS, HAURÍEM DE REVISAR O INSTAR EL PROVEÏDOR QUE JUSTIFIQUE QUE EN EL TERCER PAÍS: (I) HI HA NORMATIVA DE PROTECCIÓ DE DADES OFERISCA GARANTIES SUBSTANCIALMENT EQUIVALENTS A LES EXIGIDES EN EL DRET DE LA UNIÓ; (II) HI HA UNA AUTORITAT ON ELS INTERESSATS PUGUEN RECLAMAR EN MATÈRIA DE PROTECCIÓ DE DADES; (III) LA LEGISLACIÓ NO PERMET QUE LES AGÈNCIES D'INTEL·LIGÈNCIA PUGUEN ACCEDIR MASSIVAMENT I SENSE CONTROL JUDICIAL A LES DADES."

- hi ha normativa de protecció de dades oferisca garanties substancialment equivalents a les exigides en el Dret de la Unió;
- hi ha una autoritat on els interessats puguen reclamar en matèria de protecció de dades;
- la legislació no permet que les agències d'intel·ligència puguen accedir massivament i sense control judicial a les dades.

Si el tercer país no compleix amb aquests requisits, haurien d'aplicar-se o instar el proveïdor a incloure mesures addicionals en matèria de protecció de dades, que hauran de decidir-se cas per cas, tenint en compte totes les circumstàncies de la transferència de què es tracte.

4. Mancant garanties adequades, la transferència únicament es podria realitzar si concorre alguna de les **excepcions** de l'art. 49 RGPD (consentiment explícit; execució d'un contracte entre l'interessat i el responsable o per a l'execució de mesures precontractuals adoptades a sol·licitud de l'interessat; celebració o execució d'un contracte, en interés de l'interessat, entre el responsable del tractament i una altra persona física o jurídica; raons importants d'interés públic; formulació, exercici o la defensa de reclamacions; protegir els interessos vitals de l'interessat o d'altres persones, quan l'interessat estiga física o jurídicament incapacitat per a donar el seu consentiment; registre públic que tinga per objecte facilitar informació al públic).

   Quan tampoc siga aplicable cap d'aquestes excepcions, només es podrà dur a terme la transferència si no és repetitiva, afecta a un nombre limitat d'interessats, és necessària als fins d'interessos legítims imperiosos perseguits pel responsable del tractament sobre els quals no prevalguen els interessos o drets i llibertats de l'interessat, i el responsable del tractament vaig avaluar totes les circumstàncies i, basant-se en aquesta avaluació, oferisca garanties apropiades respecte a la protecció de dades personals.

   No obstant això, aquestes excepcions únicament han d'aplicar-se amb caràcter residual, quan resulte impossible l'aplicació d'altres eines i la transferència afecte pocs interessats.

MATERIAL COMPLEMENTARI

- Informació sobre transferències internacionals (AEPD). Consulta el seu web en aquest enllaç.
- Sentència del Tribunal de Justícia de la Unió Europea (TSJUE), de 16 de juliol de 2020, assumpte C-311/18. Consulta l'informe en aquest enllaç.
- Preguntes freqüents sobre la sentència del Tribunal de Justícia de la Unió Europea en l'assumpte C-311/18 (CEPD). Consulta el document en aquest enllaç.
- Recomanació 01/2020 sobre mesures que complementen les eines de transferència per a garantir el compliment del nivell de protecció de dades personals de la UE (CEPD). Consulta el document en aquest enllaç.
- Decisió 2010/87/UE de la Comissió, de 5 de febrer de 2010, relativa a les clàusules contractuals tipus per a la transferència de dades personals als encarregats del tractament establits en tercers països, de conformitat amb la Directiva 95/46/CE. Consulta la Decisió en aquest enllaç.
- Addenda de protecció de dades de Microsoft (actualitzada a desembre de 2020). Consulta aquest enllaç.
- Addenda de protecció de dades de Google Suite. Consulta aquest enllaç.
- Clàusules contractuals tipus Google G Suite. Consulta aquest enllaç.
- Instruccions per a acceptar el Contracte d' encarregat del tractament de Google Analytics. Consulta aquest enllaç.
- Instruccions per a acceptar el contracte de encarregat del tractament i Clàusules Contractuals Tipus de Google Workspace i Cloud Identity. Consulta aquest enllaç.
- Contracte de protecció de dades i Clàusules contractuals tipus de Mailchimp. Consulta aquest enllaç.

NOTÍCIES

- **L'Agència Espanyola de Protecció de Dades (AEPD) llança un Pacte Digital per a la protecció de les persones que promou un gran acord per la convivència ciutadana i fomenta el compromís amb la privacitat de les organitzacions.**

  La iniciativa, a la qual ja s'han adherit 40 organitzacions empresarials, fundacions, associacions de mitjans i grups audiovisuals, suposa un compromís amb la privacitat en les polítiques de sostenibilitat i els models de negoci d'empreses i organitzacions. El Pacte es compon de diversos documents: la carta d'adhesió, el compromís per la responsabilitat en l'àmbit digital i un decàleg de bones pràctiques per a mitjans de comunicació i organitzacions amb canals de difusió propis.

  Consulta la informació relativa al Pacte Digital en aquest enllaç.

- **El Comité Europeu de Protecció de Dades (CEPD) publica un document de Directrius 01/2021, sobre exemples relacionats amb la notificació de violacions de seguretat.**

  Les Directrius, basades en casos pràctics, complementen les Directrius WP 250 del GT29 i reflecteixen l'experiència de les autoritats de control en aquesta matèria des de l'entrada en vigor el RGPD. El seu objectiu és ajudar als responsables del tractament de dades a manejar les violacions de seguretat i quins factors tindre en compte durant l'avaluació de riscos, llançant llum sobre si s'ha de notificar o no a l'autoritat de control als interessats. El document està obert a consulta pública fins al 2 de març.

  Consulta el document (únicament en anglés) en aquest enllaç.