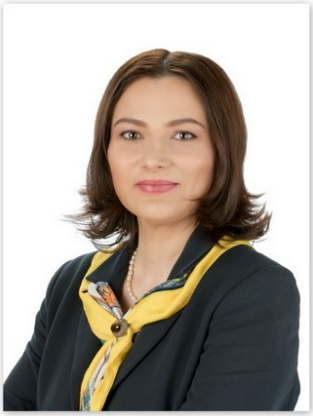
No-Deal Brexit - Impactul asupra obligațiilor de protecție a datelor



Sinopsis

Un scenariu al ieșirii Regatului Unit din UE fara acord a devenit mai probabil în ultimele zile, dar cele doua parți spera inca sa evite acest scenariu. În analiza de mai jos, Marta Popa, coordonatorul practicii noastre de protecția datelor, descrie modul în care un Brexit fara acord va afecta obligațiile dvs. de protecție a datelor.

Deși nu se poate garanta care dintre alternativele actuale de ieșire se va materializa (nota noastra: acceptarea de catre Marea Britanie a acordului convenit de Theresa May ca fiind "singura cale" pentru ca Marea Britanie sa paraseasca blocul comunitar într-un mod organizat, sau cel mai daunator scenariu (no-deal/fara acord), sau o întârziere prelungita a datei de ieșire a Regatului Unit), ce ar însemna un scenariu fara acord în ceea ce privește obligațiile de protecția datelor?

Atâta timp cât firmele din Regatul Unit ***vând bunuri și servicii cetațenilor celorlalte 27 de state membre UE*** și colecteaza, prelucreaza și stocheaza în mod activ datele cu caracter personal ale cetațenilor UE, vor fi în continuare afectate de GDPR, chiar și dupa ce ieșirea din UE, deoarece Regulamentul prevede ca indiferent de locația firmei dvs., ***daca sunteți implicat în prelucrarea datelor cu caracter personal ale cetațenilor UE, trebuie sa respectați prevederile GDPR***.

Așadar, ce ar trebui exact sa faceți în pregatire pentru un Brexit fara acord *?

❶ Revizuiți fluxurile de date catre Regatul Unit din SEE și luați în considerare mecanismele de garanție GDPR pe care va trebui sa le puneți în aplicare.

❷ Revizuiți fluxurile de date dinspre Regatul Unit, astfel încât sa puteți documenta noul temei juridic pentru aceste transferuri în conformitate cu regulile de transfer din Regatul Unit.

❸ Revizuiți informațiile de confidențialitate și documentația interna pe care le dețineți pentru a identifica detaliile care vor necesita actualizare.

❹ Asigurați-va ca persoanele cheie din organizația dvs. cunosc aceste aspecte și le vor aplica în scenariul "fara acord".

Am analizat mai detaliat aceste elemente, oferindu-va mai jos perspectiva noastra:

I. Fluxuri de Date și Instrumente de transfer de date

Ca recunoaştere a gradului de aliniere fara precedent între regimurile de protecţie a datelor din Regatul Unit şi SEE, companiile sau organizaţiile din Regatul Unit vor putea în continuare sa trimita date cu caracter personal dinspre Regatul Unit catre SEE și țari terțe considerate adecvate de catre UE la momentul ieșirii din UE a Regatului Unit.

Cu toate acestea, va exista o schimbare în modul în care datele sunt transferate dinspre SEE catre Regatul Unit.

A. Transferul de date dinspre Regatul Unit catre UE/SEE

Toate datele cu caracter personal din Regatul Unit vor putea continua sa circule liber în toate statele Uniunii Europene ("UE") și în Spațiul Economic European ("SEE"). Companiile sau organizațiile din Regatul Unit vor trebui sa respecte in continuare legislația privind protecția datelor.

B. Transferul de date dinspre UE/SEE catre Regatul Unit

În absența unei decizii de adecvare a UE în favoarea Regatului Unit, va trebui sa se instituie o anumita forma de protecție în temeiul Legii privind protecția datelor din 2018 GDPR/UK pentru a proteja transferurile internaționale dinspre UE/SEE catre Regatul Unit.

Clauzele Contractuale Standard UE (“CCS”)

În prezent, CEPD (Comitetul European pentru Protecția Datelor) a recunoscut clauzele model sau CCS pentru transferurile operator-operator sau operator-persoana împuternicita de operator. Exportatorul de date UE/SEE, atunci când are calitatea de operator de date cu caracter personal în cadrul UE, ar trebui sa se poata baza în siguranța pe CCS atunci când transfera datele cu caracter personal din UE catre o organizație din Regatul Unit care poate fi un operator sau o persoana împuternicita.

Cu toate acestea, atunci când acționeaza în calitate de persoana împuternicita (și nu operator) de date cu caracter personal din UE, entitațile din UE nu pot utiliza CCS, deoarece Comisia Europeana nu a emis CCS aprobate pentru persoana împuternicita - persoana împuternicita. Un mecanism diferit va trebui utilizat în acest scenariu.

Reguli Corporatiste Obligatorii (“RCO”)

Regulile corporatiste obligatorii sunt reguli interne pentru transferul de date în cadrul companiilor multinaționale. Regulile obligatorii ale întreprinderilor sunt ca un cod de conduita, permițând companiilor multinaționale sa transfere datele cu caracter personal la nivel internațional în cadrul aceluiași grup de companii în țari care nu ofera un nivel adecvat de protecție (cum ar fi cazul țarilor care nu aparțin UE/SEE).

Regulile corporatiste obligatorii garanteaza ca toate transferurile de date din cadrul unui grup corporativ sunt sigure. Astfel, datele cu caracter personal din UE pot fi transferate în mod liber unei organizații care a obținut aprobarea RCO de la autoritațile relevante de protecție a datelor. Cu toate acestea, exista un numar limitat de companii (aproximativ 50 - lista fiind disponibila la adresa *https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en*) care au obținut aprobarea de catre autoritațile de supraveghere a protecției datelor din UE.

Decizie de adecvare EU

Comisia Europeana are competența de a determina, pe baza articolului 45 din Regulamentul (UE) 2016/679, daca o țara din afara UE ofera un nivel adecvat de protecție a datelor. Daca Comisia Europeana emite o decizie oficiala de adecvare care sa concluzioneze ca regimul britanic de protecție a datelor ofera un nivel de protecție "echivalent în esența" cu cel furnizat în UE, aceasta ar însemna ca datele cu caracter personal din UE ar putea circula liber între UE/SEE și Regatul Unit. Cu toate acestea, Comisia Europeana a afirmat anterior ca o decizie de adecvare nu poate fi luata pâna când Marea Britanie nu parasește UE.

În conformitate cu intențiile guvernului britanic, Regulamentul General privind Protecția Datelor (GDPR) va fi introdus în legislația britanica, iar Comisarul pentru Informații (ICO) va ramâne autoritatea independenta de supraveghere a Regatului Unit privind protecția datelor. Daca se va întâmpla acest lucru, nu vor exista preocupari semnificative și este probabil sa se adopte o decizie de adecvare, deși procesul nu va fi unul rapid.

Derogari

Daca nu se poate utiliza niciuna din opțiunile de mai sus, se pot invoca o serie de derogari, sub rezerva diferitelor condiții și limitari prevazute în GDPR, inclusiv: acordul explicit al persoanei vizate; daca transferul este necesar pentru executia unui contract între persoana vizata și operator; daca transferul este necesar din motive importante de interes public; daca transferul este necesar pentru constatarea, exercitarea sau apararea unui drept în justiție; daca transferul este necesar pentru a proteja interesele vitale ale persoanei vizate sau daca este vorba de un transfer singular și exista un interes legitim determinant.

II. Desemnarea unui Reprezentant pentru Protecția Datelor în UE

Daca sunteți un operator sau o persoana împuternicita de un operator din Regatul Unit, care nu este stabilit în SEE și daca oferiți bunuri sau servicii persoanelor vizate din UE sau organizația dvs. monitorizeaza comportamentul persoanelor vizate din UE, Art. 27 GDPR va obliga sa desemnați in scris un reprezentant în Uniune ca punct de contact pentru clienți și autoritați cu privire la problemele de protecție a datelor.

§ CEPD a clarificat ca acest reprezentant în UE nu poate fi un Responsabil cu Protecția Datelor sau una din persoanele împuternicite de dvs. pentru prelucrarea datelor.

§ Datele de contact ale Reprezentantului în UE trebuie incluse în notificarile privind confidențialitatea datelor.

§ Datele de contact ale Reprezentantului în UE trebuie comunicate autoritații naționale de protecție a datelor.

Voicu Filipescu poate acționa ca reprezentant în Uniune al organizațiilor care nu au sediul în UE, potrivit art. 27 GDPR, urmând sa asigure, în baza unui mandat scris, servicii de reprezentare în chestiuni de protecția datelor.

III. Actualizarea notificarilor de confidențialitate

Ar trebui sa va revizuiți și actualizați documentele de informații privind confidențialitatea datelor pentru a înțelege mai bine fluxurile de date și a marca zonele cu referire la UE pentru a va pregati pentru schimbari.

Grupul nostru de practica pentru protecția datelor și confidențialitate va fi gata și disponibil în cazul în care este necesara asistența cu oricare dintre acțiunile menționate în acest articol. Va rugam, în acest caz, sa contactați echipa **Voicu & Filipescu** de protecție a datelor.

** Informațiile furnizate în acest document au caracter general și nu reprezinta consultanța juridica pentru*

analizarea și soluționarea unei probleme juridice specifice. Daca aveți întrebari specifice cu privire la o anumita situație, va rugam sa consultați echipa noastra de Protecția Datelor cu privire la faptele și legile care se aplica.