GRUPUL DE LUCRU PENTRU PROTECŢIA DATELOR
INSTITUIT ÎN TEMEIUL ARTICOLULUI 29

16/RO
WP 244 rev.01

Ghid pentru stabilirea autorității de supraveghere principale a operatorului sau a persoanei împuternicite de operator

Adoptat la 13 decembrie 2016
Revizuit și adoptat la 05 aprilie 2017

Cuprins

1. Stabilirea unei autorități de supraveghere principale: concepte cheie.

1.1 ”Prelucrarea transfrontalieră a datelor cu caracter personal”

Stabilirea unei autorități de supraveghere principale este importantă doar în cazul în care un operator sau o persoană împuternicită de operator efectuează prelucrări transfrontaliere de date cu caracter personal. Articolul 4(23) din Regulamentul general privind protecția datelor (RGPD) definește „prelucrarea transfrontalieră” fie ca

- *prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau*

- *prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre.*

Acest lucru înseamnă că, în cazul în care o organizație are sedii în Franța și România, de exemplu, iar prelucrarea datelor cu caracter personal se efectuează în contextul activităților proprii, atunci aceasta constituie prelucrare transfrontalieră.

În mod alternativ, organizația poate efectua activități de prelucrare a datelor doar în cadrul sediului său din Franța. Cu toate acestea, dacă activitatea afectează în mod semnificativ – ori este susceptibilă să afecteze în mod semnificativ – persoane vizate din Franța și România, atunci aceasta constituie de asemenea prelucrare transfrontalieră.

1.1.1 ”Afectează în mod semnificativ”

RGPD nu definește ”în mod semnificativ” sau ”afectează”. Intenția în formularea textului a fost aceea de a se asigura că nu orice activitate de prelucrare, cu *orice* efect și care care loc în cadrul unui singur sediu, se încadrează în definiția ”prelucrării transfrontaliere”.

Cele mai relevante sensuri în limba engleză pentru ”semnificativ” includ: ”de valoare sau dimensiune amplă ori considerabilă; însemnat, destul de mare”, sau ”având semnificație ori valoare majoră, de reală semnificație; solid; greu, important“ (Dicționar Englez Oxford).

Cel mai relevant sens al verbului ”afectează” este ”a influența” sau ”a face o impresie concretă asupra”. Substantivul înrudit - ”efect” - semnifică, printre altele, ”un rezultat” sau ”o consecință” (Dicționar Englez Oxford). Aceasta sugerează că, pentru ca o prelucrare de date să *afecteze* pe cineva, trebuie să aibă o anumită formă de impact asupra sa. Prelucrarea care nu are un efect semnificativ asupra persoanelor fizice nu se încadrează în cea de-a doua parte a definiției ”prelucrării transfrontaliere”. Cu toate acestea, s-ar încadra în prima parte a definiției cazul în care prelucrarea datelor cu caracter personal are loc în contextul activităților sediilor din cel puțin două state membre aparținând unui operator sau unei persoane împuternicite de operator pe teritoriul Uniunii, atunci când operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre.
Prelucrarea poate fi încadrată în partea a doua a definiției dacă există probabilitatea unui efect semnificativ, nu doar a unui efect semnificativ concret. Rețineți că ”probabil” nu înseamnă că

există o posibilitate îndepărtată a unui efect semnificativ. Efectul semnificativ trebuie să fie mai mult decât probabil. Pe de altă parte, aceasta înseamnă, de asemenea, că persoanele fizice nu trebuie să fie realmente afectate: probabilitatea unui efect semnificativ este suficientă pentru a încadra prelucrarea în cadrul definiției ”prelucrării transfrontaliere”.

Faptul că o operațiune de prelucrare a datelor poate implica prelucrarea unui număr – chiar a unui număr mare – de date cu caracter personal ale persoanelor fizice, în mai multe state membre, nu înseamnă neapărat că prelucrarea are, sau este susceptibilă de a avea, un efect semnificativ. Prelucrarea care nu are un efect semnificativ nu constituie prelucrare transfrontalieră în sensul celei de a doua părți a definiției, indiferent de cât de multe persoane fizice afectează.

Autoritățile de supraveghere vor interpreta ”afectează în mod semnificativ” de la caz la caz. Vom lua în considerare contextul prelucrării, tipul de date, scopul prelucrării și factori, cum ar fi, dacă prelucrarea:

- provoacă, sau este de natură să provoace, distrugerea, pierderea sau disconfortul persoanelor fizice;
- are, sau este susceptibilă de a avea, un efect real în sensul restrângerii drepturilor sau refuzării unei oportunități;
- afectează, sau este susceptibilă să afecteze, sănătatea persoanelor fizice, bunăstarea sau liniștea mentală;
- afectează, sau este susceptibilă să afecteze, statutul sau circumstanțele financiare sau economice ale persoanelor fizice;
- permite ca persoanele fizice să fie vulnerabile la discriminare sau tratament inechitabil;
- implică analizarea unor categorii de date cu caracter special sau a altor date intrusive, în special a datelor personale ale copiilor;
- provoacă, sau este de natură să provoace, modificarea comportamentului persoanelor fizice în mod semnificativ;
- are consecințe improbabile, neprevăzute sau nedorite pentru persoanele fizice;
- creează un sentiment de jenă sau alte efecte negative, inclusiv prejudiciu reputațional; sau
- implică prelucrarea unei game largi de date cu caracter personal.

În cele din urmă, testul ”efectului semnificativ” este destinat să asigure că autoritățile de supraveghere trebuie să coopereze în mod oficial doar prin intermediului mecanismului pentru asigurarea coerenței instituit de RGPD ” *în cazul în care o autoritate de supraveghere intenționează să adopte o măsură prevăzută a produce efecte juridice în ceea ce privește operațiunile de prelucrare care afectează în mod substanțial un număr semnificativ de persoane vizate din mai multe state membre*”. (*Considerentul 135*)

1.2 Autoritatea de supraveghere principală

Simplu spus, o ”autoritate de supraveghere principală” este autoritatea care are responsabilitatea principală în activitatea de prelucrare transfrontalieră a datelor, de exemplu în cazul în care o persoană vizată depune o plângere referitoare la prelucrarea datelor sale personale.

Autoritatea de supraveghere principală va coordona orice investigație, implicând alte autorități de supraveghere ”vizate”.

Stabilirea autorității de supraveghere principale depinde de identificarea locației ”sediului principal” sau a ”sediului unic” al operatorului, pe teritoriul UE. Articolul 56 al RGPD prevede că:

- *autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală pentru prelucrarea transfrontalieră efectuată de respectivul operator sau respectiva persoană împuternicită în conformitate cu procedura prevăzută la articolul 60.*

1.3 Sediul principal

Articolul 4(16) din RGPD prevede că ”sediu principal” înseamnă:

- *în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află* ***administrația centrală*** *a acestuia în Uniune, cu excepția cazului în care* ***deciziile privind scopurile și mijloacele*** *de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are* ***competența de a dispune punerea în aplicare a acestor decizii****, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;*

- *în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament.*

2. Etapele stabilirii autorității de supraveghere principale

2.1 Identificarea ”sediului principal” pentru operatori

Pentru a stabili unde se află sediul principal, este necesar în primul rând să stabilim administrația centrală a operatorului de date pe teritoriul UE, dacă este cazul.[1] Abordarea implicită în RGPD este aceea că administrația centrală pe teritoriul UE este locul în care se iau decizii cu privire la scopurile și mijloacele de prelucrare a datelor cu caracter personal și care are competența de a dispune punerea în aplicare a acestor decizii.

Esența autorității de supraveghere principale în RGPD este că supravegherea prelucrării transfrontaliere ar trebui să fie în sarcina unei singure autorități de supraveghere pe teritoriul UE. În cazurile în care deciziile privind diferitele activități de prelucrare transfrontalieră sunt

[1] RGPD este relevant pentru ZEE și va fi aplicabil după includerea sa în Acordul ZEE. RGPD este în prezent în curs de examinare pentru includere, a se vedea http://www.efta.int/eea-lex/32016R0679

luate în cadrul administrației centrale pe teritoriul UE, va fi o singură autoritate de supraveghere principală pentru diversele activități de prelucrare a datelor efectuate de compania multinațională. Cu toate acestea, ar putea fi situații în care un sediu, altul decât locul administrației centrale, să ia decizii autonome privind scopurile și mijloacele unei activități specifice de prelucrare. Aceasta înseamnă că pot exista situații în care s-ar putea stabili cel puțin două autorități de supraveghere principale, de exemplu în cazurile în care o companie multinațională decide să aibă centre de luare a deciziilor diferite, în țări diferite, pentru activități de prelucrare diferite.

Trebuie reamintit că, în cazul în care o companie multinațională centralizează toate deciziile referitoare la scopurile și mijloacele pentru activitățile de prelucrare desfășurate într-unul din sediile sale pe teritoriul UE (iar acest sediu are competența de a dispune punerea în aplicare a acestor decizii), doar o singură autoritate de supraveghere principală va fi identificată pentru multinațională.

În astfel de situații va fi esențial pentru companii să stabilească cu precizie unde se iau deciziile privind scopul și mijloacele prelucrării. Stabilirea corectă a sediului principal este în interesul operatorilor și al persoanelor împuternicite de operator, deoarece aceasta conferă claritate în privința autorității de supraveghere căreia trebuie să i se adreseze pentru respectarea diverselor responsabilități prevăzute de RGPD. Aceasta poate include, dacă este cazul, desemnarea unui responsabil cu protecția datelor sau consultarea pentru o activitate de prelucrare cu risc pe care operatorul nu o poate diminua prin mijloace rezonabile. Prevederile relevante ale RGPD sunt menite să facă aceste responsabilități ușor de gestionat.

Exemplele de mai jos ilustrează acest lucru:

Exemplul 1: Un distribuitor de produse alimentare are sediul principal (adică ”locul administrației centrale”) în Rotterdam, Olanda. Acesta are sedii în diferite alte state UE, care sunt în legătură cu persoane fizice de acolo. Toate sediile utilizează același software pentru a prelucra datele personale ale consumatorilor în scopuri de marketing. Toate deciziile privind scopurile și mijloacele de prelucrare a datelor personale ale consumatorilor în scopuri de marketing se iau în cadrul sediului principal din Rotterdam. Aceasta înseamnă, în cazul companiei, că autoritatea de supraveghere principală pentru această activitate de prelucrare transfrontalieră este autoritatea de supraveghere din Olanda.

Exemplul 2: O bancă are sediul principal al corporației în Frankfurt și toate[2] activitățile sale de prelucrări bancare sunt organizate de acolo, dar departamentul său de asigurări este situat în Viena. Dacă sediul din Viena are competența de a decide asupra întregii activități de prelucrare a datelor în scopuri de asigurări și de a dispune punerea în aplicare a acestor decizii pentru întreg teritoriul UE, atunci, așa cum prevede Art. 4(16) al RGPD, autoritatea de supraveghere din Austria va fi autoritatea principală privind prelucrările transfrontaliere de date cu caracter personal în scopuri de asigurări, iar autoritățile germane (autoritatea de supraveghere din Hessen) vor supraveghea prelucrarea datelor cu caracter personal în scopuri bancare, indiferent unde se află clienții.[3]

[2] În contextul prelucrării datelor personale în scopuri bancare, admitem că sunt implicate numeroase activități de prelucrare diferite. Cu toate acestea, pentru a simplifica lucrurile, le vom aborda pe toate ca fiind un singur scop. Aceeași situație este valabilă și în cazul prelucrării datelor în scopuri de asigurări.

[3] Trebuie reamintit, de asemenea, că RGPD prevede posibilitatea supravegherii la nivel local în anumite situații. A se vedea Considerentul (127): ”*Fiecare autoritate de supraveghere* ***care nu acționează ca*** *autoritate de*

2.1.1 Criterii de stabilire a sediului principal al unui operator în cazurile în care administrația sa centrală nu se află pe teritoriul UE

Considerentul 36 al RGPD este util în clarificarea factorului principal care va fi utilizat pentru a stabili sediul principal al operatorului în cazul în care criteriul administrației centrale nu se aplică. Acest lucru implică identificarea locului în care se exercită efectiv și real activitățile de management, care stabilesc deciziile principale privind scopurile și mijloacele de prelucrare prin acorduri stabile. Considerentul 36 clarifică, de asemenea, că ”prezența și utilizarea mijloacelor tehnice și a tehnologiilor de prelucrare a datelor cu caracter personal sau activitățile de prelucrare nu constituie un sediu principal și, prin urmare, nu sunt criteriul determinant în acest sens”.

Operatorul însuși stabilește locul unde se află sediul său principal și, în consecință, care este autoritatea de supraveghere principală. Totuși, acest lucru poate fi ulterior contestat de respectiva autoritate de supraveghere vizată.

Factorii de mai jos sunt utili pentru stabilirea locației sediului principal al unui operator, în conformitate cu prevederile RGPD, în cazurile în care aceasta nu este locația administrației sale centrale în UE.

- Unde primesc ”semnătura finală” deciziile privind scopurile și mijloacele de prelucrare?
- Unde sunt emise deciziile privind activitățile comerciale care implică prelucrarea datelor?
- Unde există competența de a avea decizii puse în aplicare în mod eficient?
- Unde se află Directorul (sau Directorii) cu responsabilitatea generală de management pentru prelucrarea transfrontalieră?
- Unde este înregistrat ca și companie operatorul sau persoana împuternicită de operator, în cazul în care se află pe teritoriul unui singur stat?

Rețineți că aceasta nu este o listă exhaustivă. Alți factori pot fi relevanți în funcție de operatorul sau activitatea de prelucrare în cauză. În cazul în care o autoritate de supraveghere are motive să se îndoiască de faptul că sediul identificat de operator este, în realitate, sediul principal, în sensul RGPD, aceasta poate – bineînțeles – să solicite operatorului furnizarea de informații suplimentare necesare pentru a dovedi unde este situat sediul său principal.

2.1.2 Grupurile de întreprinderi

În cazul în care prelucrarea este efectuată de un grup de întreprinderi cu sediul în UE, sediul întreprinderii care deține control general este prezumat a fi centrul de luare a deciziilor referitoare la prelucrarea datelor personale și, prin urmare, va fi considerat sediul principal pentru grup, exceptând situația în care deciziile privind scopurile și mijloacele prelucrării

---

*supraveghere **principală ar trebui să aibă competența de a trata cazuri locale**, în care operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre, dar obiectul respectivei prelucrări privește **doar prelucrarea efectuată într-un singur stat membru și implicând doar persoane vizate din acel unic stat membru**, de exemplu în cazul în care obiectul îl constituie prelucrarea datelor cu caracter personal ale angajaților în contextul specific legat de forța de muncă dintr-un stat membru*.” Acest principiu înseamnă că supravegherea datelor RU referitoare la contextul legat de forța de muncă la nivel local ar putea intra sub incidența mai multor autorități de supraveghere.

sunt luate de un alt sediu. Este posibil ca sediul principal să fie compania-mamă sau sediul operațional al grupului de întreprinderi din UE, deoarece acesta ar fi locul în care se află administrația sa centrală.

Referirea în definiție la locul administrației centrale a operatorului funcționează bine pentru organizațiile care au un sediu centralizat de luare a deciziilor sau structură de tip-sucursală. În astfel de cazuri este evident că competența de a lua decizii privind prelucrarea transfrontalieră de date și de a dispune punerea lor în aplicare este în cadrul sediului central al companiei. În asemenea situații, stabilirea locației sediului principal – și, prin urmare, a autorității de supraveghere principale – este facilă. Cu toate acestea, sistemul decizional al grupului de companii ar putea fi mai complex, conferind diverselor sedii independență în competențele de luare a deciziilor referitoare la prelucrarea transfrontalieră. Criteriile stabilite mai sus ar trebui să ajute grupul de întreprinderi în stabilirea sediului lor principal.

2.1.3 Operatori asociați

RGPD nu tratează în mod special problema desemnării unei autorități principale în cazul în care doi sau mai mulți operatori din UE stabilesc în comun scopurile și mijloacele de prelucrare – de ex. operatori asociați. Articolul 26(1) și Considerentul 79 precizează expres că, în situațiile operatorilor asociați, operatorii trebuie să stabilească în mod transparent responsabilitățile fiecăruia dintre ei, în îndeplinirea obligațiilor care le revin în temeiul Regulamentului. Prin urmare, pentru a beneficia de principiul ghișeului unic, operatorii asociați trebuie să stabilească (dintre sediile în care se iau deciziile) sediul operatorilor asociați care va avea competența de a dispune implementarea deciziilor referitoare la prelucrare cu privire la toți operatorii asociați. Acest sediu va fi considerat ca fiind sediul principal pentru prelucrarea efectuată în cazul operatorilor asociați. Acordul dintre operatorii asociați nu aduce atingere dispozițiilor cu privire la răspundere stipulate în RGPD, în special la Articolul 82(4).

2.2 Cazuri limită

Vor exista situații limită și complexe, în care este dificilă stabilirea sediului principal sau a locului în care sunt luate deciziile privind prelucrarea datelor. Acesta ar putea fi cazul în care se desfășoară activitate de prelucrări transfrontaliere și operatorul este stabilit în mai multe state membre, dar administrația centrală nu este în UE și niciunul dintre sediile din UE nu ia decizii cu privire la prelucrare (de ex. deciziile sunt luate exclusiv în afara UE).

În cazul de mai sus, compania care efectuează prelucrări transfrontaliere poate dori să fie reglementată de o autoritate principală pentru a beneficia de principiul ghișeului unic. Însă RGPD nu oferă o soluție pentru astfel de cazuri. În aceste condiții, compania ar trebui să stabilească sediul care are autoritatea de a implementa deciziile privind activitatea de prelucrare și de a-și asuma răspunderea pentru prelucrare, având inclusiv suficiente active, precum sediul principal. Dacă respectiva companie nu desemnează un sediu principal în acest fel, nu va fi posibilă desemnarea unei autorități principale. Autoritățile de supraveghere vor fi întotdeauna în măsură să investigheze în continuare, acolo unde este cazul.

RGPD nu permite ”forum shopping”. Dacă o companie pretinde că are sediul principal într-un stat membru, dar nici exercitarea reală și efectivă a activității de management, nici luarea deciziilor privind prelucrarea datelor personale nu au loc acolo, autoritățile de supraveghere competente (sau EDPB în cele din urmă) vor decide care autoritate de supraveghere este

”principala”, utilizând criterii obiective și analizând probele. Procesul de stabilire a sediului principal poate necesita o cercetare activă și cooperare între autoritățile de supraveghere. Concluziile nu pot fi bazate doar pe declarațiile organizației aflate în curs de examinare. Sarcina dovedirii revine în cele din urmă operatorilor și persoanelor împuternicite de aceștia pentru a demonstra autorităților de supraveghere competente unde se iau deciziile relevante privind prelucrarea și unde există competența de a implementa astfel de decizii. Evidențele efective ale activității de prelucrare a datelor vor ajuta atât organizațiile, cât și autoritățile de supraveghere să stabilească autoritatea principală. Autoritatea principală de supraveghere sau autoritățile vizate pot respinge analiza operatorului în baza unei examinări obiective a faptelor relevante, solicitând informații suplimentare dacă este necesar.

În anumite cazuri, autoritățile de supraveghere competente vor solicita operatorului să furnizeze dovezi clare, în conformitate cu orice ghiduri ale EDPB, privind locul sediului său principal sau cel în care se iau deciziile privind o anumită activitate de prelucrare a datelor. Acestor probe li se va acorda importanța cuvenită și autoritățile de supraveghere implicate vor coopera pentru a decide care dintre ele va prelua conducerea în cadrul investigațiilor. Astfel de cazuri vor fi înaintate către EDPB pentru adoptarea unei decizii în temeiul Articolului 65(1)(b) numai atunci când autoritățile de supraveghere au opinii divergente cu privire la stabilirea autorității de supraveghere principale. Cu toate acestea, în majoritatea cazurilor, este de așteptat ca autoritățile de supraveghere competente să fie în măsură să convină asupra unui curs al acțiunii reciproc satisfăcător.

2.3 Persoana împuternicită de operator

RGPD oferă, de asemenea, un sistem de ghișeu unic în beneficiul persoanelor împuternicite de operator care intră sub incidența RGPD și care au sedii în cel puțin două state membre.

Articolul 4(16)(b) al RGPD stipulează că sediul principal al persoanei împuternicite de operator va fi locul administrației centrale a persoanei împuternicite de operator în UE sau, dacă aceasta nu are administrația centrală în UE, sediul din UE în care au loc activitățile principale de prelucrare.

Cu toate acestea, potrivit Considerentului 36, în cazurile care implică atât operatorul, cât și persoana împuternicită de operator, autoritatea de supraveghere principală competentă ar trebui să fie autoritatea de supraveghere principală pentru operator. În această situație, autoritatea de supraveghere a persoanei împuternicite va fi o ”autoritate de supraveghere vizată” și ar trebui să participe la procedura de cooperare. Această regulă se va aplica doar în cazul în care operatorul are sediul în UE. În cazurile în care operatorilor li se aplică RGPD conform Articolului 3(2), acestora nu li se aplică mecanismul ghișeului unic. O persoană împuternicită de operator poate furniza servicii mai multor operatori situați în diferite state membre – de exemplu, un important furnizor de servicii cloud. În astfel de cazuri, autoritatea de supraveghere principală va fi autoritatea de supraveghere care este competentă să acționeze ca autoritate principală pentru operator. Aceasta înseamnă, de fapt, că o persoană împuternicită de operator poate avea de a face cu mai multe autorități.

3. Alte aspecte relevante

3.1 Rolul ”autorității de supraveghere vizate”

Articolul 4(22) al RGPD prevede că:

„autoritate de supraveghere vizată" înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece: (a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective; (b) persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau (c) la autoritatea de supraveghere respectivă a fost depusă o plângere.

Conceptul de autoritate de supraveghere vizată este menit să asigure că "autoritatea principală" tip nu exclude alte autorități de supraveghere care au un cuvânt de spus privind modul în care este tratată o problemă, spre exemplu, în cazul în care persoanele vizate care au reședința în afara jurisdicției autorității principale sunt afectate în mod substanțial de o activitate de prelucrare a datelor. Referitor la punctul a) de mai sus, se aplică aceleași considerații ca și în cazul stabilirii autorității principale. La punctul b) rețineți că persoana vizată trebuie pur și simplu să locuiască în statul membru în cauză; el sau ea nu trebuie să fie cetățean al acelui stat. La punctul c) va fi în general ușor de stabilit – în fapt – dacă o anumită autoritate de supraveghere a primit o plângere.

Articolul 56, prin paragrafele (2) și (5), din RGPD prevede că autoritatea de supraveghere vizată contribuie la soluționarea unui caz fără să fie autoritate de supraveghere principală. Atunci când o autoritate de supraveghere principală decide să nu trateze un caz, autoritatea de supraveghere vizată care a informat autoritatea de supraveghere principală trebuie să trateze cazul. Acest lucru este în conformitate cu procedurile prevăzute la Articolul 61 (Asistență reciprocă) și Articolul 62 (Operațiuni comune ale autorităților de supraveghere) din RGPD. Acesta ar putea fi cazul în care o companie de marketing cu sediul principal în Paris lansează un produs care afectează doar persoanele vizate care locuiesc în Portugalia. Într-o asemenea situație, autoritățile de supraveghere din Franța și Portugalia ar putea conveni că este oportun ca autoritatea de supraveghere din Portugalia să preia conducerea în tratarea cazului. Autoritățile de supraveghere pot solicita operatorilor de date să furnizeze informații pentru a clarifica acordurile corporației. Având în vedere că activitatea de prelucrare are un efect pur local – în speță asupra persoanelor fizice din Portugalia – autoritățile de supraveghere din Franța și Portugalia au libertatea de a decide care autoritate de supraveghere trebuie să se ocupe de caz – în conformitate cu Considerentul 127.

RGPD solicită autorității de supraveghere principale și autorităților de supraveghere vizate să coopereze, respectându-și reciproc opiniile, să se asigure că un caz este investigat și soluționat ținând cont de așteptările fiecărei autorități – și cu o soluție eficientă pentru persoanele vizate. Autoritățile de supraveghere ar trebui să depună eforturi pentru a ajunge la un mod de acțiune reciproc acceptabil. Mecanismul oficial pentru asigurarea coerenței ar trebui invocat numai în cazul în care cooperarea nu atinge un rezultat reciproc acceptabil.

Acceptarea reciprocă a deciziilor se poate aplica concluziilor individuale, dar și modului de acțiune asupra căruia s-a hotărât, inclusiv activității de sancționare (spre ex. investigație completă sau investigație cu obiect limitat). De asemenea, se poate aplica unei decizii de a nu trata un caz în conformitate cu RGPD, spre exemplu datorită unei politici oficiale de stabilire a priorităților sau datorită faptului că există alte autorități vizate, așa cum s-a descris mai sus.

Dezvoltarea consensului și a bunăvoinței între autoritățile de supraveghere este esențială pentru procesul de cooperare și asigurare a coerenței în conformitate cu prevederile RGPD.

3.2 Prelucrarea la nivel local

Activitatea de prelucrare a datelor la nivel local nu intră sub incidența prevederilor RGPD privind cooperarea și asigurarea coerenței. Autoritățile de supraveghere își vor respecta reciproc competențele în ceea ce privește activitatea de prelucrare a datelor la nivel local. Prelucrările efectuate de autoritățile publice vor fi întotdeauna analizate și la nivel local.

3.3 Companiile care nu au sediul pe teritoriul UE

Mecanismul de cooperare și asigurare a coerenței prevăzut de RGPD se aplică doar operatorilor care au un sediu, sau mai multe sedii, pe teritoriul Uniunii Europene. În cazul în care compania nu are un sediu în UE, simpla prezență a unui reprezentant într-un stat membru nu declanșează mecanismul ghișeului unic. Aceasta înseamnă că operatorii care nu au niciun sediu în UE trebuie să colaboreze cu autoritățile de supraveghere de la nivel local, în fiecare stat membru în care își desfășoară activitatea, prin intemediul reprezentantului lor local.

Adoptat la Bruxelles, la 13 decembrie 2016

Pentru Grupul de Lucru,
Președinte
Isabelle FALQUE-PIERROTIN

Revizuit și adoptat la 5 aprilie 2017

Pentru Grupul de Lucru,
Președinte
Isabelle FALQUE-PIERROTIN

ANEXĂ – Întrebări care să conducă la stabilirea autorității de supraveghere principale

1. Operatorul sau persoana împuternicită de operator efectuează prelucrări transfrontaliere de date cu caracter personal?

a. Da, dacă:

- operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre și
- prelucrarea datelor cu caracter personal are loc în contextul activităților sediilor din cel puțin două state membre.

➢ În acest caz, a se vedea secțiunea 2.

b. Da, dacă:

- prelucrarea datelor cu caracter personal are loc în contextul activităților sediului unic din UE al unui operator sau al unei persoane împuternicite de operator, dar
- afectează în mod semnificativ sau este susceptibilă să afecteze în mod semnificativ persoanele fizice din cel puțin două state membre.

➢ În acest caz, autoritatea principală este autoritatea sediului unic al operatorului sau al persoanei împuternicite de operator într-un singur stat membru. Acesta trebuie să fie – în mod logic – sediul principal al operatorului sau al persoanei împuternicite de operator, deoarece este unic sediu al acestuia/acesteia.

2. Cum se stabilește ”autoritatea de supraveghere principală”

a. Într-un caz care implică doar un operator:

i. Stabilirea locului administrației centrale a operatorului în UE;

ii. Autoritatea de supraveghere a statului în care se află locul administrației centrale este autoritatea principală a operatorului.

Cu toate acestea:

iii. Dacă deciziile privind scopurile și mijloacele de prelucrare se iau într-un alt sediu din UE, iar acest sediu are competența de a dispune punerea în aplicare a acestor decizii, atunci autoritatea principală este cea din statul în care se află acest sediu.

b. Într-un caz care implică un operator și o persoană împuternicită de operator:

i. Se verifică dacă operatorul are sediul în UE și dacă i se aplică mecanismul ghișeului unic. În caz afirmativ,

ii. Se stabilește autoritatea de supraveghere principală a operatorului. Această autoritate va fi autoritatea de supraveghere principală și pentru persoana împuternicită de operator.

iii. Autoritatea de supraveghere (ne-principală) competentă a persoanei împuternicite de operator va fi o ”autoritate vizată” – a se vedea secțiunea 3.

c. Într-un caz care implică doar o persoană împuternicită de operator:

i. Se stabilește locul administrației centrale a persoanei împuternicite de operator în UE;

ii. Dacă persoana împuternicită de operator nu are administrația centrală în UE, se stabilește sediul din UE în care persoana împuternicită de operator efectuează principalele activități de prelucrare.

d. Într-un caz care implică operatori asociați:

i. Se verifică dacă operatorii asociați au sediul în UE.

ii. Se stabilește, dintre sediile în care se iau deciziile privind scopurile și mijloacele de prelucrare, sediul care are competența de a pune în aplicare aceste decizii luând în considerare toți operatorii asociați. Prin urmare, acest sediu va fi considerat sediul principal pentru prelucrările efectuate de operatorii asociați. Autoritatea principală este cea din statul în care se află acest sediu.

3. Există vreo ”autoritate de supraveghere vizată”?

O autoritate este ”autoritate vizată”:

- atunci când operatorul sau persoana împuternicită de operator are un sediu pe teritoriul său, sau:

- atunci când persoanele vizate de pe teritoriul său sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare, sau:

- atunci când o plângere este primită de o anumită autoritate.