DECIZIE nr. 174 din 18 octombrie 2018privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal
EMITENT • AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL
Publicat în MONITORUL OFICIAL nr. 919 din 31 octombrie 2018
Având în vedere necesitatea asigurării unei protecţii eficiente a drepturilor persoanelor ale căror date cu caracter personal sunt supuse prelucrării, în special în cazul anumitor operaţiuni de prelucrare a datelor cu caracter personal care prezintă riscuri pentru drepturile şi libertăţile persoanelor, datorită naturii datelor prelucrate, scopului prelucrării, caracterului specific al categoriilor de persoane vizate sau mecanismelor utilizate pentru prelucrarea datelor,
ţinând cont de art. 35 alin. (1) din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE, denumit în continuare Regulamentul general privind protecţia datelor, care prevede că, având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal.
Având în vedere prevederile art. 35 alin. (3) din Regulamentul general privind protecţia datelor, referitoare la cazurile în care se impune, în mod special, evaluarea impactului asupra protecţiei datelor,
luând în considerare art. 35 alin. (4) din Regulamentul general privind protecţia datelor, care prevede că autoritatea de supraveghere întocmeşte şi publică o listă a tipurilor de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor, pe care o comunică Comitetului european pentru protecţia datelor, coroborat cu art. 35 alin. (6) din Regulamentul general privind protecţia datelor,
având în vedere art. 35 alin. (10) din Regulamentul general privind protecţia datelor, care prevede că atunci când prelucrarea în temeiul art. 6 alin. (1) litera c) sau e) din acelaşi regulament are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidenţa căruia intră operatorul, iar dreptul respectiv reglementează operaţiunea de prelucrare specifică sau setul de operaţiuni specifice în cauză şi deja s-a efectuat o evaluare a impactului asupra protecţiei datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, art. 35 alin. (1)-(7) din Regulamentul general privind protecţia datelor nu se aplică, cu excepţia cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităţilor de prelucrare.
Ţinând cont de art. 35 alin. (11) din Regulamentul general privind protecţia datelor, care prevede că, acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecţiei datelor, cel puţin atunci când are loc o modificare a riscului reprezentat de operaţiunile de prelucrare,
luând în considerare art. 63 din Regulamentul general privind protecţia datelor, care prevede că, pentru a contribui la aplicarea coerentă a regulamentului în întreaga Uniune, autorităţile de supraveghere cooperează între ele şi, după caz, cu Comisia prin mecanismul pentru asigurarea coerenţei,
ţinând cont de art. 64 alin. (1) lit. a) din Regulamentul general privind protecţia datelor, potrivit căruia Comitetul european pentru protecţia datelor emite un aviz de fiecare dată când o autoritate de supraveghere competentă intenţionează să adopte lista de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor,
având în vedere considerentul (71) al Regulamentului general privind protecţia datelor, persoana vizată ar trebui să aibă dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea automată şi care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronică, fără intervenţie umană. O astfel de prelucrare include „crearea de profiluri", care constă în orice formă de prelucrare automată a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situaţia economică, starea de sănătate, preferinţele sau interesele personale, fiabilitatea sau comportamentul, locaţia sau deplasările, atunci când aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrări, inclusiv crearea de profiluri, ar trebui permisă în cazul în care este autorizată în mod expres în dreptul Uniunii sau în dreptul intern care se aplică operatorului, inclusiv în scopul monitorizării şi prevenirii fraudei şi a evaziunii fiscale, desfăşurate în conformitate cu reglementările, standardele şi recomandările instituţiilor Uniunii sau ale organismelor naţionale de supraveghere, şi în scopul asigurării securităţii şi fiabilităţii unui serviciu oferit de operator sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator sau în cazul în care persoana vizată şi-a dat în mod explicit consimţământul. În orice caz, o astfel de prelucrare ar trebui să facă obiectul unor garanţii corespunzătoare, care ar trebui să includă o informare specifică a persoanei vizate şi dreptul acesteia de a obţine intervenţie umană, de a-şi exprima

punctul de vedere, de a primi o explicaţie privind decizia luată în urma unei astfel de evaluări, precum şi dreptul de a contesta decizia. O astfel de măsură nu ar trebui să se refere la un copil.
Având în vedere considerentul (75) al Regulamentului general privind protecţia datelor, potrivit căruia riscul pentru drepturile şi libertăţile persoanelor fizice, prezentând grade diferite de probabilitate de materializare şi de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identităţii, pierdere financiară, compromiterea reputaţiei, pierderea confidenţialităţii datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile şi libertăţile lor sau împiedicate să îşi exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenenţa sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viaţa sexuală sau privind condamnările penale şi infracţiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situaţia economică, starea de sănătate, preferinţele sau interesele personale, fiabilitatea sau comportamentul, locaţia sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal şi afectează un număr larg de persoane vizate,
având în vedere considerentul (84) al Regulamentului general privind protecţia datelor, potrivit căruia, pentru a favoriza respectarea dispoziţiilor prezentului regulament în cazurile în care operaţiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecţiei datelor, care să estimeze, în special, originea, natura, specificitatea şi gravitatea acestui risc. Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezentul regulament. În cazul în care o evaluare a impactului asupra protecţiei datelor arată că operaţiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile şi al costurilor implementării, ar trebui să aibă loc o consultare a autorităţii de supraveghere înainte de prelucrare.
Având în vedere considerentul (89) al Regulamentului general privind protecţia datelor, potrivit căruia Directiva 95/46/CE a prevăzut o obligaţie generală de a notifica prelucrarea datelor cu caracter personal autorităţilor de supraveghere, obligaţia respectivă, deşi generează sarcini administrative şi financiare, nu a contribuit întotdeauna la îmbunătăţirea protecţiei datelor cu caracter personal. Prin urmare, astfel de obligaţii de notificare generală nediferenţiată ar trebui să fie abrogate şi înlocuite cu proceduri şi mecanisme eficace care să pună accentul, în schimb, pe acele tipuri de operaţiuni de prelucrare susceptibile să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice prin însăşi natura lor, prin domeniul lor de aplicare, prin contextul şi prin scopurile lor. Astfel de tipuri de operaţiuni de prelucrare pot fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operaţiuni, pentru care nicio evaluare a impactului asupra protecţiei datelor nu a fost efectuată anterior de către operator ori care devin necesare dată fiind perioada de timp care s-a scurs de la prelucrarea iniţială.
Având în vedere considerentul (90) al Regulamentului general privind protecţia datelor, operatorul ar trebui să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecţiei datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat şi gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi sursele riscului. Respectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanţiile şi mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecţiei datelor cu caracter personal şi pentru demonstrarea conformităţii cu prezentul regulament.
Având în vedere considerentul (91) al Regulamentului general privind protecţia datelor, evaluarea impactului asupra protecţiei datelor ar trebui să se aplice, în special, operaţiunilor de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, naţional sau supranaţional, care ar putea afecta un număr mare de persoane vizate şi care sunt susceptibile de a genera un risc ridicat, de exemplu, din cauza sensibilităţii lor, în cazul în care, în conformitate cu nivelul atins al cunoştinţelor tehnologice, se foloseşte la scară largă o tehnologie nouă, precum şi altor operaţiuni de prelucrare care generează un risc ridicat pentru drepturile şi libertăţile persoanelor vizate, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile. Ar trebui efectuată o evaluare a impactului asupra protecţiei datelor şi în situaţiile în care datele cu caracter personal sunt prelucrate în scopul luării de decizii care vizează anumite persoane fizice în urma unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, pe baza creării de profiluri pentru datele respective, sau în urma prelucrării unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnările penale şi infracţiunile sau măsurile de securitate conexe. Este la fel de

necesară o evaluare a impactului asupra protecţiei datelor pentru monitorizarea la scară largă a zonelor accesibile publicului, mai ales în cazul utilizării dispozitivelor optoelectronice sau pentru orice alte operaţiuni în cazul în care autoritatea de supraveghere competentă consideră că prelucrarea este susceptibilă de a genera un risc ridicat pentru drepturile şi libertăţile persoanelor vizate, în special deoarece acestea împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract sau deoarece acestea sunt efectuate în mod sistematic la scară largă. Prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienţi sau clienţi de către un anumit medic, un alt profesionist în domeniul sănătăţii sau un avocat. În aceste cazuri, o evaluare a impactului asupra protecţiei datelor nu ar trebui să fie obligatorie.
Având în vedere considerentul (92) al Regulamentului general privind protecţia datelor, potrivit căruia în unele circumstanţe ar putea fi rezonabil şi util din punct de vedere economic ca o evaluare a impactului asupra protecţiei datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu, în cazul în care autorităţi sau organisme publice intenţionează să instituie o aplicaţie sau o platformă de prelucrare comună sau în cazul în care mai mulţi operatori preconizează să introducă o aplicaţie comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată la scară largă,
având în vedere considerentul (94) al Regulamentului general privind protecţia datelor, potrivit căruia, în cazul în care o evaluare a impactului asupra protecţiei datelor arată că prelucrarea ar genera, în absenţa garanţiilor, măsurilor de securitate şi mecanismelor de atenuare a riscului un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile şi al costurilor implementării, autoritatea de supraveghere ar trebui să fie consultată înainte de începerea activităţilor de prelucrare. Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum şi de amploarea şi frecvenţa prelucrării, care pot duce şi la producerea unor prejudicii sau pot atinge drepturile şi libertăţile persoanelor fizice. Autoritatea de supraveghere ar trebui să răspundă cererii de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacţii din partea autorităţii de supraveghere în termenul respectiv ar trebui să nu aducă atingere niciunei intervenţii a autorităţii de supraveghere în conformitate cu sarcinile şi competenţele sale prevăzute în prezentul regulament, inclusiv competenţa de a interzice operaţiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecţiei datelor efectuate cu privire la prelucrarea în cauză poate fi transmis autorităţii de supraveghere, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile şi libertăţile persoanelor fizice.
Având în vedere Ghidul privind evaluarea impactului asupra protecţiei datelor (DPIA) şi stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679 (WP 248, revizuit), adoptat de Grupul de lucru Articolul 29 în data de 4 octombrie 2017 şi aprobat de Comitetul European pentru Protecţia Datelor, inclusiv precizările referitoare la sintagma „pe scară largă" şi „monitorizare sistematică",
având în vedere că lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor nu are caracter exhaustiv,
luând în considerare Avizul Comitetului European pentru Protecţia Datelor nr. 19 din 25 septembrie 2018, comunicat pe data de 2 octombrie 2018, privind proiectul listei de operaţiuni pentru care este necesară realizarea evaluării impactului asupra protecţiei datelor [art. 35 alin. (4) din Regulamentul general privind protecţia datelor] întocmit de Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal,
în baza Referatului Biroului relaţii internaţionale nr. 134 din 15 octombrie 2018 cu privire la proiectul de Decizie privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor,
în temeiul prevederilor art. 3 alin. (5) şi (6) şi art. 10 alin. (1) lit. a) şi b) din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare, şi ale art. 6 alin. (2) lit. b) din Regulamentul de organizare şi funcţionare a Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, aprobat prin Hotărârea Biroului permanent al Senatului nr. 16/2005, cu modificările şi completările ulterioare,
preşedintele Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal emite prezenta decizie.

Articolul 1
(1) Evaluarea impactului asupra protecţiei datelor cu caracter personal de către operatori este obligatorie în special în următoarele cazuri:
a) prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
b) prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a

datelor cu caracter personal referitoare la condamnări penale și infracțiuni;
c) prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, piețe, parcuri sau alte asemenea spații;
d) prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor și ale angajaților, prin mijloace automate de monitorizare și/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfășurării activităților de reclamă, marketing și publicitate;
e) prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaștere facială în vederea facilitării accesului în diferite spații;
f) prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicații „Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, orașe inteligente sau alte asemenea aplicații);
g) prelucrarea pe scară largă și/sau sistematică a datelor de trafic și/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situații) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.
(2) Prin excepție de la alin. (1), evaluarea impactului asupra protecției datelor nu este obligatorie atunci când prelucrarea efectuată în temeiul art. 6 alin. (1) lit. (c) sau (e) din Regulamentul general privind protecția datelor are un temei juridic în dreptul Uniunii sau în dreptul intern și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări generale a impactului în contextul adoptării actelor normative respective.

Articolul 2

Prezenta decizie intră în vigoare la data publicării în Monitorul Oficial al României, Partea I.
Președintele Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal,
Ancuța Gianina Opre
București, 18 octombrie 2018.
Nr. 174.
