Revista Universul Juridic ● nr. 10, octombrie 2018, pp. 58-69

TEMEIUL JURIDIC AL PRELUCĂRII DATELOR CU CARACTER PERSONAL DE CĂTRE AUTORITĂȚI ŞI ORGANISME PUBLICE POTRIVIT ARTICOLULUI 6 DIN REGULAMENTUL GENERAL PRIVIND PROTECȚIA DATELOR

Silviu-Dorin ŞCHIOPU

Abstract

Any processing of personal data requires a valid legal ground. Although Romanian public authorities and bodies enjoy a privileged status, as each member state may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that member state, these public authorities and bodies are not exempted from the obligation to ensure the lawfulness of personal data processing. Therefore this article aims to present the particularities of choosing the legal grounds for data processing under article 6 of the General Data Protection Regulation in the case of public authorities and bodies mentioned by the Law no. 190 from 18th of July 2018 on implementing measures for Regulation (EU) 2016/679.

Keywords: *GDPR personal data, data processing, legal grounds, public authorities and bodies, lawfulness of processing.*

1. Considerații introductive

În aplicarea Regulamentului general privind protecția datelor (GDPR)[1], potrivit art. 2 alin. (1) lit. a) din Legea nr. 190/2018[2], prin „autorități şi organisme publice"[3]

[1] *Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016* privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicat în Jurnalul Oficial al Uniunii Europene, L 119 din 4 mai 2016.

[2] *Legea nr. 190 din 18 iulie 2018* privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicată în M. Of. nr. 651 din data de 26 iulie 2018.

[3] Practic redactorii legii au adaptat definiția *instituțiilor publice* din art. 2 pct. 30 al Legii nr. 500 din 11 iulie 2002 privind finanțele publice, publicată în M. Of. nr. 597 din data de 13 august 2002.

înțelegem Camera Deputaților şi Senatul, Administrația Prezidențială, Guvernul, ministerele, celelalte organe de specialitate ale administrației publice centrale, autoritățile şi instituțiile publice autonome, autoritățile administrației publice locale şi de la nivel județean, alte autorități publice, precum şi instituțiile din subordinea/coordonarea acestora[4].

Prelucrarea datelor cu caracter personal de către aceste autorități şi organisme publice prezintă unele particularități, nu numai în planul sancțiunilor[5], ci şi în ceea ce priveşte temeiurile juridice la care pot recurge autoritățile şi organismele publice în vederea asigurării legalității propriilor operațiuni de prelucrare. Corecta determinare a temeiului juridic al prelucrării facilitează acestor operatori de date cu caracter personal inclusiv îndeplinirea obligației de informare a persoanelor vizate prevăzută de art. 13 alin. (1) lit. c) şi art. 14 alin. (1) lit. c) GDPR. De asemenea, temeiul juridic al prelucrării poate fi inclus ca informație complementară în registrul de evidență a activităților de prelucrare reglementat în cadrul art. 30 GDPR şi care serveşte operatorului să demonstreze conformitatea activităților de prelucrare cu prevederile Regulamentului (UE) 2016/679, registrul constituind o condiție prealabilă pentru conformitate şi, în acelaşi timp, o dovadă de asumare a responsabilității prelucrării datelor cu caracter personal[6].

În cele ce urmează vom analiza situațiile în care autoritățile şi organismele publice (nu) pot recurge la temeiurile juridice prevăzute de art. 6 alin. (1) GDPR pentru a asigura legalitatea propriilor operațiuni de prelucrare a datelor cu caracter personal.

2. Consimțământul

Deşi persoana vizată îşi poate dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice[7], considerentul (42) subliniază că acesta „nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să îşi retragă consimțământul fără a fi prejudiciată".

În acest sens considerentul (43) precizează că, pentru a garanta faptul că a fost acordat în mod liber, „consimțământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care *există un dezechilibru evident între persoana vizată şi operator* (s.n.), în special în cazul

[4] Potrivit art. 2 alin. (1) lit. a) teza finală din Legea nr. 190/2018, unitățile de cult şi asociațiile şi fundațiile de utilitate publică sunt asimilate autorităților/organismelor publice.

[5] A se vedea art. 13 şi 14 din Legea nr. 190/2018.

[6] S.-D. Şchiopu, *Obligația de păstrare a evidenței activităților de prelucrare a datelor cu caracter personal*, în „Revista română de drept al afacerilor" nr. 1/2018, p. 94.

[7] Pentru detalii a se vedea D.-M. Şandru, *Elemente privind reglementarea consimțământului în prelucrarea datelor cu caracter personal, potrivit art. 6 din Regulamentul nr. 2016/679*, în „Revista română de drept al afacerilor" nr. 5/2017, p. 129-135.

în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare".

Totuşi, utilizarea consimțământului ca temei juridic pentru prelucrarea datelor de către autoritățile şi organismele publice nu este total exclusă de Regulamentul general privind protecția datelor, astfel că recurgerea la consimțământ poate fi adecvată în anumite circumstanțe. Un exemplu în acest sens este cazul în care o instituție de învățământ public aflată în subordinea Ministerului Educației Naționale solicită elevilor consimțământul de a le folosi fotografiile într-o revistă şcolară. Consimțământul în această situație poate fi o alegere reală însă numai în măsura în care elevii ar putea refuza utilizarea acestor fotografii fără nici un prejudiciu, beneficiind în continuare, în aceleaşi condiții, de activitățile şi serviciile educaționale[8]. Precizăm că Comitetul european pentru protecția datelor (CEPD)[9] şi-a însuşit această poziție[10].

La fel, autoritățile şi organismele publice, nici în situația în care prelucrează date cu caracter personal în contextul ocupării unui loc de muncă, pentru cea mai mare parte a operațiunilor de prelucrare a datelor personale „temeiul juridic nu poate şi nu ar trebui să fie consimțământul angajaților […], având în vedere natura relației dintre angajator şi angajat"[11], respectiv dezechilibrul dintre autoritatea sau organismul public şi angajații acestora.

Numai pentru o mică parte din activitățile de prelucrare operatorul va putea recurge la consimțământ ca temei juridic al prelucrării, însă numai în măsura în care autoritatea sau organismul public va putea demonstra faptul că persoana vizată (angajatul) şi-a dat consimțământul în mod liber pentru operațiunea de prelucrare, ceea se întâmplă numai în situații excepționale adică atunci când consecințele negative lipsesc cu desăvârşire indiferent dacă persoana vizată consimte sau nu la prelucrarea datelor sale.

Consimțământul poate fi valabil exprimat, de exemplu, atunci când, într-un anumit birou urmează a se turna un film iar angajatorul solicită tuturor angajaților care lucrează în zona respectivă consimțământul pentru a fi filmați întrucât aceştia pot apărea pe fundalul înregistrării video, cei care nu doresc a fi filmați urmând a primi birouri echivalente în altă parte a clădirii pe durata filmărilor, astfel că nu

[8] Pentru alte exemple a se vedea Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, WP259 rev. 01, as last Revised and Adopted on 10 April 2018, p. 6.

[9] C.E.P.D. este un organism al U.E. însărcinat cu aplicarea GDPR începând cu data de 25 mai 2018 şi are în componența sa şefii fiecărei autorități de supraveghere din statele membre U.E. sau reprezentanții acestora.

[10] A se vedea European Data Protection Board, *Endorsement 1/2018 of GDPR WP29 guidelines by the EDPB*, Brussels, 25 May 2018.

[11] Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, WP249, adopted on 8 June 2017, versiunea în limba română, p. 6.

sunt în nici un fel penalizați pentru refuzul de a consimți la prelucrarea datelor lor cu caracter personal (imaginea)[12].

Nu în ultimul rând precizăm că, potrivit considerentului (43), consimțământul este considerat a nu fi acordat în mod liber atunci când „executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului". De aceea, art. 7 alin. (4) GDPR prevede că în cazul evaluării „dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract".

Precum a subliniat şi Grupul de lucru art. 29, Regulamentul (UE) 2016/679 garantează faptul că prelucrarea datelor cu caracter personal pentru care se solicită consimțământul nu poate deveni direct sau indirect contraprestația unui contract iar cele două temeiuri juridice pentru prelucrarea legală a datelor cu caracter personal, şi anume consimțământul şi contractul, nu pot fi amalgamate şi indistincte[13]. La fel, atunci când serviciile pot fi obținute numai dacă anumite date cu caracter personal sunt comunicate operatorului sau ulterior unor terți, consimțământul persoanei vizate de a divulga datele care nu sunt necesare pentru încheierea sau executarea contractului nu poate fi considerat o decizie liberă şi, prin urmare, nu este valabil potrivit Regulamentului general privind protecția datelor[14].

3. Relația contractuală

Potrivit art. 6 alin. (1) lit. b) GDPR, autoritățile şi organismele publice pot recurge la relația contractuală ca temei juridic al prelucrării datelor cu caracter personal numai atunci când „prelucrarea este *necesară* (s.n.) pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract". Această prevedere include şi relațiile precontractuale[15] şi dezvoltă conținutul considerentului (44) potrivit căruia prelucrarea ar trebui să fie considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract. Trebuie să subliniem faptul că în cazul relațiilor precontractuale prelucrarea poate avea ca temei juridic art. 6 alin. (1) lit. b) GDPR numai în măsura în care persoana vizată a cerut

---

[12] Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, WP259 rev. 01, as last Revised and Adopted on 10 April 2018, p. 7.

[13] *Idem*, p. 8.

[14] European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European data protection law*, Luxembourg: Publications Office of the European Union, 2018, p. 145-146.

[15] De exemplu, o parte intenționează să încheie un contract, însă nu a făcut-o încă, posibil din cauza unor verificări rămase de finalizat iar una dintre părți trebuie să prelucreze datele în acest scop – *Idem*, p. 151.

operatorului să facă anumite demersuri înainte de încheierea contractului. Prin urmare operatorul va trebui să poată face dovada că acele demersuri (ce implică prelucrarea datelor cu caracter personal) sunt realizate la cererea persoanei vizate.

Grupul de lucru art. 29 a subliniat faptul că recurgerea la acest temei juridic trebuie interpretată în mod strict, astfel că este important să se determine cu exactitate care sunt *motivele* încheierii contractului (conținutul său şi obiectivul fundamental) şi ce date ar fi necesare pentru executarea contractului respectiv, întrucât acesta este contextul în care se verifică dacă prelucrarea datelor este sau nu necesară pentru executarea acestuia[16].

Relația contractuală nu poate constitui temei juridic al prelucrării datelor cu caracter personal atunci când prelucrarea nu este într-adevăr necesară pentru executarea unui contract, ci este mai degrabă impusă în mod unilateral de către operator persoanei vizate. Practic aici ne aflăm în prezența unei aplicații a principiului reducerea la minimum a datelor prevăzut de art. 5 alin. (1) lit. c) GDPR, potrivit căruia datele cu caracter personal trebuie să fie „adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate [încheierea sau executarea contractului – *n.n.*]". De aceea între prelucrarea datelor şi scopul executării contractului trebuie să existe o legătură directă şi obiectivă[17].

Prin urmare, dacă autoritățile şi organismele publice urmăresc a procesa date cu caracter personal care sunt efectiv necesare pentru executarea unui contract, atunci consimțământul nu constituie temei juridic adecvat[18] iar în ceea ce ne priveşte considerăm că acest aspect ar trebui evidențiat şi în registrul de evidență a activităților de prelucrare reglementat în cadrul art. 30 GDPR şi care serveşte operatorului să demonstreze conformitatea activităților de prelucrare cu prevederile Regulamentului (UE) 2016/679. Pe de altă parte, dacă operatorul va dori să legitimeze prelucrarea datelor excedentare atunci va trebui să recurgă la un alt temei juridic, precum consimțământul, pentru o parte din prelucrare[19]

4. Obligații legale ale operatorului

Potrivit art. 6 alin. (1) lit. c) GDPR, prelucrarea poate fi necesară în vederea îndeplinirii unei obligații legale ce revine autorității sau organismului public. În acest sens, art. 6 alin. (3) GDPR precizează că temeiul juridic al prelucrării (obligația legală) trebuie să fie prevăzut în dreptul Uniunii sau în dreptul intern care se

---

[16] A se vedea Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, adopted on 9 April 2014; versiunea în limba română, p. 18.

[17] Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, WP259 rev. 01, as last Revised and Adopted on 10 April 2018, p. 8.

[18] În acest sens a se vedea *ibidem*.

[19] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP187, adopted on 13 July 2011, p. 8.

aplică operatorului iar scopul prelucrării este stabilit pe baza respectivului temei juridic[20]. Această dispoziție se referă la operatorii care acționează atât în sectorul privat, cât şi în cel public, însă obligațiile legale ale operatorilor de date cu caracter personal din sectorul public pot constitui, de asemenea, obiectul art. 6 alin. (1) lit. e) GDPR[21].

În plus, art. 6 alin. (3) GDPR prevede că dreptul Uniunii sau dreptul intern trebuie să urmărească un obiectiv de *interes public* şi să fie *proporțional* cu obiectivul legitim urmărit. Pe de altă parte, considerentul (45) subliniază faptul că Regulamentul general privind protecția datelor nu impune existența unei legi specifice pentru fiecare prelucrare în parte, astfel că poate fi suficientă o singură lege drept temei pentru mai multe operațiuni de prelucrare efectuate în conformitate cu o obligație legală a operatorului.

Grupul de lucru art. 29 a precizat că desemnarea explicită a operatorului prin lege nu este frecventă şi nu pune în general probleme mari, iar în unele țări legislația națională prevede ca autoritățile publice să fie responsabile pentru prelucrarea datelor cu caracter personal ca parte a îndatoririlor acestora[22]. Mai des întâlnită este însă situația în care legislația nu desemnează direct un operator sau nu stabileşte criteriile pentru desemnarea acestuia, ci stabileşte o sarcină sau impune unei autorități sau unui organism public obligația de a colecta şi a prelucra anumite date. De asemenea, legislația poate obliga autoritățile sau organismele publice să păstreze sau să furnizeze anumite date, situație în care aceste entități vor fi considerate ca având rolul de operator pentru prelucrarea oricăror date cu caracter personal în acest context[23].

Trebuie să amintim faptul că majoritatea legilor prevăd în sarcina operatorilor, inclusiv autoritățile şi organismele publice, obligații ce întemeiază legalitatea prelucrării însă încalcă, de exemplu, principiul reducerii la minimum a datelor[24]. Rămâne de văzut cum vor aplica instanțele judecătoreşti prevederile Regulamentului (UE) 2016/679 în cazul acestor încălcări, având în vedere art. 148 alin. (2) din Constituția României, potrivit căruia „ca urmare a aderării, prevederile tratatelor constitutive ale Uniunii Europene, precum şi celelalte reglementări comunitare cu caracter obligatoriu, *au prioritate față de dispozițiile contrare din legile interne* (s.n.), cu respectarea prevederilor actului de aderare".

---

[20] Considerentul (41): „Ori de câte ori prezentul regulament face trimitere la un temei juridic sau la o măsură legislativă, aceasta nu necesită neapărat un act legislativ adoptat de către un parlament, fără a aduce atingere cerințelor care decurg din ordinea constituțională a statului membru în cauză".

[21] European Union Agency for Fundamental Rights, Council of Europe, *op. cit.*, p. 151.

[22] Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP169, adopted on 16 February 2010; versiunea în limba română, p. 10.

[23] *Ibidem*.

[24] D.-M. Şandru, *La vremuri noi, principii vechi. Observații critice privind două expresii nou introduse în art. 5 al Regulamentului General privind Protecția Datelor*, în „Revista română de drept al afacerilor" nr. 1/2018, p. 83.

Deşi, atunci când o regulă națională este contrară unei dispoziții europene, autoritățile statelor membre trebuie să aplice dispoziția europeană, avem rezerve în ceea ce priveşte aplicarea proactivă a dispozițiilor Regulamentului general privind protecția datelor de către autoritățile şi organismele publice în situația în care legea națională furnizează temeiul juridic al prelucrării datelor însă încalcă principiul minimizării datelor sau alte dispoziții ale Regulamentului (UE) 2016/679, cu atât mai mult cu cât art. 13 alin. (1) din Legea nr. 190/2018, în ceea ce priveşte aplicarea măsurilor corective autorităților şi organismelor publice, prevede într-o primă etapă numai aplicarea sancțiunii avertismentului şi la care se anexează un plan de remediere.

5. Interesele vitale ale persoanei vizate sau ale altei persoane fizice

Autoritățile şi organismele publice pot recurge la temeiul juridic prevăzut de art. 6 alin. (1) lit. d) GDPR atunci când prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice. În acelaşi sens, considerentul (46) precizează că prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes care este esențial pentru viața persoanei vizate sau pentru viața unei alte persoane fizice.

Acelaşi considerent subliniază în continuare faptul că „prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic". Prin urmare, numai în ceea ce priveşte prelucrarea datelor altor persoane fizice decât persoana vizată există interdicția recurgerii la acest temei juridic atunci când operatorul poate legitima prelucrarea întemeind-o pe un alt temei prevăzut de Regulamentului general privind protecția datelor (ex. prelucrarea datele personale ale unui părinte pentru a proteja interesele vitale ale copilului).

Considerentul (46) menționează şi câteva situații când prelucrarea poate servi intereselor vitale ale persoanei vizate, respectiv cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii şi a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.

Precizăm că autoritățile şi organismele publice nu pot recurge la temeiul juridic prevăzut de art. 6 alin. (1) lit. d) GDPR pentru a prelucra date privind sănătatea sau alte categorii speciale de date cu caracter personal atunci când persoana vizată deşi este capabilă să-şi dea consimțământul, refuză să-l dea[25].

[25] În acest sens, a se vedea Information Commissioner's Office (UK), *Guide to the General Data Protection Regulation (GDPR)*, p. 72; Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, adopted on 9 April 2014; versiunea în limba română, p. 22.

6. Interesul public sau exercitarea autorității oficiale cu care este învestit operatorul

Potrivit art. 6 alin. (1) lit. e) GDPR, prelucrarea poate fi necesară în vederea îndeplinirii unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, iar art. 6 alin. (3) GDPR precizează că în aceste situații temeiul juridic al prelucrării[26] trebuie să fie prevăzut în dreptul Uniunii sau în dreptul intern care se aplică operatorului, scopul prelucrării fiind necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului.

În acest caz, spre deosebire de prelucrarea în temeiul unei obligații legale, autorităților şi organismelor publice nu le este atribuită în mod expres prin lege calitatea de operator, nici nu li se impune obligația de a colecta şi a prelucra anumite date, însă ducerea la îndeplinire a sarcinii care serveşte unui interes public sau care rezultă din exercitarea autorității publice implică în mod necesar prelucrarea de date cu caracter personal.

Art. 2 alin. (1) lit. f) din Legea nr. 190/2018, defineşte „îndeplinirea unei sarcini care serveşte unui interes public" ca acele activități ale partidelor politice sau ale organizațiilor cetățenilor aparținând minorităților naționale, ale organizațiilor neguvernamentale, care servesc realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public ori funcționării sistemului democratic, incluzând încurajarea participării cetățenilor în procesul de luare a deciziilor şi a pregătirii politicilor publice, respectiv promovarea principiilor şi valorilor democrației. Prin urmare, în sensul legii de punere în aplicare, în măsura în care enumerarea de mai sus este exhaustivă, numai partidele politice, organizațiile cetățenilor aparținând minorităților naționale, precum şi organizațiile neguvernamentale pot prelucra date cu caracter personal în temeiul îndeplinirii unei sarcini care serveşte unui interes public.

Statele membre pot introduce dispoziții mai specifice de adaptare a aplicării normelor Regulamentului general privind protecția datelor în ceea ce priveşte prelucrarea în vederea respectării art. 6 alin. (1) lit. e) GDPR prin definirea unor cerințe specifice mai precise cu privire la prelucrare şi a altor măsuri de asigurare a unei prelucrări legale şi echitabile.

Astfel, în contextul îndeplinirii unei sarcini care serveşte unui interes public, art. 6 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 prevede în privința prelucrării datelor cu caracter personal şi a categorii speciale de date cu caracter personal că o asemenea prelucrare se poate efectua numai cu instituirea de către operator sau de către partea terță a unor garanții: *a)* punerea în aplicare a măsurilor tehnice şi organizatorice adecvate pentru respectarea principiilor legate de prelucrarea datelor cu caracter personal,

[26] Sarcina care serveşte unui interes public sau care rezultă din exercitarea autorității publice.

în special a reducerii la minimum a datelor, respectiv a principiului integrității şi confidențialității; *b)* numirea unui responsabil pentru protecția datelor, dacă aceasta este necesară în conformitate cu art. 10 din Legea nr. 190/2018[27]; *c)* stabilirea de termene de stocare în funcție de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.

Prin urmare, orice categorie de date cu caracter personal, inclusiv cele speciale, poate fi prelucrată de asociațiile şi fundațiile de utilitate publică (organizațiile neguvernamentale) în temeiul îndeplinirii unei sarcini care serveşte unui interes public numai cu instituirea garanțiilor de mai sus.

Cum asociațiile şi fundațiile de utilitate publică sunt asimilate autorităților/organismelor publice potrivit art. 2 alin. (1) lit. a) teza finală din Legea nr. 190/2018, rezultă că numai Camera Deputaților şi Senatul, Administrația Prezidențială, Guvernul, ministerele, celelalte organe de specialitate ale administrației publice centrale, autoritățile şi instituțiile publice autonome, autoritățile administrației publice locale şi de la nivel județean, alte autorități publice, precum şi instituțiile din subordinea/coordonarea acestora, vor putea recurge la exercitarea autorității publice ca temei juridic al prelucrării datelor cu caracter personal.

Potrivit considerentului (55) prelucrarea datelor cu caracter personal de către autoritățile publice în vederea realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public, şi de către asociațiilor religioase recunoscute oficial se efectuează din *motive de interes public*. Deşi unitățile de cult sunt asimilate autorităților/organismelor publice şi prelucrează datele cu caracter personal din *motive de interes public*, acestea îşi vor putea întemeia prelucrarea nu pe îndeplinirea unei sarcini care rezultă din exercitarea autorității publice, ci pe îndeplinirea unei sarcini care serveşte unui interes public.

De asemenea, considerentul (46) precizează că unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât şi intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii şi a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om. Astfel, în cazul anumitor prelucrări de date cu caracter personal putem avea un concurs de temeiuri juridice ce nu se exclud reciproc.

7. Interesele legitime urmărite de operator sau un terț

Deşi, operatorii pot recurge la interesul legitim ca temei juridic al prelucrării datelor cu caracter personal, autoritățile şi organismele publice pot recurge la

[27] Potrivit art. 37 alin. (1) lit. a) GDPR, operatorul şi persoana împuternicită de operator desemnează un responsabil cu protecția datelor ori de câte ori prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale.

temeiul juridic prevăzut de art. 6 alin. (1) lit. f) GDPR numai atunci când prelucrarea *nu* este efectuată în îndeplinirea atribuțiilor lor şi nici nu prevalează interesele sau drepturile şi libertățile fundamentale ale persoanei vizate[28].

Motivul pentru care autoritățile şi organismele publice nu se pot prevala de interesul legitim în vederea prelucrării datelor în îndeplinirea sarcinilor care le revin costă în aceea că, potrivit considerentului (47), legiuitorul trebuie să furnizeze temeiul juridic pentru aceste prelucrări realizate de către autoritățile publice.

De exemplu, potrivit art. 5 din Legea nr. 190/2018, în contextul relațiilor de muncă, autoritățile şi organismele publice, în scopul realizării intereselor lor legitime, pot prelucra date cu caracter personal prin utilizarea unor sisteme de monitorizare prin mijloace de comunicații electronice şi/sau prin mijloace de supraveghere video la locul de muncă însă numai în situația o asemenea prelucrare respectă cumulativ următoarele condiții: *a)* interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăților persoanelor vizate; *b)* angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaților; *c)* angajatorul a consultat sindicatul sau, după caz, reprezentanții angajaților înainte de introducerea sistemelor de monitorizare; *d)* alte forme şi modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficiența; şi *e)* durata de stocare a datelor cu caracter personal este proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate.

9. Concluzii

În principiu, consimțământul nu constituie un temei juridic valabil atunci când operatorul este o autoritate publică. Nici la interesul legitim nu pot recurge autoritățile şi organismele publice în vederea legitimării prelucrării datelor în îndeplinirea sarcinilor care le revin. Şi interesele vitale ale persoanei vizate sau ale altei persoane fizice au un domeniu de aplicare foarte limitat. O parte a operațiunilor de prelucrare a datelor cu caracter personal va avea ca temei juridic relația contractuală, însă de cele mai multe ori autoritățile şi organismele publice îşi vor întemeia prelucrarea pe obligațiile legale ce le revin şi exercitarea autorității oficiale cu care sunt învestite.

---

[28] Considerentul (47): „[…] În orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul şi în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele şi drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. […]"

Bibliografie:

1. *Regulamentul (UE) 2016/679* al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicat în Jurnalul Oficial al Uniunii Europene, L 119 din 4 mai 2016.

2. *Legea nr. 190 din 18 iulie 2018* privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicată în M. Of. nr. 651 din data de 26 iulie 2018.

3. *Legea nr. 500 din 11 iulie 2002 privind finanțele publice*, publicată în M. Of. nr. 597 din data de 13 august 2002.

4. Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP169, adopted on 16 February 2010; versiunea în limba română este disponibilă la adresa http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_ro.pdf, document consultat la data de 19.09.2018.

5. Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, WP187, adopted on 13 July 2011, document consultat la data de 19.09.2018, disponibil la https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/ wp187_en.pdf.

6. Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, adopted on 9 April 2014; versiunea în limba română este disponibilă la http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation /files/2014/wp217_ro.pdf, document consultat la data de 19.09.2018.

7. Article 29 Data Protection Working Party, *Opinion 2/2017 on data processing at work*, WP249, adopted on 8 June 2017; versiunea în limba română este disponibilă la http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49661, document consultat la data de 19.09.2018.

8. Article 29 Data Protection Working Party, *Guidelines on consent under Regulation 2016/679*, WP259 rev. 01, as last Revised and Adopted on 10 April 2018, disponibil la http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030, document consultat la data de 19.09.2018.

9. European Data Protection Board, *Endorsement 1/2018 of GDPR WP29 guidelines by the EDPB*, Brussels, 25 May 2018, document consultat la data de 19.09.2018, disponibil la https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

10. European Union Agency for Fundamental Rights, Council of Europe, *Handbook on European data protection law*, Luxembourg: Publications Office of the European Union, 2018.

11. Information Commissioner's Office (UK), *Guide to the General Data Protection Regulation (GDPR)*, disponibil la https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf, document consultat la data de 19.09.2018.

12. D.-M. Şandru, *Elemente privind reglementarea consimțământului în prelucrarea datelor cu caracter personal, potrivit art. 6 din Regulamentul nr. 2016/679*, în „Revista română de drept al afacerilor" nr. 5/2017, p. 129-135.

13. D.-M. Şandru, *La vremuri noi, principii vechi. Observații critice privind două expresii nou introduse în art. 5 al Regulamentului General privind Protecția Datelor*, în „Revista română de drept al afacerilor" nr. 1/2018, p. 79-84.