Revista Universul Juridic ● nr. 5, mai 2018, pp. 86-93

SCURTE CONSIDERAȚII ASUPRA DREPTULUI DE ACCES AL PERSOANEI VIZATE ÎN LUMINA REGULAMENTULUI (UE) 2016/679

Silviu-Dorin ŞCHIOPU

Abstract

The right to access one's own data is explicitly acknowledged as a fundamental right in Article 8 (2) of the Charter of Fundamental Rights of the EU which states that "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". Article 12 of the Data Protection Directive also provides that Member States are to guarantee every data subject a right of access to their personal data. Since from 25 May 2018 the General Data Protection Regulation shall apply and will replace the current Directive 95/46/EC, this article aims to provide a prima facie presentation of the new configuration of the right of access by the data subject, without overlooking its correlation with the operator's obligation to keep records of processing activities.

Keywords: *personal data, data subject, right of access, right to obtain a copy of the personal data undergoing processing, records of processing activities, Directive 95/46/EC, Romanian Law no. 677/2001, Regulation (EU) 2016/679.*

Considerații generale

Obiectivul Regulamentului (UE) 2016/679 (GDPR)[1] este, potrivit art. 1 alin. (2), acela de a proteja drepturile şi libertățile fundamentale ale persoanelor fizice şi în special a dreptului acestora la protecția datelor cu caracter personal. În acest sens, considerentul (7) precizează că persoanele fizice ar trebui să aibă *control* asupra propriilor date cu caracter personal, iar securitatea juridică şi practică pentru persoanele fizice ar trebui consolidată.

[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. [GDPR].

Precum s-a precizat şi în jurisprudența Curții de justiție a Uniunii Europene, orice prelucrare trebuie, pe de o parte, să fie conformă cu *principiile* legate de prelucrarea datelor cu caracter personal şi, pe de altă parte, să respecte unul din criteriile privind *legalitatea* prelucrării datelor[2].

Persoana vizată, pentru a fi informată cu privire la prelucrare şi mai ales pentru a putea verifica *legalitatea* acesteia, ar trebui să aibă potrivit considerentului (63) un *drept de acces* la datele cu caracter personal colectate care o privesc şi ar trebui să îşi exercite acest drept cu uşurință şi la intervale de timp rezonabile.

Dreptul de acces al persoanei vizate este înscris în art. 8 alin. (2) din Carta drepturilor fundamentale a Uniunii Europene[3] care prevede că: „Orice persoană are *dreptul de acces* la datele colectate care o privesc […]" şi este reglementat în cadrul art. 15 din Regulamentului (UE) 2016/679.

În temeiul dreptului de acces, potrivit considerentului (63), orice persoană vizată ar trebui să aibă dreptul de a cunoaşte şi de a i se comunica în special *scopurile* în care sunt prelucrate datele, dacă este posibil *perioada* pentru care se prelucrează datele cu caracter personal, *destinatarii* datelor cu caracter personal, *logica de prelucrare automată* a datelor cu caracter personal şi, cel puțin în cazul în care se bazează pe crearea de profiluri, *consecințele* unei astfel de prelucrări. De asemenea, operatorul de date, numai atunci când acest lucru este posibil, ar trebui să poată furniza acces de la distanță la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal.

Bine-înțeles, acest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale şi, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, aceste aspecte nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Astfel, secretul comercial, proprietatea intelectuală, drepturile de autor care asigură protecția programelor software şi alte drepturi sau libertăți ale altora nu pot justifica refuzul de a furniza toate informațiile persoanei vizate.

Atunci când operatorul prelucrează un *volum mare de informații privind persoana vizată*, operatorul ar trebui să poată solicita ca, înainte de a-i fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa.

Trebuie să subliniem că Regulamentul (UE) 2016/679 în considerentului (63) nu conferă operatorului posibilitatea de a impune persoanei vizate obligația de a preciza informațiile sau activitățile de prelucrare la care se referă cererea sa decât atunci când prelucrează un volum mare de informații privind însăşi persoana vizată, *nu şi în situația în care, în general, volumul de date cu caracter personal pe care le*

[2] A se vedea CJUE, *hotărârea din 1 octombrie 2015, cauza C-201/14 - Bara şi alții*, ECLI:EU:C:2015:638, publicată în Repertoriul electronic (Repertoriul general) [para. 30].

[3] Publicată în Jurnalul Oficial al Uniunii Europene, C 326 din 26 octombrie 2012.

prelucrează este mare. Oricum, în temeiul principiului prelucrării echitabile şi transparente, considerăm că operatorul *nu* poate refuza a furniza persoanei vizate toate informațiile, chiar dacă volumul acestora este mare.

Dreptul de acces este necesar pentru a-i permite persoanei vizate să exercite drepturile prevăzute la art. 15-18 GDPR, şi anume, în cazul în care prelucrarea datelor sale nu ar respecta dispozițiile regulamentului, dreptul de a obține de la operator *rectificarea*, *ştergerea* sau *restricționarea prelucrării* datelor sale.

Dreptul de acces mai este necesar şi pentru a permite persoanei vizate să exercite, în temeiul art. 19 GDPR, *dreptul de a fi informată* cu privire la destinatarii cărora operatorul le-a comunicat orice rectificare sau ştergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu art. 16, art. 17 alin. (1) şi art. 18 GDPR.

Acest drept de acces este de asemenea necesar pentru a-i permite persoanei vizate să exercite *dreptul de opoziție* la prelucrarea datelor sale cu caracter personal prevăzut de art. 21 GDPR sau *dreptul la o cale de atac*, prevăzut de art. 77-79 GDPR, în cazul în care prelucrarea datelor cu caracter personal care o vizează încalcă prevederile regulamentului.

Modalitățile de exercitare a dreptului de acces

Persoana vizată, potrivit considerentului (63), ar trebui să-şi exercite dreptul de acces *cu uşurință* şi la *intervale de timp rezonabile*, pentru a fi informată cu privire la prelucrare şi pentru a verifica legalitatea acesteia. Informațiile furnizate, orice comunicare şi orice măsuri luate în temeiul art. 15 GDPR privind dreptul de acces trebuie oferite de către operator în mod *gratuit*. Condiția privind intervalele de timp rezonabile presupune ca solicitările de acces la date să fie făcute în scopul pentru care acest drept a fost garantat, adică să nu fie făcute, de exemplu, pentru a şicana operatorul[4].

Potrivit art. 12 GDPR privind transparența informațiilor, a comunicărilor şi a modalităților de exercitare a drepturilor persoanei vizate, operatorul este obligat să facilitează exercitarea dreptului de acces de către persoana vizată.

Operatorul, potrivit art. 12 alin. (3) GDPR, are obligația să furnizeze persoanei vizate informații privind acțiunile întreprinse în urma unei cereri de acces, fără întârzieri nejustificate şi în orice caz *în cel mult o lună de la primirea cererii*. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea şi numărul cererilor, situație în care operatorul, în termen de o lună de la primirea cererii, are obligația de a informa persoana vizată cu privire la orice astfel de prelungire, indicând şi motivele întârzierii.

[4] G. Zanfir, *Protecția datelor personale: drepturile persoanei vizate*, Ed. C.H. Beck, Bucureşti, 2015, p. 108.

Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul are obligația de a informa persoana vizată, fără întârziere şi în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri şi la posibilitatea de a depune o plângere în fața unei autorități de supraveghere şi de a introduce o cale de atac judiciară.

Operatorul poate refuza să dea curs cererii persoanei vizate de a-şi exercita dreptul de acces, în măsura în care poate demonstra că nu este în măsură să identifice persoana vizată. În cazul în care este posibil, operatorul informează persoana vizată în mod corespunzător iar persoana vizată, în temeiul art. 11 alin. (2) GDPR, în scopul exercitării dreptului de acces, poate oferi informații suplimentare care permit identificarea sa. De asemenea, potrivit art. 12 alin. (6) GDPR, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate şi atunci când are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea de acces.

În cazul cererilor de acces care sunt în mod vădit nefondate sau excesive, în special datorită caracterului lor repetitiv, operatorul poate fie să perceapă o *taxă rezonabilă* ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării, fie să refuze să dea curs cererii. Sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii revine operatorului.

Potrivit art. 12 alin. (3) GDPR, atunci când persoana vizată introduce o cerere de acces în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format. Astfel, potrivit art. 12 alin. (1) GDPR, operatorul furnizează informațiile în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. De asemenea, la solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace[5].

Comunicările referitoare la prelucrare trebuie furnizate într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu.

Conținutul dreptului de acces

În primul rând, persoana vizată are dreptul de a obține din partea operatorului o *confirmare* că se prelucrează sau nu date cu caracter personal care o privesc.

În al doilea rând, în cazul afirmativ, persoana vizată, pe de o parte, are *dreptul de a-i fi furnizate o serie de informații*, iar, pe de altă parte, are un *drept de acces la datele respective*, adică de a-i fi furnizată o copie a datelor sale cu caracter personal care fac obiectul prelucrării.

[5] Considerentul (64): „Operatorul ar trebui să ia *toate măsurile rezonabile* pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online şi al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale".

Dreptul de a primi informații privind prelucrarea datelor cu caracter personal

În cazul în care operatorul confirmă că prelucrează date cu caracter personal care o privesc, persoana vizată are dreptul de a obține o serie informații. Bine-înțeles, acest drept există chiar dacă operatorul nu confirmă prelucrarea datelor cu caracter personal ale persoanei vizate, însă exercitarea sa este condiționată fie de recunoaşterea făcută de operator, fie de dovedirea prelucrării prin alte mijloace.

Informațiile privind prelucrarea datelor cu caracter personal pe care persoana vizată este îndreptățită să le primească în temeiul exercitării dreptului de acces privesc: *scopurile* prelucrării; *categoriile de date* cu caracter personal vizate (ex. nume, adrese, date de naştere, domeniul de interes al persoanei vizate, etc.); *destinatarii* sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate (în special destinatari din țări terțe sau organizații internaționale); acolo unde este posibil, *perioada* pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; orice informații disponibile privind *sursa*[6] acestora, atunci când datele cu caracter personal nu sunt colectate de la persoana vizată; existența unui proces decizional automatizat incluzând crearea de *profiluri*[7], precum şi informații pertinente privind logica utilizată şi privind importanța şi consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

Persoana vizată are dreptul să fie informată şi cu privire la *garanțiile adecvate* în temeiul art. 46 GDPR referitoare la transfer, atunci când datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională.

De asemenea, operatorul este obligat să menționeze existența dreptului de a solicita operatorului rectificarea, ştergerea şi restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată, a dreptului de a se opune prelucrării, precum şi dreptul de a depune o plângere în fața unei autorități de supraveghere.

Regulamentul (UE) 2016/679 nu specifică la ce perioadă anume din trecut se referă dreptul de acces la informații, de exemplu în privința destinatarilor sau categoriile de destinatari cărora datele cu caracter personal le-au fost divulgate.

---

[6] Un operator nu poate distruge informațiile privind sursa datelor pentru a fi scutit de obligația de a le divulga iar nedocumentarea sursei datelor prelucrate, de regulă, nu se consideră o îndeplinire a obligațiilor operatorului în ceea ce priveşte dreptul de acces – a se vedea Agenția pentru Drepturi Fundamentale a Uniunii Europene, Consiliul Europei, *Manual de legislație europeană privind protecția datelor*, Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2014, p. 112.

[7] A se vedea art. 22 alin. (1) şi (4) din Regulamentul (UE) 2016/679.

În cauza Rijkeboer, Curtea de Justiție a Uniunii Europene a precizat că „o reglementare care limitează stocarea informațiilor referitoare la destinatarii sau categoriile de destinatari ai datelor şi la conținutul datelor transmise la o perioadă de un an şi care limitează în mod corelativ accesul la aceste informații, în timp ce *datele de bază sunt stocate mult mai mult timp* (s.n.), nu poate constitui un just echilibru între interesele şi obligațiile în cauză, cu excepția situației în care se demonstrează că o stocare mai îndelungată a acestor informații ar constitui o sarcină excesivă pentru operator"8.

Din hotărârea CJUE rezultă că dreptul de acces la datele proprii nu poate fi restricționat în mod nejustificat prin termene limită iar perioada de stocare a informațiilor privind transferul datelor cu caracter personal – şi în general întreaga evidență a prelucrării – nu poate fi mai mică decât perioada de stocare a însăşi datelor de bază.

O bună parte a informațiilor ce trebuie furnizate persoanei vizate ca urmare a exercitării dreptului de acces pot fi extrase cu uşurință de către operator din *evidențele activităților de prelucrare* prevăzute în art. 30 GDPR, care cuprind: *scopurile* prelucrării; o descriere a categoriilor de persoane vizate şi a *categoriilor de date* cu caracter personal; categoriile de *destinatari* cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale; *transferurile* de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective şi, în cazul transferurilor menționate la art. 49 alin. (1) al doilea paragraf, documentația care dovedeşte existența unor garanții adecvate; precum şi, acolo unde este posibil, *termenele-limită* preconizate pentru ştergerea diferitelor categorii de date.

Deşi obligația de a păstra o evidență a activităților de prelucrare desfăşurate sub responsabilitatea lor nu se aplică, în principiu, întreprinderilor sau organizațiilor cu mai puțin de 250 de angajați[9], nimic nu împiedică inclusiv aceste entități să țină astfel de evidențe privind documentarea prelucrării datelor cu caracter personal.

Dreptul de a obține o copie a datelor cu caracter personal care fac obiectul prelucrării

Pe lângă informații privind prelucrarea datelor cu caracter personal, potrivit art. 15 alin. (3) GDPR, persoana vizată este îndreptățită să primească iar operatorul

---

[8] CJUE, *hotărârea din 7 mai 2009, C‑553/07 – Rijkeboer*, ECLI:EU:C:2009:293, publicată în Repertoriul jurisprudenței 2009 I-03889.

[9] Cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile şi libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date ori date cu caracter personal referitoare la condamnări penale şi infracțiuni (art. 10).

este obligat să furnizeze o *copie a datelor cu caracter personal care fac obiectul prelucrării*. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative.

Informațiile trebuie furnizate într-un format electronic utilizat în mod curent atunci când persoana vizată a introdus cererea în format electronic, cu excepția cazului în care persoana vizată a solicitat un alt format. Spre deosebire de exercitarea dreptului la portabilitatea datelor prevăzut de art. 20 GDPR, formatul în care sunt furnizate informațiile nu trebuie să fie structurat şi să poată fi citit automat.

Informarea persoanei vizate cu privire la datele care fac obiectul prelucrării trebuie realizată într-o formă inteligibilă, adică operatorul trebuie să explice, în mod detaliat, ce anume prelucrează. Astfel, chiar dacă operatorul stochează numai abrevieri tehnice, simpla menționare a acestora nu va fi, de regulă, suficientă[10].

Dreptul persoanei vizate de a obține o copie a datelor cu caracter personal care fac obiectul prelucrării nu poate aduce atingere drepturilor şi libertăților altora, inclusiv secretului comercial sau proprietății intelectuale şi, în special, drepturilor de autor care asigură protecția programelor software.

Restricții privind exercitarea dreptului de acces

Dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator, în temeiul art. 23 alin (1) GDPR, poate restricționa domeniul de aplicare al dreptului de acces numai printr-o *măsură legislativă*, atunci când o astfel de restricție respectă esența drepturilor şi libertăților fundamentale şi constituie o măsură necesară şi proporțională într-o societate democratică.

Restricțiile pot fi justificate de considerente precum securitatea națională, apărarea, securitatea publică, prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice şi prevenirea acestora, ş.a.m.d.

Orice măsură legislativă prin care s-ar restricționa dreptul de acces trebuie să conțină dispoziții specifice cel puțin, dacă este cazul, în ceea ce priveşte: *scopurile* prelucrării sau ale categoriilor de prelucrare; *categoriile* de date cu caracter personal; domeniul de aplicare al *restricțiilor* introduse; *garanțiile* pentru a preveni abuzurile sau accesul sau transferul ilegal; menționarea *operatorului* sau a categoriilor de operatori; *perioadele* de stocare şi *garanțiile* aplicabile având în vedere natura, domeniul de aplicare şi scopurile prelucrării sau ale categoriilor de prelucrare; *riscurile* pentru drepturile şi libertăților persoanelor vizate; şi dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.

[10] A se vedea Agenția pentru Drepturi Fundamentale a Uniunii Europene, *op. cit.*, p. 112.

Încălcarea dreptului de acces al persoanei vizate

Potrivit art. 77 alin. (1) GDPR, atunci când consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prevederile regulamentului, persoana vizată are *dreptul de a depune o plângere la o autoritate de supraveghere*, în special în statul membru în care îşi are reşedința obişnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare. Pe lângă dreptul de a depune o plângere la o autoritate de supraveghere, persoana vizata are şi *dreptul de a exercita o cale de atac judiciară eficientă* în cazul în care consideră că dreptul de acces i-a fost încălcat.

Bibliografie:

1. *Carta drepturilor fundamentale a Uniunii Europene*, publicată în Jurnalul Oficial al Uniunii Europene, C 326 din 26 octombrie 2012.

2. *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.

3. CJUE, *hotărârea din 7 mai 2009, C‑553/07 – Rijkeboer*, ECLI:EU:C:2009:293, publicată în Repertoriul jurisprudenței 2009 I-03889.

4. CJUE, *hotărârea din 1 octombrie 2015*, cauza C‑201/14 - *Bara şi alții*, ECLI:EU:C:2015:638, publicată în Repertoriul electronic (Repertoriul general).

5. Agenția pentru Drepturi Fundamentale a Uniunii Europene, Consiliul Europei, *Manual de legislație europeană privind protecția datelor*, Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2014.

6. G. Zanfir, *Protecția datelor personale: drepturile persoanei vizate*, Ed. C.H. Beck, Bucureşti, 2015.