GRUPUL DE LUCRU „ARTICOLUL 29” PENTRU PROTECȚIA DATELOR

17/RO

WP259

Orientări asupra Consimțământului în temeiul Regulamentului 2016/679

Adoptat la 28 noiembrie 2017

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 25 octombrie 1995,

luând în considerare Articolele 29 și 30 alineatele 1(a) și 3 din Directivă,

luând în considerare propriile Reguli de Procedură,

ADOPTĂ PREZENTUL DOCUMENT

Cuprins:

1. Introducere

Aceste Orientări oferă o analiză minuțioasă a conceptului de Consimțământ din Regulamentul 2016/679, Regulamentul General privind Protecția Datelor(în continuare denumit GDPR) Conceptul de Consimțământ configurat în Directiva privind Protecția Datelor (în continuare denumită Directiva 95/46/CE), precum și în Directiva asupra confidențialității și comunicațiilor electronice, în vigoare, a evoluat. GDPR oferă clarificări și precizări suplimentare cu privire la cerințele necesare obținerii și demonstrării consimțământului în mod valabil. Aceste Orientări privesc aceste noi problematici, conferind instrucțiuni practice pentru a se asigura conformitatea cu GDPR și se întemeiază pe Opinia nr. 15/2011 cu privire la Consimțământ.

Consimțământul este unul dintre cele șase temeiuri de legalitate în ceea ce privește Prelucrarea datelor cu caracter personal, enumerate de Articolul 6 din GDPR[1]. Atunci când se inițiază activități care presupun Prelucrarea de date cu caracter personal, operatorul de date trebuie întotdeauna să evalueze *dacă Consimțământul este temeiul legal adecvat* pentru Prelucrarea avută în vedere sau trebuie identificat un alt temei.

În general, Consimțământul poate fi temeiul juridic adecvat doar atunci când persoanei vizate i s-a acordat controlul și posibilitatea unei alegeri reale în ceea ce privește fie acceptarea fie respingerea termenilor conferiți sau respingerea acestora fără nici un prejudiciu. Atunci când se solicită Consimțământul, un operator de date are obligația să evalueze dacă această solicitare întrunește toate condițiile de obținere a unui Consimțământ valabil. Dacă este obținut în conformitate deplină cu GDPR, Consimțământul este un instrument care conferă persoanelor vizate controlul asupra posibilității ca datele lor cu caracter personal să fie sau nu Prelucrate. Altfel, controlul deținut de persoanele vizate devine iluzoriu și Consimțământul va fi un temei anulabil în ceea ce privește Prelucrarea, cu consecința că activitatea de Prelucrare este nelegală[2].

Actuala Opinie a Grupului de lucru „Articolului 29" (WP29) cu privire la Consimțământ[3] este relevantă, în condițiile în care este conformă cu noul cadru legal atât timp cât GDPR codifică ghidurile Grupului de Lucru „Articolul 29" iar bunele practici generale și elementele esențiale ale Consimțământului au rămas aceleași în cadrul GDPR. Ca urmare, în acest document, WP29 mai degrabă dezvoltă și întregește Opiniile anterioare asupra domeniului specific care încorporează trimiteri cu privire la Consimțământ în temeiul Directivei 95/46/CE, decât să le înlocuiască.

[1] Articolul 9 GDPR prevede o listă a posibilelor excepții de la interdicția de a Prelucra categorii speciale de date. Una dintre excepțiile enumerate este situația în care persoana vizată oferă Consimțământul explicit pentru utilizarea respectivelor date.

[2] A se vedea de asemenea Opinia nr. 15/2011 cu privire la definiția Consimțământului(WP 187), pp.6-8, și/sau Opinia nr. 06/2014 cu privire la noțiunea de interese legitime ale operatorilor de date în temeiul Articolului 7 din Directiva 95/46/CE (WP 217), pp. 9, 10, 13 și 14

[3] În special, Opinia nr. 15/2011 cu privire la definiția Consimțământului(WP 187).

Astfel cum se afirmă în Opinia nr. 15/2011 cu privire la definiția Consimțământului, cererea adresată persoanelor de fi de acord cu o Prelucrare a datelor, trebuie să fie supusă unor condiții riguroase, din moment ce se referă la drepturile fundamentale ale persoanelor vizate iar operatorii de date intenționează să intre într-o activitate de Prelucrare care ar fi ilegală fără existența Consimțământului persoanelor vizate[4]. Rolul esențial al Consimțământului este evidențiat de Articolele 7 și 8 din Carta Drepturilor Fundamentale ale Uniunii Europene. În plus, obținerea Consimțământului nu înlătură și cu atât mai puțin nu minimizează obligațiile de a respecta principiile Prelucrării ilustrate de GDPR, în special de Articolul 5 GDPR referitor la echitate, necesitate și proporționalitate, precum și în ceea ce privește calitatea datelor. Chiar și atunci când Prelucrarea datelor personale este întemeiată pe Consimțământul persoanei vizate, nu se legitimează colectarea de date care nu sunt **necesare** în raport cu scopuri specifice de Prelucrare și este în mod fundamental injustă[5].

Între timp, WP29 se preocupă de revizuirea Directivei asupra confidențialității și comunicațiilor electronice(2002/58/EC). Conceptul de Consimțământ din proiectul Regulamentului asupra confidențialității și comunicațiilor electronice rămâne legat de noțiunea de Consimțământ din GDPR[6]. Este cel mai probabil că întreprinderile au nevoie de Consimțământ în temeiul Directivei asupra confidențialității și comunicațiilor electronice, pentru majoritatea mesajelor online sau a apelurilor telefonice de marketing, și pentru metodele de control online incluzând utilizarea de cookies sau aplicații sau alte instrumente de software. WP29 deja a oferit recomandări și ghiduri legislatorului european cu privire la Regulamentul ePrivacy[7].

În ceea ce privește actuala Directivă e-Privacy, WP29 constată că referințele la amintita Directivă 95/46/CE trebuie să fie legate de referințele la GDPR[8]. Același raționament se aplică Consimțământului configurat de actuala Directivă 2002/58/CE, chiar dacă Regulamentul ePrivacy nu va fi (încă) în vigoare din 25 mai 2018. În conformitate cu Articolul 95 GDPR obligații suplimentare pentru persoanele fizice sau juridice în ceea ce privește Prelucrarea în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în rețelele de comunicații publice nu pot fi impuse atât timp cât Directiva e-Privacy impune obligații specifice cu același obiectiv. WP29 constată că condițiile pentru Consimțământ în temeiul GDPR nu sunt considerate a fi „obligație suplimentară", însă mai degrabă precondiții pentru Prelucrarea legală. De aceea, condițiile GDPR pentru obținerea Consimțământului valabil sunt aplicabile în situațiile care cad sub incidența Directivei e-Privacy.

[4] Opinia nr. 15/2011, pagina cu privire la definiția Consimțământului (WP 187), p. 8

[5] A se vedea totodată Opinia nr. 15/2011, referitoare la definiția Consimțământului (WP 187), și articolul 5 GDPR.

[6] În conformitate cu Articolul 9 din proiectul de Regulament asupra confidențialității și comunicațiilor electronice, se aplică definiția și condițiile Consimțământului prevăzute de Articolul 4(11) și Articolul 7 din GDPR .

[7] A se vedea Opinia nr. 03/2016 cu privire la evaluarea și revizuirea Directivei ePrivacy (WP 240).

[8] A se vedea Articolul 94 GDPR.

2. Consimțământul din Articolul 4(11) din GDPR

Articolul 4(11) din GDPR definește Consimțământul astfel: „„consimțământ" al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;"

Conceptul de bază al Consimțământului este asemănător aceluia în temeiul Directivei 95/46/CE iar Consimțământul este unul dintre temeiurile juridice pe baza cărora trebuie să se întemeieze Prelucrarea datelor personale, în virtutea Articolului 6 din GDPR[9]. Dincolo de definiția modificată prevăzută de Articolul 4(11), GDPR prevede îndrumări suplimentare la Articolul 7 și în considerentele 32, 33, 42 și 43 asupra modului în care Operatorul trebuie să acționeze pentru a se conforma cu elementele principale ale cerinței consimțământului.

În cele din urmă, includerea unor prevederi și considerente specifice asupra retragerii consimțământului confirmă faptul că, acordarea Consimțământul trebuie să constituie o decizie reversibilă și este menținut un grad de control de către persoana vizată.

3. Elementele Consimțământului valabil exprimat

Articolul 4 (11) GDPR prevede că, consimțământul persoanei vizate este unul:

- oferit în mod liber
- specific
- în cunoștință de cauză
- Exprimare lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

[9] Pentru ca Prelucrarea datelor să fie legală, potrivit articolului 7(a) din Directiva 95/46/CE Consimțământul persoanei vizate trebuie să reprezinte „orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate". A se vedea Opinia nr. 15/2011 asupra definiției Consimțământului (WP187), spre exemplu, asupra caracterului adecvat a Consimțământului ca temei juridic. Potrivit acestei Opinii, WP29 a oferit îndrumări pentru a se deosebi între situația în care Consimțământul constituie un temei juridic adecvat față de situația în care ne întemeiem pe interese legitime (posibil cu șansa de a avea opțiunea de ieșire) care sunt suficiente ori este recomandabilă o legătură contractuală. A se vedea WP29, paragraful III.1.2, p. 14 și următoarele. Consimțământul explicit este de asemenea o excepție față de interdicția cu privire la Prelucrarea unor categorii speciale de date: a se vedea articolul 9 GDPR.

În secțiunile de mai jos, măsura în care prevederile Articolului 4 (11) pretind Operatorilor să-și modifice formularele/cererile de obținere a consimțământului, pentru a asigura conformitatea cu GDPR[10].

3.1. Liber / Liber exprimat[11]

Elementul „liber" implică o alegere reală și un control real din partea persoanelor vizate. Ca regulă generală, GDPR-ul stipulează că, în situația în care persoana vizată nu beneficiază de o alegere reală, se simte obligată sau va suferi consecințe negative dacă nu exprimă consimțământul, consimțământul acesteia nu va fi unul valabil exprimat [12]. Dacă consimțământul este încadrat ca o parte ce nu poate fi negociată în cadrul unor termeni și condiții, se prezumă că acesta nu este exprimat în mod liber. Astfel, consimțământul nu va fi considerat ca fiind în mod liber exprimat dacă persoana vizată se află în imposibilitatea de a refuza sau a-l retrage fără a suferi un prejudiciu[13]. Termenul de dezechilibru între Operator și persona vizată este de asemenea luat în considerare de către GDPR.

> [Exemplul nr. 1]O aplicație pentru telefon mobil destinată editării fotografiilor solicită utilizatorilor să aibă localizarea GPS activată pentru a se folosi de serviciile acesteia. Aplicația de asemenea comunică utilizatorilor că aceasta va folosi datele colectate în scopuri publicitare bazate pe comportamentul persoanei. Nici localizarea GPS, nici publicitatea on-line bazată pe comportamentul persoanei nu sunt necesare pentru furnizarea aplicației de editare fotografică și exced serviciului de bază furnizat. Întrucât utilizatorii nu pot folosi aplicația fără a-și exprima consimțământul privind prelucrarea acestor date, exprimarea acestuia nu poate fi considerată ca fiind una făcută în mod liber.

[10] Pentru îndrumare referitor la activitățile de procesare ce se află în curs de desfășurare în temeiul consimțământului prevăzut în Directiva 95/46, a se vedea capitolul 7 al acestui document și considerentul 171 al GDPR.

[11] Conform mai multor opinii, Grupul de lucru „Articolul 29" (WP29) a examinat limitele consimțământului în situațiile în care acesta nu poate fi liber exprimat. Această ipoteză a fost, în special, reprezentată în Opinia nr. 15/2011 privind definiția consimțământului (WP 187), Documentul de Lucru privind procesarea datelor cu caracter personal referitor la sănătate din cadrul înregistrărilor electronice a sănătății (WP 131), Opinia nr. 8/2001 privind procesarea datelor cu caracter personal în cadrul procesului de angajare (WP 48) și Opinia doi nr. 4/2009 privind procesarea datelor de către Agenția Mondială Anti-Doping (WADA) (Standard Internațional privind Protecția Vieții Private și Informației Personale în conformitate cu dispozițiile corespunzătoare ale Codului WADA și altor situații legate de confidențialitate, în contextul luptei împotriva folosirii dopajului în sport de către WADA și organizațiile (naționale) anti-doping (WP 162).

[12] A se vedea Opinia nr. 15/2011 privind definiția consimțământului (WP 187), p.12.

[13] A se vedea Considerentele 42, 43 GDPR și Opinia nr. 15/2011 privind definiția consimțământului (WP 187), p.12.

3.1.1. Dezechilibrul de puteri

Considerentul 43[14] indică în mod clar că este puțin probabil ca **autoritățile publice** pot să se bazeze pe consimțământul acordat pentru Prelucrarea datelor întrucât de fiecare dată când Operatorul este o autoritate publică, deseori există un dezechilibru clar al puterilor în relația dintre Operator și persoana vizată. Este de asemenea clar că în majoritatea cazurilor persoana vizată nu va avea alternative reale acceptării Prelucrării (termenilor) din partea Operatorului. WP 29 consideră că există alte temeiuri legale care sunt, în principiu, mai adecvate activității autorităților publice[15].

Fără a aduce atingere acestor considerații generale, folosirea consimțământului ca o bază legală pentru procesarea datelor de către autoritățile publice nu este exclusă în totalitate potrivit cadrului legal prevăzut de către GDPR. Exemplele următoare arată că folosirea consimțământului poate fi adecvată în anumite circumstanțe:

> [Exemplul nr. 2]Administrația publică locală planifică niște lucrări de întreținere a drumului. Întrucât lucrările pot perturba traficul pentru o perioadă mai lungă, administrația oferă cetățenilor oportunitatea de a se abona la o listă prin e-mail, pentru a primit actualizări privind mersul lucrărilor și întârzierile preconizate. Administrația comunică faptul că nu este nici o obligație de a se abona și solicită consimțământul pentru a folosi adresele de e-mail pentru acest scop (în mod exclusiv). Cetățenii care nu își exprimă consimțământul nu vor pierde accesul la vreun serviciu de bază al administrației sau exercițiul vreunui drept, astfel că aceștia pot să dea sau să refuze consimțământul privind folosirea datelor, în mod liber. Toată informația privind lucrările asupra drumului sunt de asemenea disponibile pe site-ul municipalității.
>
> [Exemplul nr. 3]O persoană ce are în proprietate terenuri are nevoie de anumite autorizări din partea administrației publice locale și guvernului provincial (administrației regionale sau centrale – n.t.) sub care rezidă municipalitatea. Ambele organe publice solicită aceeași informație pentru emiterea autorizărilor, dar nu accesează una alteia propria bază de date. Astfel, ambele solicită aceeași informație și proprietarul trimite informațiile solicitate ambelor organe publice. Municipalitatea și autoritatea provincială solicită consimțământul pentru a uni dosarele, pentru a evita duplicitatea procedurilor și corespondenței. Ambele organe publice specifică că această propunere este opțională și solicitările de obținere a autorizărilor vor fi procesate separat în cazul în care proprietarul nu dorește unificarea acestora. Proprietarul este în situația de a de a decide asupra exprimării consimțământului privind conexarea dosarelor, în mod liber.

[14] Considerentul 43 al GDPR prevede: „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 și operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare.[…]”.

[15] A se vedea Articolul 6 GDPR, în special alineatele (1c) și (1e).

[Exemplul nr. 4]O școală de stat solicită elevilor consimțământul acestora pentru a folosi fotografiile acestora într-o revistă tipărită dedicată acestora. Exprimarea consimțământului în astfel de situații se consideră a fi o alegere potrivită întrucât elevii nu vor fi îngrădiți în dreptul lor la studiu sau acces la servicii și pot refuza folosirea acestor fotografii fără a fi prejudiciați în vreun mod[16].

Un dezechilibru de putere apare de asemenea în contextul legat de forța de muncă.[17] Luând în considerarea dependența ce rezultă dintre relația angajator/angajat, este puțin probabil ca persoana vizată să poată să refuze consimțământul angajatorului ei/lui pentru Prelucrarea datelor cu caracter personal fără să experimenteze temerea sau un risc real cu efecte prejudiciabile ca rezultat al unui refuz. Este puțin probabil ca un angajat să poată să răspundă sincer la cererea angajatorului ei/lui de a-și da consimțământul angajatorului, spre exemplu, pentru a activa sisteme de monitorizare, care ar putea fi camere de supraveghere la locul de muncă, sau să completeze fișe de evaluare, fără a simți nicio presiune legată de consimțământ.[18] Prin urmare, WP29 consideră problematică Prelucrarea de către angajator a datelor cu caracter personal a angajaților actuali cât și viitori pe baza consimțământului, având în vedere că acesta este puțin probabil de a fi oferit în mod liber. Pentru majoritatea acestor Prelucrări de date personale din cadrul locului de muncă, baza legală nu poate și nu ar trebui să fie consimțământul angajaților [Art. 6, alin.1, lit. a)] datorită naturii relației dintre angajat si angajator.[19]

Cu toate acestea, acest lucru nu înseamnă că angajatorii nu pot să se bazeze niciodată pe consimțământul angajaților ca bază legală pentru prelucrarea datelor. Pot exista situații când angajatorul poate demonstra că acordarea Consimțământului a fost făcută cu adevărat în mod liber. Luând în considerarea dezechilibrul de putere dintre angajator împreună cu personalul de conducere, angajații își pot oferi liber consimțământul doar în situații excepționale, când nu vor exista deloc consecințe adverse indiferent că și-au oferit sau nu consimțământul.[20]

[Exemplul numărul 5]Un echipaj de filmare urmează să filmeze într-o anume parte dintr-un birou. Angajatorul cere tuturor angajaților care își desfășoară activitatea în acea parte, consimțământul de a fi filmați, deoarece aceștia ar putea să apară pe fundalul

[16] Pentru scopurile acestui exemplu, o școală public înseamnă o școală finanțată din fonduri publice sau orice altă facilitate educațională care se califică drept autoritate public sau organ public potrivit dreptului național.

[17] A se vedea de asemenea articolul 88 GDPR, unde este evidențiată necesitatea protecției unor interese specifice a angajaților și este stabilită o posibilitate de derogare prin legea statelor membre.

[18] A se vedea Opinia nr. 15/2011 privind definiția conimțământului (WP 187), pp. 12-14, Opinia nr. 8/2001 privind prelucrarea datelor cu caracter personal în contextul legat de forța de muncă (WP 48), Capitolul 10, Documentul de lucru privind supravegherea comunicațiilor electronice la locul de muncă (WP 55), paragraful 4.2 și Opinia nr. 2/2017 privind prelucrarea de datelor la locul de muncă (WP 249), paragraful 6.2.

[19] A se vedea Opinia nr. 2/2017 privind prelucrarea datelor la locul de muncă, pp. 6-7.

[20] A se vedea și Opinia nr. 2/2017 privind prelucrarea datelor la locul de muncă (WP 249), paragraful 6.2.

filmării. Cei care nu vor să fie filmați nu sunt sancționați sub nicio formă dar în schimb le sunt oferite munci echivalente în altă parte a clădirii pe durata filmărilor.

Dezechilibrul de putere nu se limitează la autorități publice și angajatori, ci poate apărea și în alte situații. Așa cum este subliniat de WP29 în câteva Opinii, consimțământul poate fi considerat valid doar dacă persoana vizată poate să aibă exercițiul unei alegeri reale, și nu există nici un risc de înșelăciune, intimidare, constrângerea sau a unor consecințe negative semnificante (spre exemplu, costuri suplimentare substanțiale) dacă nu-și oferă consimțământul. Consimțământul nu va fi liber în cazurile în care există vreun element de constrângere, presiune sau incapacitate de exercitare liberă a voinței.

3.1.2. Condiționalitate

Articolul 7 (4) GDPR joacă un rol important[21] pentru a evalua dacă consimțământul este oferit în mod liber.

Articolul 7 (4) GDPR indică faptul că, *inter alia*, situația de „grupare" a consimțământului odată cu acceptarea termenilor și condițiilor, sau „legarea" prevederilor unui contract sau a unui serviciu de solicitarea consimțământului de Prelucrare a datelor cu caracter personal fără a fi necesară pentru executarea acelui contract sau al serviciului respectiv, este considerată a fi extrem de indezirabilă. Dacă în această situație este acordat consimțământul, atunci se prezumă că acesta nu a fost liber manifestat (considerentul 43). Articolul 7 (4) caută să asigure că scopul Prelucrării de date personale nu este deghizat sau legat de clauza unui contract de servicii pentru realizarea căruia aceste date cu caracter personal nu sunt necesare. În acest sens, GDPR asigură că Prelucrarea de date cu caracter personal pentru care este solicitat consimțământul nu poate deveni direct sau indirect o contraprestație a executării contractului. Cele două temeiuri juridice pentru Prelucrarea de date cu caracter personal în mod legal, și anume consimțământul și contractul, nu pot fi amestecate sau lipsite de claritate.

Constrângerea de a fi de acord cu utilizarea datelor personale în plus față de cele strict necesare limitează opțiunile persoanei vizate și împiedică manifestarea liberă a consimțământului. Având în vedere că Dreptul protecției datelor are ca scop protejarea drepturile fundamentale ale omului, un control al persoanei asupra datelor sale cu caracter personal este esențial și există o prezumție puternică că Consimțământul privind Prelucrarea

[21] Art. 7(4) din GDPR: „Atunci când se evaluează 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." A se vedea și Considerentul 43 din GDPR, care prevede „[...]Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului."

datelor cu caracter personal care nu sunt necesare, nu poate fi văzut ca o cerință obligatorie în schimbul executării contractului sau furnizării unui serviciu.

Prin urmare, când o solicitare de Consimțământ este legată de executarea contractului de către Operator, iar persoana vizată nu dorește să facă datele ei/lui cu caracter personal disponibile în vederea Prelucrării de către Operator, apare riscul ca serviciile solicitate de către aceasta să fie refuzate.

Pentru a evalua dacă apare o asemenea situație de grupare sau legare, este important să se determine care este scopul contractului sau al serviciului. Conform Opiniei nr. 06/2014 a WP29, termenul „necesar pentru executarea contractului" trebuie să fie interpretat strict. Prelucrarea trebuie să fie necesară pentru realizarea contractului în ceea ce privește fiecare persoană vizată, privită individual. Aceasta poate include, de exemplu, procesarea adresei persoanei vizate pentru ca bunurile cumpărate online să poată fi livrate, sau procesarea informațiilor legate de contul de credit pentru a se putea efectua o plată. În contextul legat de forța de muncă, acest motiv poate permite, de exemplu, procesarea datelor referitoare la informațiile salariale și detaliile contului bancar pentru a putea fi plătit salariul persoanei vizate.[22] Trebuie să existe o legătură directă și obiectivă între Prelucrarea de date cu caracter personal și scopul executării contractului.

Dacă un operator urmărește să Prelucreze date cu caracter personal care sunt necesare în fapt pentru executarea în sine contractului, cel mai probabil este că baza legală a acestuia o constituie Art. 6, alin. 1, lit. b) (contractul). În acest caz nu este nevoie să se utilizeze alt temei juridic, precum consimțământul, iar Art. 7 (4) nu se aplică. În ceea ce privește Necesitatea în scopul executării contractului aceasta nu reprezintă un temei juridic în situația Prelucrării unor categorii speciale de date, aspect important în mod special de reținut pentru Operatorii care procesează categorii speciale de date cu caracter personal.[23]

> [Exemplul 6]O bancă solicită consimțământul clienților pentru a le utiliza detaliile de plată în scop de marketing. Această activitate de prelucrare nu este necesară pentru executarea contractului încheiat cu clientul și furnizarea de servicii bancare obișnuite. În situația în care refuzul clientului de a-și da consimțământul cu privire la acest scop al prelucrării ar avea drept consecință refuzul prestării serviciilor bancare, închiderea contului bancar sau majorarea taxei, consimțământul nu poate fi acordat sau retras în mod liber.

Alegerea legiuitorului de a pune accent pe condiționalitate, printre altele, ca o prezumție a lipsei libertății de a consimți, demonstrează nevoia de examinare atentă a condiționalității. Sintagma ,,se ține seama cât mai mult" din articolul 7 (4) GDPR sugerează că este necesară o

[22] Pentru mai multe exemple și informații, a se vedea Opinia nr. 06/2014 privind noțiunea de interes legitim al operatorului de date cu caracter personal sub imperiul Articolului 7 din Directiva 95/46/CE, adoptată de WP29 în data de 9 aprilie 2014, pp. 16-17 (WP 217).
[23] A se vedea și Articolul 9(2) GDPR.

prudență deosebită din partea operatorului atunci când un contract/serviciu implică o cerere conexă de consimțământ pentru prelucrarea datelor cu caracter personal.

Întrucât limbajul articolului 7 (4) nu are stabilește o regulă absolută, ar putea exista excepții limitate în care această condiționalitate nu afectează validitatea consimțământului. Totuși, sintagma ,,presupus" din considerentul 43 indică în mod clar că astfel de cazuri vor reprezenta situații excepționale.

În orice situație, sarcina probei prevăzută la articolul 7 (4) revine operatorului.[24] Această regulă specifică reflectă principiul general al răspunderii în cadrul GDPR. Cu toate acestea, atunci când se aplică articolul 7 (4), operatorului îi va fi mai dificil să demonstreze acordarea consimțământului în mod liber de către persoana vizată.[25]

Operatorul ar putea susține că organizația sa oferă persoanelor vizate posibilitatea unei alegeri reale între un serviciu care include, pe de o parte, consimțământul pentru utilizarea datelor cu caracter personal pentru scopuri adiționale, și un serviciu echivalent care nu implică consimțământul pentru utilizarea datelor pentru alte scopuri, pe de altă parte. Cât timp există posibilitatea de executare a contractului sau de furnizare de către operator a serviciului contractat fără consimțământul acestuia pentru scopuri adiționale, înseamnă că nu există condiționalitate. Cu toate acestea, ambele servicii trebuie să fie cu adevărat echivalente, fără a implica costuri suplimentare.

Pentru a evalua dacă consimțământul este dat în mod liber, nu ar trebui să se țină cont doar de situația specifică a executării unui contract sau de prestare a unui serviciu, astfel cum este descris la articolul 7 (4). Redactarea articolului 7 (4) a fost realizată în mod neexhaustiv prin folosirea sintagmei ,,inter alia", ceea ce înseamnă că pot exista o serie de alte situații care intră sub incidența acestei prevederi. În linii generale, orice element de presiune inadecvată sau de influență a persoanei vizate (care se poate manifesta multe moduri diferite), care împiedică persoana vizată să își exprime voința în mod liber, are ca efect invalidarea consimțământului.

3.1.3. Granularitate

Un serviciu poate implica multiple operațiuni de prelucrare pentru mai multe scopuri. În astfel de cazuri, persoanele vizate ar trebui să aibă libertatea de a alege scopul pe care îl acceptă, fără

[24] A se vedea articolul 7 (1) GDPR - operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

[25] Într-o anumită măsură, introducerea acestui alineat este o codificare a orientărilor existente ale Grupul de lucru „Articolul 29". Potrivit Opiniei nr. 15/2011, atunci când persoana vizată se află într-o relație de dependență cu operatorul de date - datorită naturii relației sau unor circumstanțe speciale - poate exista o prezumție puternică conform căreia libertatea de a consimți este limitată în astfel de contexte (de exemplu, într-o relație de muncă sau dacă prelucrarea datelor este realizată de o autoritate publică). Prin intrarea în vigoare a articolului 7 (4), operatorului îi va fi mai dificil să demonstreze exprimarea consimțământului în mod liber de către persoana vizată. A se vedea: Opinia nr. 15/2011 cu privire la definiția Consimțământului (WP 187), pp. 12-17.

a fi nevoite să consimtă la un pachet de scopuri de prelucrare. Într-un caz concret, potrivit GDPR, poate fi justificată acordarea mai multor consimțăminte în vederea furnizării unui serviciu.

Considerentul 43 aduce o clarificare, consimțământul prezumându-se a nu fi acordat în mod liber în cazul în care procesul/procedura de obținere a consimțământului nu permite persoanelor vizate să acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal (de exemplu, numai pentru anumite operațiuni de prelucrare și nu pentru altele), deși acest lucru este adecvat în cazul particular. Considerentul 32 prevede ,,Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării."

În cazul în care operatorul are mai multe scopuri de prelucrare și nu a încercat să solicite consimțământul separat pentru fiecare scop, există o lipsire de libertate. Această granularitate este strâns legată de necesitatea consimțământului de a fi specific, așa cum se va discuta în secțiunea 3.2 în continuare. Atunci când prelucrarea datelor se realizează pentru mai multe scopuri, soluția pentru a îndeplini condițiile validității consimțământului constă în granularitate, adică separarea acestor scopuri și obținerea consimțământului pentru fiecare scop în parte.

> [Exemplul 7]În cadrul aceleiași solicitări de consimțământ, un vânzător cu amănuntul solicită clienților săi consimțământul de a le utiliza datele pentru a le trimite oferte prin e-mail și pentru a le transmite altor companii din grup. Acest consimțământ nu este unul granular, deoarece nu există consimțământ separat pentru aceste două scopuri distincte, prin urmare consimțământul nefiind valabil.

3.1.4. Prejudiciu

Operatorul trebuie să demonstreze că persoana vizată este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată (considerentul 42). De exemplu, operatorul trebuie să demonstreze că retragerea consimțământului nu conduce la niciun cost pentru persoana vizată și, prin urmare, nu prezintă un dezavantaj clar pentru cei care își retrag consimțământul.

Alte exemple de prejudiciu sunt înșelăciunea, intimidarea, constrângerea sau consecințele negative semnificative în cazul în care persoana vizată nu își dă consimțământul. Operatorul ar trebui să poată demonstra că persoana vizată a realizat o alegere liberă sau reală în privința acordării și a posibilității retragerii consimțământului fără a suferi vreun prejudiciu.

Dacă un operator este capabil să demonstreze că un serviciu include posibilitatea retragerii consimțământului fără a avea consecințe negative, de exemplu fără ca prestarea serviciului să fie afectată în detrimentul utilizatorului, acest lucru îi poate servi pentru a demonstra acordarea consimțământului în mod liber.

3.2. Specific

Articolul 6 (1)(a) confirmă faptul că acordarea consimțământului de către persoana vizată trebuie să fie făcută în raport cu ,,unul sau mai multe scopuri specifice" și că persoana vizată are posibilitatea de a alege în ceea ce privește fiecare dintre ele.[26] Cerința conform căreia consimțământul trebuie să fie ,,specific" urmărește să asigure un grad de control al utilizatorilor și transparență pentru persoana vizată. Această cerință nu a fost modificată de GDPR și rămâne strâns legată de cerința de a fi ,,informat". În același timp, aceasta trebuie interpretată în conformitate cu cerința ,,granularității" pentru obținerea consimțământului în mod ,,liber".[27] În concluzie, pentru a respecta elementul ,,specific", operatorul trebuie să aplice:

(i) specificarea scopului ca garanție împotriva denaturării funcției,

(ii) granularitatea în solicitările de consimțământ, și

(iii) separarea clară a informațiilor legate de obținerea consimțământului pentru prelucrarea datelor față de informațiile referitoare la alte aspecte.

Ad. (i) Potrivit articolului 5 (1) (b) GDPR, obținerea unui consimțământ valabil este întotdeauna precedată de determinarea unui scop specific, explicit și legitim pentru activitatea de prelucrare preconizată.[28] Necesitatea consimțământului specific în combinație cu noțiunea de limitare a scopului prevăzută la articolul 5 (1) (b) funcționează ca o garanție împotriva lărgirii treptate sau a estompării scopurilor pentru care sunt prelucrate datele, după ce persoana vizată a fost de acord cu colectarea inițială a datelor. Acest fenomen, cunoscut și sub denumirea ,,denaturare a funcției", reprezintă un risc pentru persoanele vizate, deoarece poate conduce la o utilizare neprevăzută a datelor cu caracter personal de către operator sau de către terți și la pierderea controlului persoanelor vizate.

Dacă operatorul se bazează pe articolul 6 (1)(a), persoanele vizate trebuie să își dea întotdeauna consimțământul pentru un anumit scop al prelucrării.[29] Conform noțiunii de *limitare a scopului*, articolului 5 (1)(b) și considerentului 32, consimțământul poate să acopere diferite operațiuni, atâta timp cât acestea servesc aceluiași scop. Este evident că un consimțământ specific poate fi obținut numai atunci când persoanele vizate sunt informate în mod specific cu privire la scopurile vizate de utilizare a datelor acestora.

---

[26] Îndrumări suplimentare privind determinarea ,,scopurilor" pot fi găsite în Opinia nr. 3/2013 privind limitarea scopului (WP 203).

[27] Considerentul 43 GDPR enunță că un consimțământ separat pentru diferite operațiuni de prelucrare va fi necesar ori de câte ori se impune. Ar trebui să fie disponibile opțiuni de consimțământ granular pentru a permite persoanelor vizate să își dea consimțământul separat pentru scopuri separate.

[28] A se vedea WP 29 Opinia nr. 3/2013 privind limitarea scopului (WP 203), p. 16: ,,Pentru aceste motive, un scop vag sau general, cum ar fi *îmbunătățirea experienței utilizatorilor*, *scopuri de marketing*, *scopuri de securitate IT* sau *cercetare viitoare* - de obicei nu îndeplinește criteriile de a fi *specific*."

[29] În concordanță cu WP29 Opinia nr. 15/2011 privind definiția consimțământului (WP 187), de exemplu, la p. 17.

Dacă un Operator prelucrează date bazate pe Consimțământ și dorește să prelucreze aceste date pentru un nou scop, operatorul trebuie să solicite un nou consimțământ din partea persoanei vizate pentru noul scop de prelucrare. Consimțământul originar nu va legitima alte sau noi scopuri de prelucrare.

> [Exemplul 8] O rețea de televiziune prin cablu colectează datele personale ale abonaților, pe baza consimțământului acestora, pentru a le prezenta sugestii personale pentru filme noi care le-ar putea prezenta interes în funcție de obiceiurile lor de vizionare. După un timp, rețeaua de televiziune decide că ar dori să le permită terților să trimită (sau să afișeze) publicitate orientată pe baza obiceiurilor de vizionare ale abonatului. Având în vedere acest nou scop, un nou consimțământ este necesar.

Ad. (ii): Modul de exprimare al consimțământului nu trebuie să fie doar granular pentru a îndeplini cerința de „libertate", ci trebuie să întrunească și cerința de „specificitate". Acest lucru înseamnă că un operator care încearcă să obțină consimțământul pentru diferite scopuri ar trebui să ofere o opțiune separată pentru fiecare scop, pentru a permite utilizatorilor să își exprime consimțământul pentru fiecare scop în parte.

Ad. (iii): În cele din urmă, operatorii trebuie să furnizeze informații specifice pentru fiecare solicitare de consimțământ cu privire la datele care sunt prelucrate pentru fiecare scop, astfel încât persoanele vizate să fie conștiente de impactul fiecărei opțiuni pe care o fac. Astfel, persoanele vizate își pot exprima consimțământul în cunoștință de cauză. Această problemă se suprapune cu cerința conform căreia operatorii trebuie să ofere informații clare, după cum se va analiza la paragraful 3.3 de mai jos.

3.3. Informat

GDPR consolidează cerința conform căreia consimțământul trebuie să fie unul dat în cunoștință de cauză. În baza articolului 5 din GDPR, cerința de transparență reprezintă unul dintre principiile fundamentale, strâns legat de principiile echității și legalității. Furnizarea de informații persoanelor vizate înainte de obținerea consimțământului este esențială pentru a le permite să ia decizii în cunoștință de cauză, să înțeleagă cu ce sunt de acord și, de exemplu, să își exercite dreptul de a-și retrage consimțământul. Dacă operatorul nu furnizează informații accesibile, controlul pe care îl are persoana vizată devine iluzoriu, iar consimțământul va fi un temei nevalabil pentru prelucrare.

Consecința nerespectării cerinței privind consimțământul exprimat în cunoștință de cauză, constă în faptul că acesta va fi invalid, iar operatorul ar fi în situația încălcării articolului 6 GDPR.

3.3.1. Cerințele minime pentru un consimțământ „informat"

Pentru ca un consimțământ să fie exprimat în cunoștință de cauză, este necesar ca persoana vizată să fie informată cu privire la anumite elemente care sunt esențiale pentru a se lua o

decizie. Prin urmare, WP29 este de părere că cel puțin următoarele informații sunt necesare pentru obținerea consimțământului valabil:

(i) identitatea operatorului,
(ii) scopul fiecărei operațiuni de prelucrare pentru care se solicită consimțământul[30],
(iii) ce (tip de) date vor fi colectate și utilizate;[31]
(iv) existența dreptului de retragere a consimțământului,[32]
(v) informații privind utilizarea datelor pentru deciziile bazate exclusiv pe prelucrarea automatizată, inclusiv profilul, în conformitate cu articolul 22 (2)[33] și
(vi) dacă Consimțământul se referă la transferuri, cu privire la posibilele riscuri de transfer de date către țări terțe, în absența unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate [articolul 49 (1)(a)].[34]

În ceea ce privește punctele (i) și (iii), WP29 constată că într-un caz în care mai mulți operatori (asociați) trebuie să se bazeze pe consimțământul solicitat sau dacă datele urmează să fie transferate sau prelucrate de alți operatori care doresc să se bazeze pe consimțământul originar, toate aceste organisme trebuie să fie nominalizate. Persoanele împuternicite de operatori nu trebuie să fie identificate, ca și parte a cerințelor ce privesc consimțământul, deși pentru a se conforma articolelor 13 și 14 GDPR, operatorii trebuie să furnizeze o listă completă a destinatarilor sau a categoriilor de destinatari, inclusiv a persoanelor împuternicite de operatori. În concluzie, WP29 constată că, în funcție de circumstanțele și contextul fiecărui caz, pot fi necesare mai multe informații pentru a permite persoanei vizate să înțeleagă cu adevărat activitățile de prelucrare aflate în discuție.

3.3.2. Cum să furnizezi informațiile

GDPR nu stabilește modul sau forma în care trebuie furnizate informațiile pentru a fi îndeplinită cerința privind exprimarea unui consimțământului informat. Aceasta înseamnă că informațiile valide pot fi prezentate în moduri diferite, cum ar fi declarații scrise sau orale sau mesaje audio sau video. Cu toate acestea, GDPR stabilește mai multe cerințe pentru existența unui consimțământul informat, în special în articolul 7 (2) și în considerentul 32. Acestea conduc la un standard mai ridicat pentru claritatea și accesibilitatea informației.

[30] A se vedea, de asemenea, considerentul 42 GDPR.
[31] A se vedea, de asemenea, Opinia WP29 15/2011 privind definiția consimțământului (WP 187) pp. 19-20.
[32] A se vedea, de exemplu, considerentul 42 din GDPR: „[...] Pentru ca acordarea consimțământului să fie în cunoștință de cauză, persoana vizată ar trebui să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal”.
[33] A se vedea, de asemenea, Orientările WP29 privind luarea deciziei individuale automatizate și profilarea în sensul Regulamentului 2016/679 (WP251), paragraful IV.B, p. 20 și următoarele.
[34] A se vedea, de asemenea WP29 Opinia nr. 15/2011 privind definiția consimțământului (WP 187) p. 19

Atunci când solicită consimțământul, operatorii trebuie să se asigure că folosesc un limbaj clar în toate cazurile. Aceasta înseamnă că un mesaj ar trebui să fie ușor de înțeles pentru o persoana obișnuită și nu numai pentru avocați. Operatorii nu pot folosi politici de confidențialitate lungi și ilizibile sau declarații pline de expresii juridice. Consimțământul trebuie să fie clar și ușor de distins de alte chestiuni și să fie exprimat într-o formă inteligibilă și ușor accesibilă. Această cerință înseamnă, în esență, că informațiile relevante pentru luarea unor decizii în cunoștință de cauză privind acordarea sau nu a consimțământului nu pot fi ascunse în termeni și condiții generale.[35]

Operatorul trebuie să se asigure că consimțământul este furnizat pe baza informațiilor care permit persoanelor vizate să identifice cu ușurință cine este operatorul și să înțeleagă cu ce sunt de acord. Operatorul trebuie să descrie în mod clar scopul prelucrării datelor pentru care se solicită consimțământul.[36]

Alte instrucțiuni specifice privind accesibilitatea au fost stabilite în Orientările WP29 privind transparența. În cazul în care consimțământul trebuie dat prin intermediul mijloacelor electronice, cererea trebuie să fie clară și concisă. Informațiile granulare și stratificate pot fi o modalitate adecvată de a face față obligației duale de a fi precise și complete, pe de o parte, și ușor de înțeles pe de altă parte.

Operatorul trebuie să evalueze publicul țintă care furnizează date personale organizației respective. De exemplu, în cazul în care publicul țintă include persoane vizate minore, este de așteptat ca operatorul să se asigure că informațiile sunt ușor de înțeles pentru minori.[37] După identificarea publicului țintă, operatorii trebuie să stabilească ce informații trebuie să furnizeze și, ulterior, cum vor prezenta acele informații persoanelor vizate.

Articolul 7 (2) reglementează cu privire la declarațiile de consimțământ scrise și ante-redactate care privesc alte probleme. Atunci când acordul este solicitat ca parte a unui contract (pe format fizic), cererea de consimțământ trebuie să fie într-o formă care o diferențiază în mod clar de celelalte aspecte. Dacă contractul pe suport de hârtie cuprinde multe aspecte care nu sunt în legătură cu chestiunea consimțământului privind datele cu caracter personal, problematica consimțământului ar trebui soluționată într-un mod foarte aparte, sau într-un document separat. De asemenea, în cazul în care consimțământul este solicitat prin mijloace electronice, cererea de consimțământ trebuie să fie separată și distinctă, nu poate fi pur și simplu un paragraf cuprins în termeni și condiții, în temeiul Considerentului 32[38]. Pentru a se

[35] Declarația de consimțământ trebuie menționată ca atare. Redactarea, cum ar fi „Știu că ...” nu îndeplinește cerința unui limbaj clar.

[36] A se vedea articolul 4 (11) și articolul 7 (2) din GDPR.

[37] A se vedea, de asemenea, considerentul 58 privind informațiile ușor de înțeles pentru copii.

[38] A se vedea, de asemenea, Considerentul 42 și directiva 93/13/CE, în special articolul 5 (într-o formă inteligibilă, iar în caz de îndoieli, interpretarea se va face în favoarea consumatorului) și articolul 6 (nevalabilitatea clauzelor abuzive, contractul continuă să existe chiar și fără acești termeni numai în

potrivi cu ecranele de mici dimensiuni sau cu situații unde spațiul pentru prezentarea informațiilor este restrâns, se poate lua în considerare, dacă este adecvat, o metodă stratificată de prezentare a informațiilor, pentru a evita perturbarea excesivă a experienței utilizatorului sau a designului produsului.

Un operator care se bazează pe consimțământul persoanei vizate trebuie, de asemenea, să se ocupe separat de obligațiile de informare prevăzute de articolele 13 și 14 astfel încât să existe conformitatea cu GDPR. În practică, conformitatea cu obligațiile de informare și cu cerința informării consimțământului poate conduce, în multe cazuri, la o abordare integrată. Cu toate acestea, această secțiune este scrisă în sensul soluției că există Consimțământ valabil ,,informat", chiar dacă nu sunt menționate toate elementele articolelor 13 și/sau 14 în procesul de obținere a consimțământului (aceste puncte ar trebui, bineînțeles, menționate în alte locuri, cum ar fi notificarea privind confidențialitatea companiei). WP29 a emis orientări distincte în privința cerinței de transparență.

> [Exemplul 9] Compania X este un operator care a primit plângeri că nu este clar pentru persoanele vizate în ce scopuri de utilizare a datelor li se cere să consimtă. Compania consideră că este necesar să se verifice dacă informațiile sale cuprinse în cererea de consimțământ sunt ușor de înțeles pentru persoanele vizate. X organizează panouri de testare voluntară pentru anumite categorii de clienți și prezintă noile actualizări ale informațiilor privitoare la consimțământ acestor audiențe (de testare) înainte de a le comunica în exterior. Selectarea panourilor respectă principiul independenței și este făcută pe baza unor standarde care asigură un rezultat reprezentativ și imparțial. Grupul primește un chestionar în care să indice ce au înțeles din informațiile prezentate și cum ar nota acestea prin prisma informațiilor relevante și ușor de înțeles. X întocmește un raport ca urmare a testului și îl păstrează pentru referințe ulterioare. Acest exemplu arată o posibilă modalitate pentru ca X să demonstreze că persoanele vizate primesc informații clare înainte de a consimți la prelucrarea datelor cu caracter personal de către X.
>
> [Exemplul 10] O companie prelucrează date cu caracter personal în baza consimțământului. Compania utilizează o notificare de confidențialitate stratificată care include și o solicitare de consimțământ. Compania face publice toate detaliile de bază ale operatorului și ale activităților de prelucrare a datelor avute în vedere[39]. Cu toate

---

cazul în care poate continua să existe fără clauzele abuzive; în caz contrar, întreg contractul nu este valid).

[39] De reținut că atunci când identitatea operatorului sau scopul prelucrării nu sunt exteriorizate (vizibile-n.t.) din primul strat de informație al notei stratificate de confidențialitate (ci se află în sub-straturi ulterioare), va fi dificil pentru operatorul de date să demonstreze că persoana vizată și-a dat consimțământul în cunoștință de cauză, cu excepția cazului în care operatorul de date poate să demonstreze că persoana vizată la care ne referim, a accesat aceste informații înainte de a își da consimțământul.

acestea, compania nu indică modul în care poate fi contactat Responsabilul cu protecția datelor în notificare. În scopul de a avea o bază legală după cum este menționat în articolul 6, acest operator a obținut un consimțământ ,,în cunoștință de cauză" valid, chiar și atunci când datele de contact ale responsabilului cu protecția datelor nu au fost comunicate persoanei vizate prin (primul nivel de informare al) această notificare de confidențialitate, în conformitate cu articolul 13 (1)(b) sau articolul 14 (1)(b) din GDPR.

3.4. Indicarea lipsită de ambiguitate a Voinței

GDPR prevede clar că consimțământul necesită o declarație din partea persoanei vizate sau un act afirmativ clar ceea ce înseamnă că trebuie să fie dat întotdeauna printr-o manifestare activă de voință sau printr-o declarație. Trebuie să fie evident că persoana vizată și-a dat consimțământul pentru o anumită Prelucrare.

Articolul 2 (h) din Directiva 95/46/CE descrie consimțământul drept o „manifestare de voință, liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc." Articolul 4 (11) din GDPR se bazează pe această definiție, clarificând faptul că acordul valabil exprimat necesită o manifestare de voință *lipsită de ambiguitate* prin intermediul unei declarații sau printr-o acțiune afirmativă clară, în conformitate cu îndrumările anterioare emise de WP29.

Un „act afirmativ clar" înseamnă că persoana vizată trebuie să fi luat o acțiune deliberată pentru consimțirea la acea prelucrare specifică[40]. Considerentul 32 stabilește îndrumări suplimentare în acest sens. Consimțământul poate fi obținut printr-o declarație scrisă sau o declarație orală (înregistrată), inclusiv prin mijloace electronice.

[40] A se vedea ,,Commission Staff Working Paper" (Documentul de lucru al serviciilor Comisiei), Evaluarea de impact, Anexa 2, p. 20 și, de asemenea, pp. 105-106: ,,Așa cum s-a subliniat și în punctul de vedere al WP29 asupra consimțământului, este esențial să se clarifice faptul că Consimțământul valabil necesită utilizarea de mecanisme care nu lasă nici o îndoială cu privire la intenția persoanei vizate de a consimți, în timp ce clarifică faptul că – în contextul mediului online – utilizarea opțiunilor standard pe care persoana vizată trebuie să le modifice pentru a respinge prelucrarea (,,consimțământul bazat pe tăcere") nu constituie, în sine, un consimțământ neechivoc". Acest lucru ar da indivizilor mai mult control asupra propriilor date, ori de câte ori prelucrarea se bazează pe consimțământul acestora. În ceea ce privește impactul asupra operatorilor de date, acest lucru nu ar avea un impact major, deoarece clarifică și clarifică mai bine implicațiile Directivei curente în raport cu condițiile pentru un consimțământ semnificativ și valabil exprimat din partea persoanei vizate. În mod aparte, până la măsura în care consimțământul ,,explicit" ar clarifica – prin înlocuirea ,,neechivoc" - modalitățile și calitatea consimțământului și că nu intenționează să se extindă și asupra cazurilor și situațiilor în care (în mod explicit) consimțământul ar trebui folosit ca temei pentru prelucrare, impactul acestei măsuri asupra operatorilor de date nu este de așteptat să fie major.

Poate că modul cel mai literal pentru a îndeplini criteriul unei „declarații scrise” este de a vă asigura că persoana vizată scrie o scrisoare sau un e-mail către operator explicând exact cu ce este de acord. Cu toate acestea, acest lucru cel mai adesea nu este realist. Declarațiile scrise pot fi în variate forme și dimensiuni care ar putea fi conforme cu GDPR.

Fără a aduce atingere legislației contractuale (naționale) în vigoare, consimțământul poate fi obținut printr-o declarație orală înregistrată, deși trebuie să se țină seama de informațiile disponibile pentru persoana vizată, înainte de manifestarea consimțământului. Utilizarea casetelor de înscriere pre-bifate nu este validă odată cu prevederile GDPR. Tăcerea sau lipsa de activitate din partea persoanei vizate, precum și simpla continuare a utilizării unui serviciu nu pot fi considerate ca o manifestare activă a opțiunii acesteia.

> [Exemplul 11] La instalarea software-ului, aplicația solicită persoanei vizate consimțământul să utilizeze rapoarte de defectare a sistemului fără a fi anonime, pentru îmbunătățirea software-ului. Anunțul de confidențialitate stratificat care furnizează informațiile necesare însoțește solicitarea Consimțământului. Prin bifarea căsuței opționale care prevede că „consimt”(I consent –ad.t.), utilizatorul poate să îndeplinească în mod valabil un „act afirmativ clar” pentru a consimți prelucrarea.

Un operator de date trebuie, de asemenea, să țină cont cu precauție de faptul că consimțământul nu poate fi obținut prin aceeași propunere cu aceea de a accepta contractarea sau acceptarea termenilor și condițiilor unui serviciu. Acceptarea în alb a termenilor și condițiilor generale nu poate fi văzută ca o acțiune afirmativă clară de a consimți la utilizarea datelor cu caracter personal. GDPR nu permite Operatorilor să pună la dispoziție casete ante-bifate sau modalități de tip „excludere voluntară”(Opt-out) care pretind o intervenție din partea persoanei vizate pentru a împiedica realizarea acordului (de exemplu, casete de tip „excludere voluntară”- „opt-out boxes”)[41].

3.4.1. Consimțământ în format electronic

În cazul în care Consimțământul trebuie acordat în urma unei cereri transmise în format electronic, solicitarea consimțământului nu ar trebui să perturbe *în mod inutil* utilizarea serviciului pentru care se acordă consimțământul.[42] O acțiune neechivocă prin care persoana vizată își manifestă consimțământul poate fi necesară în situația în care o altă metodă care să încalce ori afecteze mai puțin drepturile persoanei poate crea ambiguitate. Așadar, ar putea fi necesar ca solicitarea consimțământului să întrerupă activitatea utilizatorului într-o anumită măsură, pentru ca cererea să fie efectivă.

Totuși, potrivit cerințelor GDPR, operatorii au libertatea de a dezvolta un flux de obținere a consimțământului care se potrivește organizației lor. În acest sens, faptele fizice pot fi calificate ca o acțiune afirmativă clară în conformitate cu GDPR.

---

[41] A se vedea Articolul 7(2). A se vedea și Documentul de Lucru nr. 02/2013 privind obținerea consimțământului pentru cookies(WP 208), pp. 3-6.

[42] A se vedea considerentul 32 GDPR.

[Exemplul 12] Glisarea pe ecran, a face cu mâna în fața unei camera smart, a învârti telefonul smart în sensul acelor de ceasornic sau în forma opt, pot fi modalități prin care se manifestă acceptarea, atâta timp cât sunt furnizate informații clare și este clar că fapta în cauză reprezintă acceptare pentru o anume solicitare (ex. Dacă se glisează în stânga, accepți utilizarea informației X pentru scopul Y. Repetă mișcarea pentru a confirma.) Operatorul trebuie să poată demonstra că a fost obținut consimțământul în această modalitate și persoana vizată trebuie să poată să își retragă consimțământul la fel de ușor cum l-a exprimat.

[Exemplul 13] Plimbarea cursorului în jos sau glisarea prin termenii și condițiile care includ declarația consimțământului (în situația în care pe ecran apare o alertă prin care i se aduce la cunoștință persoanei vizate că plimbarea cursorului în jos reprezintă consimțământ) nu satisface cerința unei acțiuni clare și afirmative. Asta se întâmplă deoarece alerta poate fi omisă de către persoana vizată atunci când plimbă cursorul repede prin texte ample și o astfel de acțiune nu este suficient de clară. În contextul digital, multe servicii au nevoie de datele cu caracter personal pentru a funcționa, deci, persoanele vizate primesc o multitudine de cereri privind acordarea consimțământului în baza unui click sau a unei glisări, în fiecare zi. Aceasta poate rezulta, într-o oarecare epuizare în urma click-urilor: când este întâlnit de prea multe ori, efectul de prevenire propriu-zis al mecanismelor de acordare a consimțământului se diminuează.

Aceasta rezultă într-o situație în care cererile privind consimțământul nu mai sunt citite. Acesta este un risc aparte pentru persoanele vizate deoarece, de obicei, consimțământul este cerut pentru acțiuni care sunt de principiu nelegale fără acest consimțământ. GDPR pune în sarcina operatorilor obligația de a dezvolta modalități de combatere a acestei probleme. Un exemplu des menționat pentru a realiza asta în contextul online este obținerea consimțământului utilizatorului de internet prin setările browser-ului. Asemenea setări ar trebui dezvoltate în concordanță cu condițiile pentru un consimțământ valabil potrivit GDPR, cum ar fi de exemplu că consimțământul ar trebui să fie particular pentru fiecare scop avut în vedere și că informația care trebuie oferită, ar trebui să numească operatorii.

În orice caz, consimțământul trebuie întotdeauna obținut înainte ca operatorul să înceapă procesarea datelor cu caracter personal pentru care consimțământul este necesar. WP29 a susținut în mod constant în opiniile anterioare că consimțământul ar trebui acordat anterior activității de procesare.[43] Deși GDPR nu prevede în mod literar în articolul 4(11) că consimțământul trebuie dat anterior activității de procesare, aceasta se presupune în mod clar.

Teza introductivă a articolului 6(1) și folosirea cuvintelor „și-a dat” în articolul 6(1)(a) susțin această interpretare. Este logic dedus din articolul 6 și din considerentul 40 că un temei juridic valid trebuie să existe înainte de începerea procesării datelor. Așadar, consimțământul ar trebui

[43] WP29 și-a susținut această interpretare potrivit Opiniei nr. 15/2011 privind consimțământul (WP189), p. 30-31.

dat anterior activității de procesare. În principiu, poate fi suficient ca persoanei vizate să îi fie cerut consimțământul o singură dată. Totuși, operatorii trebuie să obțină un consimțământ nou și specific dacă scopul procesării datelor se modifică după ce consimțământul a fost obținut sau dacă un nou scop este avut în vedere.

4. Obținerea consimțământului explicit

Consimțământul explicit este necesar în anumite situații în care apare riscul în ceea ce privește protecția datelor, deci, unde un nivel ridicat de control asupra datelor necesare este considerat oportun. Potrivit GDPR, consimțământul explicit joacă un rol în articolul 9 referitor la Prelucrarea de categorii speciale de date cu caracter personal, în prevederile referitoare la transferul datelor către țări terțe sau organizații internaționale în lipsa garanțiilor adecvate din articolul 49[44] și în articolul 22 privind Procesul decizional individual automatizat, inclusiv crearea de profiluri.[45]

GDPR indică faptul că o „acțiune neechivocă" este o condiție prealabilă pentru consimțământul „obișnuit". Având în vedere că consimțământul „obișnuit" este deja ridicat la un standard înalt în GDPR în comparație cu consimțământul din Directiva 95/46/EC, trebuie clarificat ce eforturi suplimentare sunt necesare să întreprindă operatorul pentru a obține consimțământul explicit al unei persoane vizate în concordanță cu GDPR. Termenul explicit se referă la modul în care consimțământul este exprimat de către persoana vizată. Asta înseamnă că persoana vizată trebuie să dea o declarație expresă de consimțământ. Un mod evident de a fi sigur că consimțământul este explicit ar fi exprimarea expresă a consimțământului printr-o declarație scrisă. Când se consideră oportun, operatorul se poate asigura că declarația scrisă este semnată de persoana vizată, pentru a înlătura orice dubiu posibil și o eventuală lipsă de dovadă pentru viitor. [46]

Totuși, o astfel de declarație semnată nu este singura metodă de a obține un consimțământ explicit și nu poate fi susținut că GDPR presupune declarații scrise și semnate în toate

[44] Potrivit art. 49(1)(a) GDPR, consimțământul explicit poate ridica interdicția transferului de date către țări care nu oferă un nivel adecvat de protecție a datelor. A se lua în considerare și documentul privind interpretarea comună a art. 26(1) din Directiva 95/46/EC din 24 octombrie (WP 114), p. 11, în care WP29 a indicat faptul că consimțământul pentru transferul datelor care are loc periodic sau în baza unui temei constant este neadecvat.

[45] În articolul 22, GDPR introduce prevederi pentru a proteja persoanele vizate împotriva deciziilor individuale automatizate, inclusiv crearea de profiluri. Deciziile luate în baza acestui temei sunt permise doar dacă îndeplinesc anumite cerințe legale. Consimțământul joacă un rol cheie în acest mecanism de protecție, având în vedere că art. 22 (2)(c) GDPR prevede clar că un operator poate procesa în baza deciziilor individuale automatizate, inclusiv crearea de profiluri, care pot afecta individul în mod semnificativ, în baza consimțământului explicit. WP29 a realizat ghiduri separate pentru aceste probleme: Ghidul(Orientările) WP29 privind Procesul decizional individual automatizat, inclusiv crearea de profiluri în baza scopurilor Regulamentului, 3 Octombrie 2017 (WP 251).

[46] A se avea în vedere și Opinia nr. 15/2011 a WP29 privind definiția consimțământului (WP 187), p. 25.

circumstanțele care necesită consimțământ expres valabil. De exemplu, în contextul digital și online, persoana vizată are posibilitatea de a emite declarația cerută prin completarea unui formular electronic, prin trimiterea unui e-mail, prin încărcarea unui document scanat care poartă semnătura persoanei vizate. În teorie, utilizarea declarațiilor orale poate fi suficientă pentru a obține consimțământ explicit valabil, deși, poate fi dificil de dovedit de către operator că au fost îndeplinite condițiile pentru un consimțământ explicit valabil în momentul obținerii declarației.

> [Exemplul 14] O clinică pentru chirurgie estetică solicită consimțământul explicit din partea unui pacient pentru transferarea dosarului său medical către un expert căruia i se solicită o a doua opinie asupra stării pacientului. Dosarul medical este un fișier digital. Dat fiind natura specifică a informațiilor în cauză, clinica solicită semnătura electronică a persoanei vizate pentru obținerea consimțământului explicit valabil și pentru posibilitatea demonstrării faptul că s-a obținut consimțământul explicit.[47]

Verificarea în două etape a consimțământului poate fi, de asemenea, o modalitate de a asigura valabilitatea consimțământului valabil. De exemplu, o persoană vizată primește un e-mail care îl notifică cu privire la intenția operatorului de a prelucra o înregistrare conținând informații medicale. Operatorul explică în e-mail că solicită consimțământul pentru utilizarea unui anumit set de informații pentru un anumit scop. Dacă persoana vizată este de acord cu utilizarea acestor informații, operatorul îi solicită răspunsul printr-un e-mail conținând declarația „Sunt de acord." În urma trimiterii răspunsului, persoana vizată primește un link de verificare pe care trebuie făcut clic, sau un mesaj SMS cu un cod de verificare, pentru confirmarea acordului.

Trebuie reamintit că existența consimțământului explicit nu este singura modalitate de a justifica prelucrarea datelor din categorii speciale, anumite transferuri de date etc. Consimțământul explicit nu este întotdeauna adecvat într-o situație specifică, iar GDPR enumeră celelalte câteva posibilități pentru asigurarea că aceste activități se pot desfășura într-o manieră legală. De exemplu, articolul 9 (2) enumeră nouă alte temeiuri juridice pentru ridicarea interdicției de prelucrare a categoriilor speciale de date.

5. Condiții suplimentare pentru obținerea consimțământului valabil

GDPR introduce cerințe pentru ca operatorii să desfășoare mecanisme suplimentare pentru asigurarea că obțin, mențin și pot demonstra consimțământul valabil. Art. 7 GDPR stabilește aceste condiții suplimentare pentru valabilitatea consimțământului, cu prevederi specifice asupra păstrării înregistrărilor consimțământului și a dreptului de retragere a consimțământului în mod facil. Articolul 7 se aplică, de asemenea, consimțământului la care se face referire în alte

[47] Acest exemplu nu aduce atingere Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2016 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă.

articole ale GDPR, de ex. Articolele 8 și 9. Recomandări privind cerințele suplimentare pentru demonstrarea consimțământului valabil și asupra retragerii consimțământului sunt oferite mai jos.

5.1. Demonstrarea consimțământului

În articolul 7 (1), GDPR subliniază clar obligația explicită a operatorului de a demonstra consimțământul persoanei vizate. Sarcina probei revine operatorului, potrivit articolului 7 (1).

Considerentul 42 prevede: „În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare."
Operatorii au libertatea de a dezvolta metode pentru a respecta prevederea într-o modalitate potrivită operațiilor lor zilnice. În același timp, obligația de a demonstra obținerea consimțământului valabil de către operator nu ar trebui să conducă în sine la volume excesive de date suplimentare de prelucrat. Acest lucru înseamnă că operatorii ar trebui să aibă destule date pentru a prezenta o legătură cu prelucrarea (pentru a prezenta obținerea consimțământului), dar nu ar trebui să colecteze mai multe informații decât este necesar.

Este de datoria operatorului să dovedească obținerea consimțământului de la persoana vizată. GDPR nu stabilește exact cum trebuie acest lucru realizat. Cu toate acestea, operatorul trebuie să poată dovedi că o persoană vizată și-a dat consimțământul, într-o situație specifică. Atât timp cât o activitate de prelucrare de date în cauză durează, există obligația de demonstrare a consimțământului. La încheierea activității de prelucrare a datelor, dovada consimțământului ar trebui păstrată doar atât cât este necesar pentru respectarea obligațiilor legale sau pentru stabilirea, exercitarea sau apărarea drepturilor în justiție, potrivit articolului 17 (3)(b) și (3)(e).

De exemplu, operatorul poate păstra o evidență a declarațiilor de consimțământ primite, pentru a putea prezenta modul de obținere a consimțământului, momentul obținerii consimțământului și posibilitatea de demonstrare a informațiilor furnizate persoanei vizate la momentul respectiv. Operatorul trebuie să poată, de asemenea, demonstra că persoana vizată a fost informată și fluxul de lucru al operatorului îndeplinește toate criteriile relevante pentru consimțământul valabil. Raționamentul ce stă la baza acestei obligații în GDPR este faptul că operatorii trebuie să fie responsabili cu privire la obținerea consimțământului valabil de la persoanele vizate, și cu privire la mecanismele instituite de către ei. De exemplu, într-un context online, un operator ar putea păstra informații într-o sesiune în care consimțământul a fost exprimat, împreună cu documentația fluxului de lucru privind consimțământul la momentul sesiunii, precum și o copie a informației prezentate persoanei vizate la momentul respectiv. Nu este suficientă simpla referire la configurația corectă a site-ului respectiv.

> [Exemplul 15]Un spital instituie un program de cercetare științifică, numit proiectul X, pentru care sunt necesare dosarele dentare ale pacienților reali. Participanții se recrutează prin intermediul apelurilor telefonice către pacienți care au fost de acord în mod voluntar să figureze pe o listă de candidați care pot fi abordați pentru acest scop.

Operatorul solicită consimțământul explicit de la persoanele vizate pentru utilizarea dosarelor lor dentare. Consimțământul se obține în timpul unui apel telefonic prin înregistrarea unei declarații orale a persoanei vizate, în care aceasta confirmă acordul cu utilizarea datelor lor pentru scopul proiectului X.

Nu există o **limită temporală** în GDPR pentru durata consimțământului ca cerință de valabilitate. Durata consimțământului depinde de context, domeniul de aplicare a consimțământului inițial și așteptările persoanei vizate. Dacă operațiunile de prelucrare se modifică sau evoluează considerabil, atunci consimțământul inițial nu mai este valabil. În acest caz, trebuie obținut un consimțământ nou.

Grupul de lucru „Articolul 29" recomandă ca bune practici reînnoirea consimțământului la intervale adecvate. Oferirea tuturor informațiilor de asemenea ajută la asigurarea că persoana vizată este bine informată despre modul în care datele lor sunt utilizate și cum își exercită drepturile.[48]

5.2 Retragerea consimțământului

Un loc important în GDPR îl ocupă retragerea consimțământului. Dispozițiile si considerentele ce fac referire la retragerea consimțământului în GPDR pot fi luate în considerare ca o codificare a unei interpretări deja existente a acestei probleme în Opiniile WP29.[49]

Articolul 7 (3) GDPR prevede faptul că operatorul trebuie să se asigure că, consimțământul persoanei vizate poate fi retras în orice moment la fel de ușor ca și când a fost dat. GDPR nu prevede că acordarea și retragerea consimțământului trebuie realizate întotdeauna prin același tip de acțiune.

Cu toate acestea, când consimțământul este obținut prin mijloace electronice doar prin folosirea unui click al mouse-ului, o glisare sau o atingere, persoana vizată trebuie, în practică, să aibă posibilitatea de a-și retrage consimțământul la fel de ușor cum l-a dat. Când consimțământul este obținut prin folosirea unei interfețe de utilizator specifice domeniului de activitate (exemplu, la un website, o aplicație, o logare într-un cont, interfața unui dispozitiv IoT sau prin E-mail), persoana vizată trebuie să-și poată retrage consimțământul prin aceeași interfață prin care l-a acordat fără nici un dubiu, deoarece schimbarea interfeței respective doar pentru retragerea consimțământului ar reprezenta efort nejustificat. Mai mult decât atât, persoana vizată ar trebui să-și poată retragă consimțământul fără nici un prejudiciu. Această

[48] A se vedea Orientările WP29 privind transparența (citările vor fi finalizate când sunt disponibile).
[49] WP 29 a dezbătut acest subiect în Opinia cu privire la consimțământ (a se vedea Opinia nr. 15/2011 privind definiția consimțământului (WP 187), pp. 9, 13, 20, 27 și 32-33) și, printre altele, Opinia privind folosirea datelor de localizare. [a se vedea Opinia nr. 5/2005 cu privire la folosirea datelor de localizare în scopul de a oferi un plus de valoare serviciilor (WP 115), p. 7].

înseamnă că, printre altele, operatorul trebuie să facă posibilă retragerea consimțământului fără a fi nevoie de o plată adițională sau fără scăderea calității serviciului.[50]

> [Exemplul 16] Un festival de muzică vinde bilete de intrare prin intermediul unui agent online de bilete. Cu fiecare bilet vândut, consimțământul este cerut pentru a se folosi datele de contact în scopuri de marketing. Pentru a-și oferi consimțământul pentru acest scop, clienții pot selecta fie Nu, fie Da. Operatorul de date cu caracter personal informează clienții privind posibilitatea acestora de a-și retrage consimțământul. Pentru a face acest lucru, clienții trebuie să contacteze gratuit un centru de apeluri, în zilele lucrătoare între orele 8-17. În exemplul anterior operatorul nu se conformează cu Articolul 7 (3) GDPR. Retragerea consimțământului în acest caz îl constituie un apel efectuat în programul de lucru, însemnând o procedură mai împovărătoare decât o apăsare de mouse necesară pentru oferirea consimțământului prin chioșcul online de bilete, care e deschis 24/7.

Cerințele unei ușoare retrageri (a consimțământului) sunt descrise ca fiind aspecte necesare de validare a consimțământului în GDPR. În cazul în care dreptul la retragerea consimțământului nu îndeplinește cerințele impuse de GPDR, atunci mecanismul operatorului cu privire la consimțământ nu se conformează cu GDPR. Cum este menționat în secțiunea 3.1 cu privire la condițiile unui consimțământ informat, operatorul trebuie să informeze persoana vizată cu privire la dreptul lui/ei de a-și retrage consimțământul chiar în prealabil de a își exprima acordul în temeiul Articolului 7 (3) GDPR. În plus, operatorul are obligația de a informa persoanele vizate în privința exercitării drepturilor în temeiul obligației de transparență.[51]

Ca regulă generală, dacă consimțământul este retras, toate operațiile procesate care s-au bazat pe acesta și au avut loc înaintea retragerii – și în concordanță cu GDPR – rămân legale, dar, operatorul trebuie să oprească toate acțiunile de procesare respective.[52]

La fel cum s-a menționat anterior în aceste ghiduri, este foarte important ca operatorul de date să evalueze scopul pentru care datele personale sunt de fapt procesate și bazele legale pe care se bazează procesarea, anterior colectării de date. În multe cazuri, companiile au nevoie de date cu caracter personal pentru mai multe scopuri, iar Prelucrarea acestora se bazează pe mai multe temeiuri juridice, de exemplu, datele personale ale clienților ar putea fi folosite în contract și cu privire la consimțământ. În consecință, o eventuală retragere a consimțământului nu duce la obligația operatorului la ștergerea datelor care sunt procesate pentru scopul de a

[50] A se vedea și WP29 Opinia nr. 4/2010 privind Codul de Conduită European al FEDMA în privința utilizării de date cu caracter personal în marketingul direct (WP 174) și Opinia cu privire la folosirea datelor de localizare în scopul de a oferi un plus valoare serviciilor (WP 115).

[51] Considerentul 39 GDPR ce face referire la Articolele 13 și 14 din Regulament, statuează că „persoanele fizice ar trebui informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea."

[52] A se vedea Articolul 17 (1)(b) și (3).

duce la executarea contractului cu persoana vizată. Operatorii prin urmare, ar trebui să știe de la bun început care este scopul aplicabil pentru fiecare element de date cu caracter personal și pe ce temei juridic se bazează.

Pe lângă obligația operatorului de a șterge datele care au fost procesate pe bază de consimțământ odată ce acesta a fost retras, o persoana fizică vizată are posibilitatea de a cere ștergerea altor date cu privire la persoana lui care încă sunt în posesia operatorului, de exemplu, în temeiul Articolului 6 (1)(b). În acest scop, persoana vizată ar trebui să-și exercite dreptul de a-și avea datele personale șterse, așa cum este prevăzut de Articolul 17 (1)(b) și în Considerentul 65. WP 29 recomandă operatorilor de a evalua dacă continuarea procesării datelor personale respective este adecvată, chiar și în absența unei cereri de ștergere a datelor din partea persoanei vizate.

În cazurile în care persoana vizată își retrage consimțământul iar operatorul de date dorește să continue procesarea datelor cu caracter personal bazându-se pe un alt temei juridic, aceștia nu pot trece de la consimțământ (care este retras) la un alt temei legal. Mai mult decât atât, orice schimbare a temeiului legal trebuie notificată persoanei vizate în concordanță cu obligațiile de raportare prevăzute în Articolele 13 și 14 și de principiul general al transparenței.

6. Interacțiunea dintre consimțământ și alte temeiuri legale în baza Articolului 6 GDPR

Articolul 6 stabilește condițiile pentru o Prelucrare legală a datelor cu caracter personal și enunță șase temeiuri juridice pe care operatorul se poate baza. Utilizarea unuia dintre aceste șase temeiuri juridice trebuie stabilită anterior procesării și în relație cu un scop clar definit. Ca regulă generală, o activitate de procesare pentru un anumit scop specific, nu poate fi bazată pe mai multe temeiuri juridice. Cu toate acestea, este posibil ca operatorul să se bazeze pe mai multe temeiuri juridice pentru a justifica procesarea, dacă datele în cauză sunt folosite pentru mai multe scopuri deoarece fiecare scop al procesării trebuie să se lege de o bază legală. Cu toate acestea, operatorul trebuie să identifice aceste scopuri și bazele legale aferente anterior procesării. Temeiul legal al procesării nu poate fi modificat în cursul acesteia. În consecință, operatorul nu poate trece de la un temei legal la altul. De exemplu, nu este permisă utilizarea retroactivă a interesului legitim pentru a justifica procesarea, unde au fost întâmpinate probleme privind validitatea consimțământului. Prin urmare, sub imperiul GDPR, operatorii care cer consimțământul persoanelor vizate pentru a le utiliza datele cu caracter personal, în principiu, nu ar trebui să se poată baza pe un alt temei legal privind Articolul 6 ca un plan de rezervă chiar și atunci când aceștia nu pot demonstra, în raport de GDPR, conformitatea oferirii consimțământului de către persoana vizată sau dacă consimțământul valabil a fost retras ulterior. Prin prisma obligației de a divulga temeiurile juridice pe baza cărora operatorul acționează la momentul în care se colectează datele cu caracter personal, acesta trebuie să se decidă în prealabil colectării, care sunt bazele legale aplicabile.

7. Domenii specifice vizate de GDPR

7.1 Copiii (Articolul 8)

În comparație cu directiva actuală, GDPR instituie un nivel suplimentar de protecție atunci când sunt Prelucrate datele cu caracter personal a persoanelor vizate care sunt vulnerabile, în special ale copiilor. Articolul 8 introduce obligații suplimentare pentru a se asigura un nivel sporit de protecție a datelor cu caracter personal ale copiilor în relație cu serviciile societății informaționale. Motivul pentru această protecție îmbunătățită este specificat în Considerentul 38: „[...](copiii) pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal [...]". Același considerent mai menționează faptul că „Această protecție specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator și la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor." Sintagma „în particular" indică faptul că protecția specifică categoriei, nu se limitează la marketing sau la crearea de profiluri ci include în mod mai amplu „colectarea de date cu caracter personal în ceea ce privește copii".

Articolul 8 (1) prevede că atunci când Consimțământul se aplică, în relație cu oferta serviciilor societății informaționale, în mod direct unui copil, Prelucrarea de date cu caracter personal va fi legală dacă copilul are cel puțin 16 ani împliniți. Când copilul se află sub vârsta de 16 ani, o astfel de procesare a datelor cu caracter personal este legală numai dacă și în măsura în care Consimțământul a fost dat sau autorizat de titularul răspunderii părintești asupra copilului[53]. Referitor la limita de vârstă pentru un consimțământ valabil, GDPR este flexibil, Statele Membre putând să prevadă prin legea națională o vârstă mai mică, dar aceasta nu poate să fie mai mică de 13 ani.

La fel cum este menționat în secțiunea 3.1 în legătură cu consimțământul în cunoștință de cauză, informația ar trebui să fie inteligibilă de către ușor înțeleasă de audiența căreia i se adresează Operatorul, acordându-se o atenție specială copiilor. Pentru a obține un „consimțământ informat" de la un copil, operatorul de date trebuie să folosească un limbaj adecvat și simplu pentru ca acesta să înțeleagă cum intenționează operatorul să îi proceseze datele personale pe care le colectează[54].

Se înțelege clar de mai sus că Articolul 8 ar trebui să fie aplicabil doar când următoarele condiții sunt întrunite:

[53] Fără a se aduce atingere posibilității legii Statului Membru de a deroga de la limita de vârstă, a se vedea Articolul 8(1).

[54] Considerentul 58 GDPR reafirmă această obligație prin aceea că prevede că, dacă este cazul, un Operator trebuie să se asigure că informația furnizată este înțeleasă ușor de copii.

- Prelucrarea privește oferta serviciilor societății informaționale direct către un copil[55,56]
- Prelucrarea are la bază consimțământul

7.1.1. Serviciile societății informaționale

Pentru a determina scopul noțiunii ,,serviciile societății informaționale" în GDPR, se face referire în articolul 4 (25) GDPR la Directiva 2015/1535.

La evaluarea scopului definiției, Grupul de lucru „Articolul 29" face referire și la jurisprudența CJUE[57]. CJUE a statuat că serviciile societății informaționale se referă la contracte și alte servicii care sunt încheiate și transmise on-line. În cazul în care un serviciu are două componente independente economic, una fiind componenta online, cum ar fi oferta și acceptarea ofertei în contextul încheierii unui contract sau informația privind produsele sau serviciile, incluzând activitățile de marketing, această componentă este definită ca fiind serviciu al societății informaționale, cealaltă componentă de livrare fizică sau distribuție de mărfuri nefiind acoperită de noțiunea serviciu al societății informaționale. Livrarea online a unui serviciu nu va

[55] În conformitate cu articolul 4(25) GDPR un serviciu al societății informaționale înseamnă un serviciu astfel cum este definit la punctual (b) al articolului 1(1) din Directiva 2015/1535: „„serviciu" înseamnă orice serviciu al societății informaționale, adică orice serviciu prestat în mod normal în schimbul unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului.
În sensul prezentei definiții:
(i) „la distanță" înseamnă că serviciul este prestat fără ca părțile să fie prezente simultan;
(ii)„prin mijloace electronice" înseamnă că serviciul este transmis inițial și primit la destinație prin intermediul echipamentului electronic pentru prelucrarea (inclusiv arhivarea digitală) și stocarea datelor și este transmis integral, transferat și recepționat prin cablu, radio, mijloace optice sau alte mijloace electromagnetice;
(iii)„la solicitarea individuală a beneficiarului serviciilor" înseamnă că serviciul este prestat prin transmiterea datelor în urma solicitării individuale." O listă orientativă a serviciilor care nu intră sub incidența prezentei definiții este prevăzută la Anexa I a Directivei amintite. A se vedea de asemenea Considerentul 18 al Directivei 2000/31.

[56] O referință posibilă a definiției termenului „copil" din Convenția Națiunilor Unite privind Drepturile Copilului se găsește la articolul 1, care prevede că „(…) prin copil se înțelege orice ființă umană sub vârsta de 18 ani, exceptând cazurile în care legea aplicabilă copilului stabilește limita majoratului sub această vârstă" A se vedea Națiunile Unite, Adunarea Generală, Rezoluția nr. 44/25 din 20 noiembrie 1989 (Convenția cu privire la drepturile copilului).
[57] A se vedea Curtea Europeană de Justiție, 2 decembrie 2010, Cauza C-108/09, (*Ker-Optika*), paragrafele 22 și 28. În legătură cu „serviciile compuse" , WP29 face trimitere și la Opinia Avocatului General în cauza C-434/15 [*Asociacion Profesional Elite Taxi v Uber System Spain SL.*(paragrafele 30-)punctul 17) și 3]. Opinia AG arată că în situațiile în care două componente descrise mai sus fac parte dintr-un întreg inseparabil, un serviciu compus va cădea sub imperiul definiției serviciului societății informaționale atâta timp cât componenta principală (sau toate componentele esențiale) a serviciului îndeplinește criteriile definiției. Aceasta include și cazul vânzării de mărfuri online.

intra sub domeniul de aplicare a noțiunii de serviciu al societății informaționale în baza articolului 8 GDPR.

7.1.2. Oferirea în mod direct unui copil

Includerea sintagmei ,,oferirea în mod direct unui copil" arată că articolul 8 urmărește aplicarea la unele, nu la toate serviciile societății informaționale. În acest sens, dacă un furnizor al unui serviciu al societății informaționale le specifică în mod clar potențialilor utilizatori că oferă servicii doar persoanelor care au împlinit 18 ani, și acest aspect nu este compromis de alte dovezi (cum ar fi conținutul unei pagini de internet sau planurile de marketing) atunci serviciul nu va fi considerat ca fiind ,,oferit în mod direct unui copil", iar articolul 8 nu va fi aplicabil.

7.1.3. Vârsta

GDPR stabilește că ,,Statele membre pot prevedea prin lege o vârstă inferioară în aceste scopuri, cu condiția ca acea vârstă inferioară să nu fie mai mică de 13 ani." Operatorul trebuie să fie conștient de diferitele legi naționale, luând în considerare publicul căruia îi sunt destinate serviciile. În special, trebuie remarcat faptul că un operator care furnizează servicii transfrontaliere nu se poate baza întotdeauna doar pe respectarea legislației statului membru în care își are sediul principal, ci trebuie să respecte legislația fiecărui stat membru în care își furnizează serviciile societății informaționale. Acest aspect depinde de alegerea pe care o face statul membru de a folosi ca reper în legislația sa națională fie sediul principal al operatorului de date, fie reședința persoanei vizate. În luarea acestei decizii, statele membre vor avea în vedere, înainte de toate, interesul superior al copilului. În această materie, Grupul de lucru „articolul 29" pentru protecția datelor încurajează statele membre să caute o soluție conciliantă.

Atunci când se oferă copiilor servicii ale societății informaționale în baza consimțământului, operatorii de date trebuie să facă eforturi rezonabile pentru a verifica dacă utilizatorul a împlinit vârsta minimă pentru consimțământul digital. Măsurile pe care le iau operatorii de date trebuie să fie proporționale cu natura și riscurile activităților de prelucrare.

Dacă utilizatorii afirmă că au împlinit vârsta minimă necesară pentru consimțământul digital, atunci operatorul de date poate efectua verificări adecvate pentru a se asigura că această afirmație este adevărată. Deși obligația de a verifica vârsta nu este descrisă explicit în GDPR, aceasta este implicit necesară. Dacă copilul care își exprimă consimțământul nu a împlinit vârsta cerută pentru exprimarea consimțământului în nume propriu, atunci prelucrarea datelor este ilegală.

Dacă utilizatorul afirmă că nu a împlinit vârsta minimă pentru consimțământul digital, atunci operatorul de date poate accepta acest răspuns fără alte verificări suplimentare dar va trebui să obțină autorizarea părintească și să verifice că persoana care acordă consimțământul este titularul răspunderii părintești.

Verificarea vârstei nu ar trebui să conducă la o prelucrare excesivă a datelor. Mecanismul ales pentru a verifica vârsta persoanei vizate ar trebui să includă o evaluare a riscurilor pe care le implică respectiva prelucrare. În anumite situații cu risc scăzut, în cazul abonării la un serviciu a unui nou utilizator, solicitarea de a dezvălui anul nașterii sau de a completa un formular care să ateste că utilizatorul este sau nu este minor poate fi considerată o verificare adecvată[58]. În cazul în care apar îndoieli, operatorul de date ar trebui să revizuiască mecanismele de verificare a vârstei în anumite situații și ar trebui să analizeze dacă alte verificări complementare sunt necesare.[59]

7.1.4. Consimțământul copilului și răspunderea părintească

Cu privire la exprimarea autorizării de către titularul răspunderii părintești, GDPR nu precizează metode practice de a obține consimțământul părintelui sau de a stabili că cineva este îndreptățit să facă acest lucru.[60] Prin urmare, Grupul de lucru „articolul 29“ pentru protecția datelor recomandă adoptarea unei abordări proporționale, în concordanță cu articolul 8 (2) și articolul 5 (1)(c) GDPR (referitoare la principiul reducerii la minimum a datelor). O abordare proporțională a operatorului ar fi să se concentreze pe obținerea restrânsă de informații, de exemplu datele de contact ale părintelui sau tutorelui.

O prelucrare rezonabilă, în ce privește verificarea dacă utilizatorul a împlinit vârsta minimă necesară pentru a-și exprima propriul consimțământ sau verificarea dacă persoana care exprimă consimțământul în numele copilului este titularul răspunderii părintești, poate depinde atât de riscurile specifice prelucrării cât și de tehnologia utilizată.

În situații de prelucrare a datelor cu riscuri scăzute, verificarea răspunderii părintești prin e-mail poate fi suficientă. În schimb, în situații de prelucrare a datelor cu risc ridicat, ar putea fi oportun să se solicite mai multe dovezi, astfel încât operatorul de date să poată verifica și păstra informațiile în conformitate cu art. 7 (1) GDPR.[61] Serviciile de verificare efectuate de părți terțe de încredere pot oferi soluții care să reducă la minim cantitatea de date cu caracter personal pe care operatorul de date trebuie să o prelucreze el însuși.

[58] Chiar dacă aceasta nu este neapărat o soluție perfectă pentru orice ipoteză, este un exemplu de management a acestei prevederi.

[59] A se vedea Opinia nr.5/2009 privind serviciile rețelelor sociale (WP163) a Grupului de lucru „articolul 29” pentru protecția datelor.

[60] Grupul de lucru „articolul 29“ pentru protecția datelor constată că nu întotdeauna titularul răspunderii părintești este părintele natural al copilului, iar răspunderea părintească poate fi deținută de mai multe părți, atât persoane juridice, cât și persoane fizice.

[61] De exemplu, părintele sau tutorele ar putea fi rugați să facă o plata de 0,01euro operatorului prin intermediul unei tranzacții bancare care să includă o confirmare scurtă, în secțiunea dedicată descrierii tranzacției, că titularul contului bancar este titularul răspunderii părintești asupra utilizatorului. Unde este cazul, pentru a evita un tratament discriminatoriu față de persoanele care nu sunt titularele unui cont bancar, ar trebui prevăzute metode alternative de verificare.

[Exemplul 17] O platformă de jocuri online dorește să se asigure că utilizatorii minori se pot abona la serviciile sale numai cu consimțământul părinților sau tutorilor. Operatorul de date parcurge următoarele etape:
Pasul 1: întreabă utilizatorul dacă are mai mult sau mai puțin de 16 ani (sau altă vârstă obligatorie pentru consimțământul digital). Dacă utilizatorul afirmă că vârsta sa este sub vârsta minimă cerută pentru consimțământul digital:
Pasul 2: Platforma informează minorul că, pentru a avea acces la serviciile oferite, este nevoie ca părintele sau tutorele său să consimtă sau să autorizeze prelucrarea datelor. Utilizatorului îi sunt cerute adresele de e-mail ale părintelui sau ale tutorelui.
Pasul 3: Platforma contactează părintele sau tutorele, obține consimțământul acestora privind prelucrarea datelor via e-mail și ia toate măsurile rezonabile pentru a confirma că adultul este titularul răspunderii părintești.
Pasul 4: În cazul unor plângeri, platforma ia măsuri suplimentare pentru a verifica vârsta utilizatorului înscris. Dacă platforma a întrunit celelalte cerințe cu privire la consimțământ, aceasta se poate conforma și cu cerințele suplimentare prevăzute de articolul 8 GDPR urmând acești pași.

Exemplul arată că operatorul de date poate fi în măsură să demonstreze că a făcut eforturi rezonabile pentru a se asigura de validitatea consimțământului obținut în cazul serviciilor oferite unui minor. Articolul 8(2) subliniază că „Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.“

Este deci în competența operatorului de date să determine care sunt măsurile necesare într-o anumită situație. Ca regulă generală, operatorii de date ar trebuie să evite soluțiile de verificare care ar implica colectări excesive de date cu caracter personal.

Grupul de lucru „articolul 29“ pentru protecția datelor admite că pot fi cazuri în care verificarea este o provocare (spre exemplu, în cazul în care copiii care își exprimă consimțământul nu au încă stabilită o ‘amprentă digitală’ sau în cazul în care răspunderea părintească nu poate fi verificată cu ușurință). Aceste aspecte pot fi luate în considerare pentru a stabili care eforturi sunt rezonabile dar se așteaptă de la operatorii de date o reevaluare permanentă a proceselor desfășurate de aceștia și a tehnologiei disponibile.

Cu referire la libertatea persoanei vizate de a consimți la prelucrarea datelor sale personale și de a avea control deplin asupra prelucrării, consimțământul acordat sau autorizat de titularul răspunderii părintești expiră odată ce minorul a atins vârsta minimă obligatorie pentru exprimarea consimțământului digital. Începând cu acea dată, operatorul de date trebuie să obțină consimțământul valabil de la persoana vizată ale cărei date sunt prelucrate. În concret, acest lucru poate însemna că operatorul de date care se bazează pe consimțământul utilizatorilor săi va fi nevoit să trimită periodic mesaje pentru a reaminti utilizatorilor că, în cazul copiilor, consimțământul expiră odată ce aceștia împlinesc vârsta de 16 ani iar din acel moment, consimțământul trebuie reafirmat de către persoana vizată personal.

Este important de subliniat că, în conformitate cu considerentul 38, consimțământul unui părinte sau al unui tutore nu este necesar în contextul serviciilor de prevenire sau de consiliere acordate în mod direct unui copil. Spre exemplu, furnizarea online a serviciilor de protecție a copilului prin intermediul unui serviciu de „chat online" nu necesită o autorizare părintească.

În fine, GDPR prevede că normele referitoare la cerințele privind autorizarea părintească față de copii nu trebuie să interfereze cu „dreptul general al contractelor aplicabil în statele membre, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil". Prin urmare, cerințele privind Consimțământul valabil, exprimat în vederea utilizării de date despre copii, fac parte dintr-un cadru legal care trebuie privit ca fiind diferit de legislația națională în materie de contracte. Așadar, acest document de orientare nu răspunde la întrebarea dacă este legal ca un minor să încheie contracte online. Ambele regimuri juridice pot fi aplicate simultan, iar scopul GDPR nu include armonizarea dispozițiilor naționale în materie de contracte.

7.2. Cercetarea științifică

Definirea scopurilor de cercetare științifică are ramificații substanțiale în ceea ce privește activitățile de prelucrare de date pe care un operator le poate desfășura, odată ce a fost obținut un Consimțământ valabil. Acest fapt este relevant mai ales atunci când categorii speciale de date sunt utilizate în scopuri științifice, ca de exemplu în domeniul medical.

Termenul „cercetare științifică" nu este definit în GDPR. Considerentul 159 prevede că „(…) În sensul prezentului regulament, prelucrarea datelor cu caracter personal în scopuri de cercetare științifică ar trebui să fie interpretată în sens larg. (…)". Cu toate acestea, WP29 consideră că noțiunea nu poate fi extinsă înafara sensului comun și înțelege că „cercetare științifică" în acest context înseamnă un proces de cercetare instituit în conformitate cu standarde metodologice și etice relevante din sectorul la care se referă.

Considerentul 33 pare să aducă puțină flexibilitate gradului de specificitate și de granularitate a Consimțământului în contextul cercetării științifice. Acesta prevede că: „Adesea nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare științifică. Din acest motiv, persoanelor vizate ar trebui să li se permită să își exprime consimțământul pentru anumite domenii ale cercetării științifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea științifică. Persoanele vizate ar trebui să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat."

În primul rând, trebuie menționat că considerentul 33 nu pune în aplicare obligațiile în ceea ce privește solicitarea unui Consimțământ specific. Aceasta înseamnă că, în principiu, proiectele de cercetare științifică pot include date cu caracter personal doar în baza Consimțământului, dacă au un scop bine descris. Când scopurile sunt neclare la începutul programului de cercetare științifică, operatorii vor întâmpina dificultăți în a continua programul cu respectarea GDPR.

Pentru cazurile în care scopul prelucrării datelor în cadrul unui proiect de cercetare științifică nu poate fi specificat de la început, considerentul 33 permite o excepție potrivit căreia scopul poate fi descris la un nivel mai general. Luând în considerare condițiile stricte prevăzute de Articolul 9 GDPR privitoare la prelucrarea categoriilor speciale de date, WP29 reține că atunci când categorii speciale de date sunt prelucrate, aplicarea unei abordări flexibile a considerentului 33 va fi subiect al unei interpretări mai stricte și necesită un grad ridicat de control. Atunci când este privit ca un întreg, GDPR nu poate fi interpretat astfel încât să permită unui operator să navigheze în jurul principiului cheie conform căruia este necesar să se specifice scopurile pentru care Consimțământul persoanei vizate este cerut.

Atunci când scopurile cercetării nu pot fi pe deplin specificate, un operator trebuie să caute alte modalități de a asigura că esența cerințelor privind Consimțământul este respectată cel mai bine, spre exemplu, să permită persoanelor vizate să își exprime Consimțământul cu privire la scopul cercetării în termeni mai generali și cu privire la stadii specifice ale proiectului de cercetare, despre care se știe de la început că se vor desfășura. Pe măsură ce avansează cercetările, Consimțământul pentru etapele ulterioare ale proiectului poate fi obținut înainte ca stadiile următoare să înceapă. Cu toate acestea, un astfel de Consimțământ ar trebui să respecte în continuare standardele etice aplicabile cercetării științifice.

Mai mult de atât, operatorul poate aplica garanții suplimentare în astfel de cazuri. De exemplu, Articolul 89(1) evidențiază nevoia de garanții în activitățile de prelucrare de date în scopuri de cercetare științifică sau istorică ori în scopuri statistice. Prelucrarea în aceste scopuri „are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile și libertățile persoanelor vizate.” Reducerea la minimum a datelor, anonimizarea și securitatea datelor sunt menționate ca posibile garanții[62]. Anonimizarea este soluția preferată de îndată ce scopul cercetării poate fi atins fără prelucrarea datelor cu caracter personal.

Transparența este o garanție suplimentară atunci când circumstanțele cercetării nu permit un Consimțământ specific. Nespecificarea scopului poate fi compensată de furnizarea regulată de informații privitoare la dezvoltarea scopului de către operatori, pe măsură ce proiectul progresează, astfel încât, în timp, Consimțământul va fi cât de specific posibil. Astfel, persoana

[62] A se vedea spre exemplu considerentul 156. Procesarea de date cu caracter personal ar trebui de asemenea să respecte alte dispoziții relevante cum ar fi cele referitoare la studiile clinice, a se vedea considerentul 156, Regulamentul (UE) nr. 536/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind studiile clinice pentru evaluarea produselor medicamentoase de uz uman. A se vedea opinia WP29 nr. 15/2011 privind definiția consimțământului (WP 187), p. 7: „În plus, obținerea consimțământului nu anulează obligațiile operatorului în temeiul Articolului 6 în ceea ce privește corectitudinea, necesitatea și proporționalitatea, precum și calitatea datelor. De exemplu, chiar dacă prelucrarea datelor cu caracter personal se bazează pe consimțământul utilizatorului, acest lucru nu ar legitimiza colectarea datelor în mod excesiv în raport cu un anumit scop [...] În principiu, consimțământul nu trebuie văzut ca o excepție de la celelalte principii de protecție a datelor, ci ca o garanție. Este în primul rând un motiv de legalitate și nu se opune aplicării altor principii.”

vizată are cel puțin o viziune de ansamblu asupra situației actuale, permițându-i să evalueze dacă să se folosească sau nu, spre exemplu, de dreptul la retragerea Consimțământului în conformitate cu Articolul 7(3).[63]

De asemenea, deținerea unui plan cuprinzător de cercetare aflat la dispoziția persoanelor vizate pentru al lua în considerare înainte de a-și da consimțământul ar putea contribui la compensarea lipsei specificării scopului.[64] Acest plan de cercetare ar trebui să specifice întrebările de cercetare și metodele de lucru avute în vedere cât mai clar posibil. Planul de cercetare ar putea contribui, de asemenea la respectarea normelor articolului 7(1), operatorii fiind nevoiți să arate care informații au fost disponibile persoanelor vizate în momentul consimțământului pentru a putea demonstra că consimțământul este valid.

Este important de reținut că dacă consimțământul este folosit ca bază legală pentru prelucrare, trebuie să existe posibilitatea persoanei vizate de a-și retrage consimțământul. WP29 menționează că retragerea consimțământului ar putea submina tipurile de cercetare științifică care necesită date care pot fi legate de indivizi, cu toate acestea GDPR este clar cu privire la faptul că consimțământul poate fi retras iar operatorii trebuie să acționeze în acest sens – nu se acordă nici o scutire de la această cerință în vederea cercetării științifice.[65] Dacă un operator primește o cerere de retragere, trebuie să șteargă sau să anonimizeze datele personale imediat dacă dorește să folosească datele pentru scopurile de cercetare[66].

7.3. Drepturile persoanei vizate

Dacă o activitate de prelucrare a datelor este bazată pe consimțământul persoanei vizate, aceasta va afecta drepturile acelui individ. Persoanele vizate pot avea dreptul la portabilitatea datelor (art. 20) când prelucrarea este bazată pe consimțământ. În același timp, dreptul la opoziție (art. 21) nu se aplică atunci când prelucrarea este bazată pe consimțământ, deși dreptul la retragerea consimțământului în orice moment poate oferi un rezultat similar.

[63] Alte măsuri de transparență ar putea fi de asemenea relevante. Când operatorii se angajează să prelucreze date cu caracter personal în scopuri științifice, iar toată informația nu poate fi oferită de la început, aceștia ar putea desemna o persoană de contact căreia persoanele vizate să i se adreseze cu întrebări.

[64] O astfel de posibilitate se regăsește în articolul 14 (1) din actualul Act privind datele personale din Finlanda (Henkilötietolaki, 523/1999).

[65] Acest lucru nu trebuie confundat cu articolul 17 GDPR („dreptul de a fi uitat"), care este supus unei excepții pentru arhivare în scopuri de interes public, cercetare științifică sau istorică sau scopuri statistice, în conformitate cu articolul 89 (1). Cu toate acestea, Operatorii vor avea în continuare nevoie de o bază legală în temeiul articolului 6 GDPR pentru păstrarea datelor.

[66] A se vedea și Opinia Grupului de lucru „Articolul 29" nr. 05/2014 privind „Tehnica de anonimizare"(WP216).

Articolele 16-20 GDPR indică faptul că atunci când prelucrarea datelor este bazată pe consimțământ, persoanele vizate au dreptul la ștergerea datelor, ,,dreptul de a fi uitat" atunci când consimțământul a fost retras și dreptul la restricționare, rectificare și acces[67].

8. Consimțământul obținut sub Directiva 95/46/EC

Operatorii care în prezent prelucrează date pe baza consimțământului în conformitate cu legea națională pentru protecția datelor nu sunt obligați în mod automat să reîmprospăteze complet toate relațiile de consimțământ cu persoanele vizate în pregătirea lor pentru GDPR. Consimțământul care a fost obținut până în prezent continuă să fie valabil atâta timp cât este în conformitate cu condițiile prevăzute în GDPR.

Este important pentru operatori să evalueze procesele de lucru prezente și evidențele în detaliu, înainte de 25 mai 2018, ca să se asigure că consimțămintele existente îndeplinesc standardul GDPR (vezi Considerentul 171 din GDPR[68]). În practică, GDPR ridică ștacheta în privința implementării mecanismului de consimțământ și introduce mai multe cerințe noi care impun operatorilor să modifice mecanismul de consimțământ, decât să rescrie doar politicile de confidențialitate.

De exemplu, GDPR impune faptul că un operator trebuie să fie capabil să demonstreze că a fost obținut un consimțământ valid, toate consimțămintele presupuse cărora nu se păstrează referințe vor fi sub standardul pentru consimțământ al GDPR în mod automat și vor trebui reînnoite. În mod similar cum GDPR impune o „declarație sau o acțiune afirmativă clară", toate consimțămintele presupuse care au fost bazate pe o formă de acțiune mai implicită de către persoana vizată (ex. ignorarea unei casete de înscriere pre-bifată) de asemenea, nu vor fi conforme standardului consimțământului GDPR.

În continuare, pentru a fi capabil să demonstreze că consimțământul a fost obținut sau pentru a permite pentru mai multe manifestări de voință granulare a persoanei vizate, operațiunile și sistemele IT pot avea nevoie de revizuiri. De asemenea, trebuie oferite mecanisme pentru persoanele vizate de a retrage consimțământul într-un mod ușor. Dacă procedurile existente

[67] În cazurile în care anumite activități de prelucrare a datelor sunt restricționate în conformitate cu articolul 18 GDPR, este necesar consimțământul persoanei vizate pentru a se ridica restricția.

[68] Considerentul 171 din GDPR prevede: „Directiva 95/46 / CE ar trebui abrogată prin prezentul regulament. Prelucrarea aflată deja în curs la data aplicării prezentului regulament ar trebui adusă în conformitate cu prezentul regulament în termen de doi ani de la intrarea în vigoare a prezentului regulament. În cazul în care prelucrarea se bazează pe consimțământul în temeiul Directivei 95/46 / CE, nu este necesar ca persoana vizată să își dea din nou consimțământul, în cazul în care modul în care a fost acordat consimțământul este conform cu condițiile prezentului regulament, astfel încât să permită operatorului să continue prelucrarea după data de aplicare a prezentului regulament. Deciziile Comisiei adoptate și autorizațiile autorităților de supraveghere în temeiul Directivei 95/46 / CE rămân în vigoare până la modificarea, înlocuirea sau abrogarea acestora."

pentru obținerea și administrarea consimțământului nu întâlnesc standardele GDPR, operatorii trebuie să obțină un nou consimțământ conform cu GDPR.

Pe de altă, deoarece nu toate elementele menționate în articolele 13 și 14 trebuie să fie întotdeauna prezente ca condiții pentru consimțământul în cunoștință de cauză(informat), obligațiile de informare extinse sub tutela GDPR nu se opun neapărat continuității consimțământului care a fost acordat înainte ca GDPR să intre în vigoare (a se vedea pagina 15 de mai sus). Sub Directiva 95/46/CE, nu exista cerința de a informa persoana vizată despre temeiul pe baza căruia se desfășura prelucrarea.

Dacă un operator descoperă că consimțământul obținut (anterior) conform legislației vechi nu îndeplinește standardul consimțământului GDPR, atunci operatorii trebuie să evalueze dacă prelucrarea poate fi întemeiată pe o bază legală diferită, luând în considerare condițiile stabilite de GDPR. Cu toate acestea, aceasta este o situație unică, deoarece operatorii se mută de la aplicarea directivei la aplicarea GDPR. Sub tutela GDPR, nu este posibil schimbul între o bază legală și alta. Dacă un operator nu poate să reînnoiască consimțământul într-un mod compatibil și, de asemenea, nu poate să efectueze tranziția la respectarea GDPR bazându-se pe prelucrarea datelor pe o bază legală diferită, asigurând în același timp că prelucrarea continuă este corectă și contabilizată, activitățile de prelucrare trebuie să fie oprite. În orice caz, operatorul trebuie să respecte principiile procesării legale, corecte și transparente.

9. Întrebări frecvente

[Se va face după consultarea publică a acestui document de orientare.]

-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*SFÂRȘITUL DOCUMENTULUI*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-*-

Precizări ale autorilor documentului:

1. Documentul utilizează adesea acronime din limba engleză, precum GDPR – Regulamentul General privind Protecția Datelor; WP29 – Grupul de lucru „Articolul 29" pentru protecția datelor; Opiniile Grupului de lucru „articolul 29" sunt redate cu menționarea numărului documentului și alăturarea grupului de litere WP.
2. Unii termeni care au o importanță specifică și un conținut de bază, relevant în cadrul frazei sau propozițiilor, sunt menționați cu majusculă, chiar dacă apar în cadrul, iar nu la începutul propoziției. Exemple: Articol; Consimțământ, Prelucrare, Operator
3. Există formulări variate a unor reglementări, în funcție de cunoașterea sau sinteza denumirii în limba engleză, precum: Directiva asupra confidențialității și comunicațiilor electronice(2002/58/EC) – E-Privacy Directive
4. Se întâlnesc abrevieri sau expresii în limba latină: *inter alia* – printre altele; e.g.(*exempli gratia*) – de exemplu
5. Uneori s-au utilizat expresii mai literare pentru o înțelegere mai adecvată a textului. Spre exemplu, în loc de „informat" s-a utilizat uneori expresia „în cunoștință de cauză";
6. Uneori au fost lăsați termeni în limba engleză fără a fi traduși ca atare, datorită expresivității și cunoașterii lor generale. De exemplu: design, în loc de model; online în loc de pe rețeaua de net, cookies în loc de .....
7. Erate: La paragraful al doilea de la punctul 3.4. textul normativ indicat a fost preluat din conținutul Directivei 95/46/CE deoarece nu era complet cel trecut în Orientări.
8. Pentru a determina scopul noțiunii ,,serviciile societății informaționale" în GDPR, se face referire în articolul 4 (25) GDPR la Directiva 2015/1535 spun autorii prezentei Orientări – directivă disponibilă la adresa http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32015L1535&from=RO. Cu toate acestea textul articolului 4(25) din GDPR în limba română face trimitere în mod greșit la Directiva 98/34/CE a Parlamentului European și a Consiliului din 22 iunie 1998 de stabilire a unei proceduri pentru furnizarea de informații în domeniul standardelor și reglementărilor tehnice și al normelor privind serviciile societății informaționale - http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016R0679&from=ro .
Textul în limba engleză al articolului 4(25) GDPR este corect: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=en
9. S-a preferat traducerea titlului acestui document să fie „**Orientări** asupra Consimțământului în temeiul Regulamentului 2016/679", chiar dacă în practica de traduceri apărute pe site-ul autorității naționale de supraveghere din România se utilizează în mod constant expresia „Ghid", întrucât această practică nu reflectă exigențele de traducere din limba engleză în română și nici metoda legală comparativă, în sensul că în limba engleză cuvântul „ghid" se traduce de regulă cu termenul „Guide", în timp ce în Directiva 95/46/CE (traducerea în limba română) stabilește că Grupul de lucru „Articolul 29" emite doar opinii și orientări, nicidecum ghiduri.
10. Traducerea a fost realizată de membrii Centrului pentru Protecția Datelor Personale din cadrul Universității ,,Petru Maior" din Tîrgu Mureș.