CEPD
Comitetul european pentru protecția datelor

Orientări

Orientările 03/2022 privind modelele de interfață înșelătoare ale platformelor de comunicare socială: cum să le recunoaștem și să le evităm

Versiunea 2.0

adoptată la 14 februarie 2023

Istoricul versiunii

Versiunea 2.0	14 februarie 2023	Adoptarea Orientărilor pentru consultare publică
Versiunea 1.0	14 martie 2022	Adoptarea Orientărilor pentru consultare publică

Traducerea dată nu este o traducere oficială a Comitetului European pentru Protecția Datelor (EDPB) și a fost asigurată, în cadrul unui schimb între GIZ și EDPB, ca rezultat al unui acord reciproc între GIZ și CNPDCP, cu sprijinul financiar al GIZ în cadrul proiectului "Re-ingineria serviciilor publice în cadrul Parteneriatului Estic" din cadrul Fondului Regional pentru Reformele Administrației Publice al Parteneriatului Estic, comandat și finanțat de BMZ.

REZUMAT EXECUTIV

Orientările de față oferă recomandări practice furnizorilor de platforme de comunicare socială în calitate de operatori, proiectanți și utilizatori ai platformelor de comunicare socială cum să evalueze și să evite așa-numitele „modele de interfață înșelătoare" pe platformele de comunicare socială, care încalcă cerințele RGPD. În acest scop, CEPD recomandă operatorilor să implice echipe interdisciplinare, formate inclusiv din proiectanți, responsabili cu protecția datelor și factori de decizie. Este important să menționăm că lista modelelor de interfață înșelătoare și a celor mai bune practici, precum și cazurile de utilizare, nu sunt exhaustive. Furnizorii platformelor de comunicare socială sunt responsabili și poartă răspundere pentru asigurarea conformității platformelor lor cu prevederile RGPD.

Modelele de interfață înșelătoare ale platformelor de comunicare socială

În contextul acestor Orientări, „modele de interfață înșelătoare" sunt considerate interfețe și călătorii ale utilizatorilor implementate pe platformele de comunicare socială, care încearcă să influențeze utilizatorii să ia decizii neintenționate, nedorite și potențial dăunătoare, deseori împotriva celor mai bune interese ale utilizatorilor și în favoarea intereselor platformelor de comunicare socială, cu privire la prelucrarea datelor cu caracter personal ale acestora. Modelele de interfață înșelătoare au scopul de a influența comportamentul utilizatorilor și pot împiedica capacitatea acestora de a-și proteja în mod eficient datele cu caracter personal și de a face alegeri conștiente. Autoritățile de protecție a datelor sunt responsabile pentru sancționarea utilizării modelelor de interfață înșelătoare, dacă acestea încalcă cerințele RGPD. Modelele de interfață înșelătoare abordate în aceste Orientări pot fi clasificate în următoarele categorii:

- ***Supraîncărcarea*** înseamnă că utilizatorii se confruntă cu o avalanșă/un număr mare de solicitări, informații, opțiuni sau posibilități pentru a-i determina să partajeze mai multe date sau să permită neintenționat prelucrarea datelor lor cu caracter personal împotriva așteptărilor persoanei vizate. Următoarele trei tipuri de modele de interfață înșelătoare se încadrează în această categorie: ***Solicitare continuă, Labirint de confidențialitate*** și ***Prea multe opțiuni.***

- ***Omiterea*** înseamnă proiectarea interfeței de utilizator sau a călătoriei utilizatorului într-un mod în care utilizatorii uită sau nu se gândesc la toate sau la unele aspecte legate de protecția datelor.
  Următoarele două tipuri de modele de interfață înșelătoare se încadrează în această categorie: ***Comoditatea înșelătoare*** și ***Uita-te acolo***

- ***Agitarea*** afectează alegerea pe care utilizatorii ar face-o apelând la emoțiile lor sau folosind ghionturi vizuale.
  Următoarele două tipuri de modele de interfață înșelătoare se încadrează în această categorie: ***Dirijare emoțională*** și ***Ascuns la vedere***.

- ***Obstrucționarea*** înseamnă împiedicarea sau blocarea utilizatorilor în procesul lor de informare sau gestionare a datelor lor, făcând acțiunea complicat sau imposibil de realizat.
  Următoarele trei tipuri de modele de interfață înșelătoare se încadrează în această categorie: ***Fundătură, Mai lungă decât este necesar*** și ***Acțiune înșelătoare***

- ***Schimbător*** înseamnă că proiectul interfeței nu este coerent și clar, complicând navigarea utilizatorului prin diferite instrumente de control al protecției datelor și înțelegerea scopului prelucrării.
  Următoarele patru tipuri de modele de interfață înșelătoare se încadrează în această categorie: ***Lipsa ierarhiei, Decontextualizarea, Interfața incoerentă*** și ***Discontinuitatea limbajului***

- ***Lăsată în întuneric*** înseamnă că o interfață este concepută astfel încât să ascundă informațiile sau instrumentele de control legate de protecția datelor sau să lase utilizatorii nesiguri cu privire la modul de prelucrare a datelor lor și tipul de control, pe care ar putea să-l aibă asupra acesteia în ceea ce privește exercitarea drepturilor lor.
  Următoarele două tipuri de modele de interfață înșelătoare se încadrează în această categorie: ***Informații conflictuale*** și ***Formulare sau informații ambigue***

Prevederile relevante ale RGPD pentru evaluările modelelor de interfață înșelătoare

În ceea ce privește conformitatea cu cerințele de protecție a datelor a interfețelor de utilizator ale aplicațiilor online din sectorul comunicării sociale, principiile de protecție a datelor aplicabile sunt prevăzute la articolul 5 din RGPD. Principiul prelucrării echitabile prevăzut la articolul 5 alineatul (1) litera (a) din RGPD servește drept punct de plecare pentru evaluarea faptului dacă un model de interfață constituie într-adevăr un „model de interfață înșelătoare". Alte principii, care joacă un rol în această evaluare, sunt principiile transparenței, minimizării datelor și răspunderii în conformitate cu articolul 5 alineatul (1) literele (a), (c) și alineatul (2) din RGPD, precum și, în unele cazuri, limitarea scopului în conformitate cu articolul 5 alineatul (1) litera (b) din RGPD. În alte cazuri, evaluarea juridică se bazează și pe condițiile consimțământului în temeiul articolului 4 alienatul (11) și articolului 7 din RGPD sau pe alte obligații specifice, cum ar fi cele prevăzute la articolul 12 din RGPD. Evident, în contextul drepturilor persoanelor vizate, trebuie luat în considerare și al treilea capitol al RGPD. În cele din urmă, cerințele de protecție a datelor începând cu momentul conceperii și în mod implicit în temeiul articolului 25 din RGPD joacă un rol esențial, deoarece aplicarea acestora înainte de lansarea unui proiect de interfață ar ajuta furnizorii platformelor de comunicare socială să evite modelele de interfață înșelătoare în primul rând.

Exemple de modele de interfață înșelătoare în cazurile utilizării ciclului de viață al unui cont pe o platformă de comunicare socială

Prevederile RGPD se aplică întregului proces de prelucrare a datelor cu caracter personal ca parte a operării platformelor de comunicare socială, adică întregului ciclu de viață al unui cont de utilizator. CEPD oferă exemple concrete de tipuri de modele de interfață înșelătoare pentru următoarele cazuri de utilizare diferite în cadrul acestui ciclu de viață: înregistrarea, adică procesul de înregistrare; cazurile de utilizare a informațiilor referitoare la notificarea de confidențialitate, controlul comun și comunicările privind încălcarea securității datelor cu caracter personal; managementul consimțământului și al protecției datelor; exercitarea drepturilor persoanelor vizate în timpul utilizării platformelor de comunicare socială; și, în cele din urmă, închiderea unui cont pe o platformă de comunicare socială. Legăturile cu prevederile RGPD sunt explicate în două moduri: în primul rând, fiecare caz de utilizare explică mai detaliat care dintre prevederile RGPD menționate mai sus sunt deosebit de relevante pentru aceasta. În al doilea rând, alineatele care conțin exemple de modele de interfață înșelătoare explică modul în care acestea încalcă prevederile RGPD.

Recomandări de cele mai bune practici

Pe lângă exemplele de modele de interfață înșelătoare, Orientările mai prezintă și cele mai bune practici la sfârșitul fiecărui caz de utilizare, precum și în Anexa II la aceste Orientări. Aceste exemple conțin recomandări specifice de proiectare a interfețelor de utilizator, care facilitează implementarea eficientă a RGPD.

Lista de verificare a categoriilor de modele de interfață înșelătoare

O listă de verificare a categoriilor de modele de interfață înșelătoare poate fi găsită în Anexa I la prezentele Orientări. Acesta oferă o prezentare generală a categoriilor menționate mai sus și a tipurilor de modele de interfață înșelătoare, împreună cu o listă de exemple pentru fiecare model, care sunt menționate în cazurile de utilizare. Unii cititori ar putea considera util să folosească lista de verificare ca punct de plecare pentru familiarizarea cu aceste Orientări.

Cuprins

Comitetul European pentru Protecția Datelor

Luând în considerare prevederile de la articolul 70 alineatul (1) litera (e) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (denumit în continuare „RGPD”),

Având în vedere Acordul privind SEE, în special Anexa XI și Protocolul 37 la acesta, astfel cum a fost modificat prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

Luând în considerare prevederile articolului 12 și articolului 22 din Regulamentul său de procedură,

A ADOPTAT URMĂTOARELE ORIENTĂRI

1. DOMENIUL DE APLICARE

1. Scopul acestor Orientări este de a oferi recomandări și îndrumări pentru proiectarea interfețelor platformelor de comunicare socială. În sensul prezentelor Orientări, platformele de comunicare socială sunt înțelese ca platforme online, care permit dezvoltarea rețelelor și comunităților de utilizatori, între care se partajează informații și conținut.[2] Orientările pot fi folosite fie la etapa de concepere a unei interfețe de utilizator pentru a evita implementarea modelelor de interfață înșelătoare[3] de la început, fie pe un serviciu existent pentru a evalua conformitatea interfeței acestuia. Orientările sunt destinate furnizorilor platformelor de comunicare socială în calitate de operatori ai platformelor respective, care au responsabilitatea de proiectare și operare a platformelor de comunicare socială. În acest sens, Orientările reamintesc obligațiile, care decurg din RGPD, cu referire specială la principiile legalității, corectitudinii, transparenței, limitării scopului și minimizării datelor în proiectarea interfețelor de utilizator și prezentarea conținutului serviciilor și aplicațiilor lor web. Principiile menționate mai sus trebuie implementate într-un mod substanțial și, din punct de vedere tehnic, acestea constituie cerințe de proiectare a software-ului și a serviciilor, inclusiv a interfețelor de utilizator. Cerința RGPD este studiată profund atunci când se aplică interfețelor de utilizator și prezentării conținutului, și se clarifică ceea ce ar trebui considerat un „model de interfață înșelătoare”, o modalitate de proiectare și prezentare a conținutului, care încalcă substanțial aceste cerințe,

[1] Referințele la „State membre” din acest document ar trebui înțelese ca referințe la „Statele membre ale SEE”.

[2] Definiție identică cu definiția dată în Orientările 08/2020 ale CEPD privind direcționarea utilizatorilor platformelor de comunicare socială, p. 1, a se vedea nota de subsol 1 în acestea pentru o descriere mai detaliată; disponibile la https://edpb.europa.eu/system/files/2021-04/edpb guidelines 082020 on the targeting of social media users en.pdf.

[3] Pentru versiunea 2.0 a acestor Orientări, CEPD utilizează termenul mai cuprinzător și descriptiv de „model de interfață înșelătoare” în loc de „model întunecat”.

pretinzând în continuare că se conformează în mod oficial. Aceste Orientări se potrivesc, de asemenea, pentru sporirea gradului de conștientizare a utilizatorilor cu privire la drepturile lor și riscurile, care decurg din partajarea prea multor date sau partajarea datelor lor într-un mod necontrolat. Aceste Orientări au, de asemenea, scopul de a ajuta utilizatorii să recunoască „modele de interfață înșelătoare" (astfel cum sunt definite în cele ce urmează) și cum să le abordeze pentru a-și proteja confidențialitatea într-un mod conștient. În cadrul analizei, a fost examinat ciclul de viață al unui cont pe o platformă de comunicare socială pe baza a cinci cazuri de utilizare: „Deschiderea unui cont pe o platformă de comunicare socială" (cazul de utilizare 1), „Informarea continuă pe platforma de comunicare socială" (cazul de utilizare 2), „Protejarea continuă pe platforma de comunicare socială" (cazul de utilizare 3), „Corectitudinea continuă pe platforma de comunicare socială: drepturile persoanei vizate" (cazul de utilizare 4) și „Adio: închiderea unui cont pe platforma de comunicare socială" (cazul de utilizare 5).

2. În aceste Orientări, termenul „interfața de utilizator" corespunde mijloacelor prin care oamenii pot interacționa cu platformele de comunicare socială. Documentul se concentrează pe interfețele grafice de utilizator (de exemplu, este utilizat pentru interfețe de computer și telefon inteligent), dar unele observații se pot aplica și interfețelor controlate prin voce (de exemplu, utilizate pentru difuzoare inteligente) sau interfețe bazate pe gesturi (de exemplu, utilizate în realitatea virtuală). Termenul „călătoria utilizatorului" corespunde unui număr de acțiuni sau pași, pe care utilizatorii trebuie le/să-i efectueze pentru a-și atinge obiectivul care, pe rețelele de socializare, pot fi navigarea în feed-ul lor, partajarea unei postări, setarea preferințelor etc. Termenul „experiența utilizatorului" corespunde experienței generale a utilizatorilor legate de platformele de comunicare socială, care include utilitatea percepută, ușurința de utilizare și eficiența interacțiunii cu aceasta. Proiectul interfeței de utilizator și proiectul experienței utilizatorului au evoluat în mod continuu în ultimul deceniu. Mai recent, acestea s-au bucurat de interacțiuni și experiențe omniprezente, personalizate și așa-numite interacțiuni și experiențe fără întreruperi ale utilizatorului: interfața perfectă ar trebui să fie foarte personalizată, ușor de utilizat și multi-modală.[4] Chiar dacă aceste tendințe ar putea simplifica și mai mult utilizarea serviciilor digitale, acestea pot fi utilizate astfel încât să promoveze în primul rând comportamente ale utilizatorilor care contravin spiritului RGPD.[5] Acest fapt este relevant în special în contextul economiei atenției, în care atenția utilizatorului este considerată o marfă. În aceste cazuri, limitele permise din punct de vedere juridic ale RGPD pot fi depășite, iar proiectul interfeței de utilizator și proiectul experienței utilizatorului, care duc la astfel de cazuri sunt descrise mai jos ca „modele de interfață înșelătoare".

3. În contextul acestor Orientări, „modele de interfață înșelătoare" sunt considerate interfețe de utilizator și călătorii ale utilizatorilor implementate pe platformele de comunicare socială, care au scopul să influențeze utilizatorii să ia decizii neintenționate, respectiv nedorite și/sau potențial dăunătoare, deseori față de o opțiune, care este împotriva celor mai bune interese ale utilizatorilor și în favoarea interesului platformelor de comunicare socială, în ceea ce privește datele lor cu caracter personal. Modelele de interfață înșelătoare au scopul de a influența comportamentele utilizatorilor, bazându-se în general pe prejudecăți cognitive, și le pot împiedica capacitatea „de a-și proteja în mod eficient datele cu caracter personal și de a face alegeri conștiente"[6], de exemplu, făcându-i incapabili „să-și exprime un consimțământ informat

[4] Pentru mai multe detalii vezi CNIL, Report IP No. 6: Shaping Choices in the Digital World, 2019. p. 9 https://www.cnil.fr/sites/default/files/atoms/files/cnil ip report 06 shaping choices in the digital world.pdf.
[5] CNIL, Shaping Choices in the Digital World, 2019. p. 10.
[6] CNIL, Shaping Choices in the Digital World, 2019. p. 27.

și liber”[7]. Această tehnică poate fi utilizată în mai multe aspecte ale proiectului, cum ar fi alegerea culorilor interfețelor și plasarea conținutului. În schimb, prin oferirea stimulentelor și proiectelor ușor de utilizat, poate fi susținută realizarea regulamentelor privind protecția datelor.

4. Modelele de interfață înșelătoare nu duc neapărat doar la o încălcare a regulamentelor privind protecția datelor. Acestea pot, de exemplu, încălca și regulamente privind protecția consumatorilor. Granițele dintre încălcările impuse de autoritățile de protecție a datelor și cele impuse de autoritățile naționale de protecție a consumatorilor, de concurență sau alte autorități se pot suprapune.[8] Conform RGPD, autoritățile de protecție a datelor sunt responsabile pentru sancționarea utilizării modelelor de interfață înșelătoare, dacă acestea încalcă de fapt standardele de protecție a datelor și, prin urmare, RGPD. Încălcările cerințelor RGPD trebuie evaluate de la caz la caz. Aceste Orientări se referă doar la modelele de interfață înșelătoare, care ar putea fi obiectul acestui mandat de reglementare. Din acest motiv, pe lângă exemplele de modele de interfață înșelătoare, Orientările prezintă și cele mai bune practici care pot fi utilizate pentru a proiecta interfețe de utilizator, care facilitează implementarea eficientă a RGPD. Acest tip de cele mai bune practici pot oferi un prim pas către o modalitate standardizată pentru ca utilizatorii să își controleze în mod eficient datele și să își exercite drepturile.

5. Modelele de interfață înșelătoare[9] abordate în aceste Orientări rezultă dintr-o analiză interdisciplinară a interfețelor existente și pot fi divizate în următoarele categorii:

Supraîncărcarea: înseamnă că utilizatorii se confruntă cu o avalanșă/un număr mare de solicitări, informații, opțiuni sau posibilități pentru a-i determina să partajeze mai multe date sau să permită neintenționat prelucrarea datelor lor cu caracter personal împotriva așteptărilor persoanei vizate.

Omiterea: proiectarea interfeței de utilizator sau a călătoriei utilizatorului într-un mod în care utilizatorii uită sau nu se gândesc la toate sau la unele aspecte legate de protecția datelor.
Agitarea: afectează alegerea, pe care ar face-o utilizatorii apelând la emoțiile lor sau utilizând ghionturi vizuale.

Obstrucționarea: împiedicarea sau blocarea utilizatorilor în procesul lor de informare sau gestionare a datelor lor, făcând acțiunea complicat sau imposibil de realizat.

Schimbător: proiectul interfeței nu este coerent și clar, complicând navigarea utilizatorului prin diferite instrumente de control al protecției datelor și înțelegerea scopului prelucrării.

Lăsată în întuneric: o interfață este concepută astfel încât să ascundă informațiile sau instrumentele de control al protecției datelor sau să lase utilizatorii nesiguri cu privire la modul

[7] A se vedea Consiliul Norvegian al Consumatorilor, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy,* p. 10 https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf, și de asemenea CNIL, Shaping Choices in the Digital World, p. 30, 31.
[8] În acest sens, articolul 25 alineatul (2) din Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale), clarifică faptul că interdicția interfețelor online înșelătoare sau manipulatoare în temeiul articolului 25 alineatul (1) nu se aplică practicilor reglementate de Directiva 2005/29/CE (Directiva privind practicile comerciale neloiale ale întreprinderilor de pe piața internă față de consumatori, DPCN) sau RGPD. De asemenea, Comunicarea Comisiei UE (2021/C 526/01) oferă orientări privind interpretarea și aplicarea DPCN, inclusiv privind „modele întunecate” în secțiunea sa 4.2.7.
[9] Categoriile de modele înșelătoare și tipurile de modele înșelătoare din cadrul acestor categorii vor fi afișate ***cu caractere aldine și cursive*** în textul Orientărilor. O prezentare detaliată este oferită în Anexă.

de prelucrare a datelor lor și tipul de control, pe care ar putea să-l aibă asupra acesteia în ceea ce privește exercitarea drepturilor lor.

6. Pe lângă regruparea modelelor de interfață înșelătoare în aceste categorii în dependență de efectele lor asupra comportamentului utilizatorilor, aceste modele pot fi, de asemenea, divizate în modele bazate pe conținut și modele bazate pe interfață pentru a aborda mai precis aspectele interfeței de utilizator sau ale călătoriei utilizatorului. Modelele bazate pe conținut se referă la conținutul real și, prin urmare, la formularea și contextul propozițiilor și componentelor informaționale. De asemenea, mai există și componente, care au o influență directă asupra percepției acestor factori. Aceste modele bazate pe interfață sunt legate de modalitățile de afișare a conținutului, de navigare prin conținut sau interacțiune cu acesta.

7. Este important să rețineți că modelele de interfață înșelătoare generează preocupări suplimentare cu privire la impactul potențial asupra copiilor,[10] înregistrarea pe platforma de comunicare socială și, de asemenea, alte grupuri vulnerabile de persoane, cum ar fi persoanele în vârstă, persoanele cu deficiențe de vedere sau care nu au cunoștințe digitale ca alte persoane. Grupurile vulnerabile, cum ar fi utilizatorii în vârstă, sunt deseori nu doar mai puțin capabile să identifice practicile de proiectare manipulatoare, ci și mai puțin conștiente de faptul că comportamentul lor digital este influențat. RGPD cere garanții suplimentare în cazurile în care prelucrarea se referă la datele cu caracter personal ale copiilor, deoarece aceștia din urmă pot fi mai puțin conștienți de riscurile și consecințele legate de drepturile lor la prelucrare.[11] Considerentul 58 afirmă în mod explicit că, în cazul în care prelucrarea este adresată unui copil, orice informație ar trebui să fie prezentată într-un limbaj clar și simplu, pe care copiii îl pot înțelege cu ușurință. De asemenea, RGPD prevede în mod explicit prelucrarea datelor persoanelor fizice, în special ale copiilor, ca situații în care riscul pentru drepturile și libertățile persoanelor cu o probabilitate și severitate diferită poate apărea din prelucrarea datelor care ar putea genera prejudicii materiale sau morale.[12]

8. Ținând cont de cele menționate mai sus, ar trebui să fie clar că modelele de interfață înșelătoare nu sunt unice pentru platformele de comunicare socială. Opinii forme cu privire la această problemă au fost exprimate în timpul consultării publice a acestor Orientări. Interfețele sunt prezente în multe alte situații, în care utilizatorii interacționează cu produse și servicii bazate pe sau legate de operațiunile de prelucrare a datelor. Acestea pot include site-uri web și bannere cookie,[13] magazine online, jocuri video, aplicații mobile și microplăți, etc. Deși modelele de interfață înșelătoare descrise mai jos pot să nu fie prezente în exact aceeași formă, variațiile lor pot încălca drepturile persoanelor vizate sau ale consumatorilor. Cu toate acestea, Orientările de față se referă doar la modelele de interfață înșelătoare ale platformelor de comunicare socială,

[10] A se vedea, de asemenea, Considerentul 81, fraza a 4-a din Regulamentul (UE) 2022/2065 (Regulamentul privind serviciile digitale).
[11] RGPD, Considerentul 38.
[12] RGPD, Considerentul 75; a se vedea, de asemenea, Orientările CEPD 8/2020 privind direcționarea utilizatorilor platformelor de comunicare socială, p. 16 https://edpb.europa.eu/system/files/2021-04/edpb guidelines 082020 on the targeting of social media users en.pdf.
[13] În urma mai multor plângeri primite de la NOYB, un grup operativ al CEPD a făcut schimb de opinii cu privire la o serie de elemente de interfață din bannerele cookie. Numitorul comun convenit de autoritățile de supraveghere în interpretarea lor a cadrului legal aplicabil pe mai multe straturi a fost rezumat într-un „Raport al activității întreprinse de grupul operativ Cookie Banner" din 17 ianuarie 2023, disponibil la https://edpb.europa.eu/system/files/2023-01/edpb 20230118 report cookie banner taskforce en.pdf.

deoarece influența acestor platforme asupra vieții cotidiene a oamenilor și a popoarelor este în continuă creștere, fapt clarificat în documentele anterioare ale CEPD.[14]

2. PRINCIPII APLICABILE - CE TREBUIE REȚINUT?

9. În ceea ce privește conformitatea cu cerințele de protecție a datelor a interfețelor de utilizator ale aplicațiilor online din sectorul comunicării sociale, principiile de protecție a datelor aplicabile sunt prevăzute în articolul 5 din RGPD. Principiul prelucrării echitabile prevăzut la articolul 5 alineatul (1) litera (a) din RGPD este un punct de plecare pentru evaluarea existenței unor modele de interfață înșelătoare. După cum a afirmat deja CEPD, corectitudinea este un principiu general, care cere ca datele cu caracter personal să nu fie prelucrate într-un mod dăunător, discriminatoriu, neașteptat sau înșelător pentru persoana vizată.[15] Dacă interfața are informații insuficiente sau înșelătoare pentru utilizatori și corespunde caracteristicilor modelelor de interfață înșelătoare, aceasta poate fi clasificată ca prelucrare neechitabilă. Principiul echității are o funcție tip umbrelă și toate modelele de interfață înșelătoare nu l-ar respecta, indiferent de respectarea altor principii de protecție a datelor.

10. Pe lângă această prevedere fundamentală de echitate a prelucrării, principiile responsabilității, transparenței și obligației de protecție a datelor începând cu momentul conceperii menționate la articolul 25 din RGPD sunt, de asemenea, relevante în ceea ce privește cadrul de proiectare, iar modelele de interfață înșelătoare ar putea încălca aceste prevederi. Cu toate acestea, este posibil ca evaluarea juridică a modelelor de interfață înșelătoare să se bazeze pe elementele privind definițiile generale, cum ar fi articolul 4 alienatul (11) din RGPD, definiția consimțământului sau alte obligații specifice, cum ar fi articolul 12 din RGPD. Articolul 12 alineatul (1) fraza 1 din RGPD impune operatorilor să ia măsuri adecvate pentru a furniza orice comunicări referitoare la drepturile persoanei vizate, precum și orice informații, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Conform Considerentului 39 fraza 3 privind principiul transparenței, această cerință nu se limitează la notificările privind protecția datelor[16] sau la drepturile persoanelor vizate,[17] ci se aplică mai degrabă oricărei informații și comunicări referitoare la prelucrarea datelor cu caracter personal. Fraza 5 din Considerent clarifică, de asemenea, că persoanele vizate ar trebui să fie conștiente de riscuri, reguli, garanții și drepturi în legătură cu prelucrarea datelor cu caracter personal și modul în care își exercită drepturile în legătură cu o astfel de prelucrare.

11. Pentru proiectarea interfețelor de utilizator ale aplicațiilor online, este, de asemenea, important să se țină cont de principiul limitării scopului în conformitate cu articolul 5 alineatul (1) litera (b) din RGPD, precum și de principiul minimizării datelor în conformitate cu articolul 5 alineatul (1) litera (c) din RGPD. În orice caz, pentru a asigura conformitatea cu cerințele de protecție a datelor, operatorii sunt îndemnați să verifice de două ori conformitatea cu toate principiile de protecție a datelor în baza RGPD.

---

[14] Orientările CEPD 8/2020 privind direcționarea utilizatorilor platformelor de comunicare socială, Declarația 2/2019 privind utilizarea datelor cu caracter personal în cadrul campaniilor politice https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political en.

[15] Orientările CEPD 4/20219 privind articolul 25 Protecția datelor începând cu momentul conceperii și cel al protecției implicite, versiunea 2.0, adoptată la 20 octombrie 2020, p. 16; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and en.

[16] Abordate în partea 3.2. – cazul de utilizare 2a din prezentele Orientări.

[17] Abordate în cazurile de utilizare 4 și 5, adică părțile 3.4 și 3.5 din prezentele Orientări.

2.1 Responsabilitatea

12. Principiul responsabilității trebuie să se reflecte în fiecare interfață de utilizator.

13. Conform articolului 5 alineatul (2) din RGPD, operatorul trebuie să fie responsabil și să poată demonstra conformitatea cu principiile prevăzute în RGPD la articolul 5 alineatul (1) din RGPD. Astfel, acest principiu este strâns legat de principiile relevante menționate mai sus. Responsabilitatea poate fi asigurată de elemente, care oferă dovada conformității furnizorului platformei de comunicare socială cu prevederile RGPD. Interfața de utilizator și călătoria utilizatorului pot fi folosite ca instrument de documentare pentru a demonstra că utilizatorii, în timpul acțiunilor lor pe platforma de comunicare socială, au citit și au luat în considerare informațiile privind protecția datelor, și-au exprimat liber consimțământul, și-au exercitat cu ușurință drepturile etc. Metodele calitative și cantitative de cercetare a utilizatorilor, cum ar fi testarea A/B, urmărirea cu ochii sau interviurile cu utilizatorii, rezultatele și analiza acestora pot fi, de asemenea, utilizate pentru a susține demonstrarea conformității. Este important de menționat faptul că astfel de metode de cercetare deseori implică și prelucrarea datelor cu caracter personal, care, prin urmare, trebuie să fie în conformitate cu prevederile RGPD. Dacă, de exemplu, utilizatorii trebuie să bifeze o casetă sau să facă clic pe una din mai multe opțiuni de protecție a datelor, capturile de ecran ale interfețelor pot arăta calea utilizatorilor prin informațiile privind protecția datelor și pot explica modul în care utilizatorii iau o decizie informată. Rezultatele cercetării efectuate de utilizatori pe această interfață ar aduce elemente suplimentare, care explică detaliat de ce interfața este optimă pentru atingerea unui obiectiv de informare.

14. În ceea ce privește interfețele de utilizator, astfel de elemente documentare pot fi găsite în informațiile despre anumite acorduri, în special atunci când se obțin dovezi, de exemplu, de exprimare a consimțământului sau de confirmare a citirii.

2.2 Transparența

15. Principiul transparenței prevăzut la articolul 5 alineatul (1) litera (a) din RGPD are o suprapunere mare cu domeniul responsabilității generale. Chiar dacă operatorii trebuie să protejeze anumite informații comerciale sensibile față de terți, accesibilitatea sau posibilitatea de înregistrare a documentației privind prelucrarea ar putea contribui la asigurarea răspunderii: Confirmarea citirii poate fi obținută, de exemplu, pentru un text, pe care operatorul trebuie să îl pună la dispoziție în conformitate cu principiul transparenței. Acesta poate întotdeauna facilita asigurarea transparenței față de persoanele vizate.

16. Toate principiile de protecție a datelor prevăzute la articolul 5 din RGPD sunt specificate în continuare în RGPD. Conform articolului 5 alineatul (1) litera (a) din RGPD, datele cu caracter personal trebuie prelucrate într-un mod transparent în raport cu persoana vizată. Orientările privind transparența specifică elementele de transparență prevăzute la articolul 12 din RGPD, adică necesitatea de a prezenta informațiile într-o formă „concisă, transparentă, inteligibilă și

ușor accesibilă, într-un limbaj clar și simplu".[18] Aceste Orientări oferă, de asemenea, îndrumare cu privire la modul de îndeplinire a obligațiilor de informare în temeiul articolelor 13 și 14 din RGPD cu privire la furnizorii platformelor de comunicare socială.

17. De asemenea, textul principiilor de protecție a datelor de la articolul 5 alineatul (1) litera (a) din RGPD și alte dispoziții legale speciale din Regulament conțin mult mai multe detalii despre principiul transparenței, care sunt legate de principii juridice specifice, cum ar fi cerințele de transparență prevăzute la articolul 7 din RGPD pentru obținerea consimțământului.

2.3 Protecția datelor începând cu momentul conceperii și în mod implicit

18. Articolul 25 alineatul (1) din RGPD specifică faptul că operatorii trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate, care sunt destinate să pună în aplicare principiile de protecție a datelor, în timp ce articolul 25 alineatul (2) din RGPD clarifică faptul că astfel de măsuri trebuie să fie, de asemenea puse în aplicare pentru asigurarea că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. În contextul Orientărilor 04/2019 privind articolul 25 referitor de asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, există câteva elemente cheie de care operatorii și persoanele împuternicite de operatori trebuie să le ia în considerare atunci când implementează protecția datelor începând cu momentul conceperii pentru o platformă de comunicare socială. Conform uneia dintre ele, în ceea ce privește principiul echității, informațiile și opțiunile de prelucrare a datelor ar trebui asigurate într-un mod obiectiv și neutru, evitând orice limbaj sau interfață înșelătoare sau manipulatoare.[19] Orientările prezintă elementele principiilor de protecție a datelor începând cu momentul conceperii și în mod implicit, printre altele, care devin și mai relevante în ceea ce privește modelele de interfață înșelătoare:[20]

- Autonomia – Persoanelor vizate ar trebui să li se acorde cel mai înalt grad de autonomie posibil pentru a determina utilizarea datelor lor cu caracter personal, precum și autonomie în privința domeniului și condițiilor utilizării sau prelucrării respective.
- Interacțiunea – Persoanele vizate trebuie să poată comunica și exercita drepturile cu privire la datele cu caracter personal prelucrate de operator.
- Așteptarea – Prelucrarea trebuie să corespundă așteptărilor rezonabile ale persoanelor vizate.
- Alegerea consumatorului – Operatorii nu ar trebui să-și „blocheze" utilizatorii într-un mod injust. Ori de câte ori un serviciu de prelucrare a datelor cu caracter personal este proprietar, acesta poate bloca accesul la serviciu, ceea ce poate să nu fie echitabil, dacă afectează posibilitatea persoanelor vizate de a-și exercita dreptul la portabilitatea datelor în conformitate cu articolul 20 din RGPD.
- Echilibrul de putere – Echilibrul de putere ar trebui să fie un obiectiv cheie al relației dintre operator și persoana vizată. Dezechilibrele de putere ar trebui evitate. Dacă nu este posibil, acestea ar trebui recunoscute și luate în considerare cu contramăsuri corespunzătoare.

[18] Articolul 29 din Orientările grupului de lucru privind transparența în conformitate cu Regulamentul 2016/679, aprobate de CEPD https://ec.europa.eu/newsroom/article29/item-detail.cfm7item id=622227.

[19] A se vedea Orientările 04/20219 privind articolul 25 referitor de asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, p. 18, alin. 70.

[20] Extras - pentru lista completă, a se vedea Orientările privind articolul 25 referitor de asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, alin. 70.

- Lipsa de înșelăciune – Informațiile și opțiunile de prelucrare a datelor trebuie asigurate într-un mod obiectiv și neutru, evitând orice limbaj sau interfață înșelătoare sau manipulatoare.
- Veridicitatea – operatorii trebuie să pună la dispoziție informații despre modul în care prelucrează datele cu caracter personal, ar trebui să acționeze astfel cum declară că vor acționa și să nu inducă în eroare persoanele vizate.

19. Conformitatea cu dispozițiile privind protecția datelor începând cu momentul conceperii și în mod implicit este importantă în procesul de evaluare a modelelor de interfață înșelătoare, deoarece în primul rând ar contribui la evitarea acestora. Într-adevăr, confruntarea serviciului și a interfețelor asociate cu elementele care cuprind principii de protecție a datelor începând cu momentul conceperii și în mod implicit, cum ar fi cele menționate mai sus, va facilita identificarea aspectelor serviciului, care ar constitui un model de interfață înșelătoare înainte de lansarea serviciului. De exemplu, dacă informațiile privind protecția datelor sunt prezentate fără a respecta principiul „Lipsei de înșelăciune", atunci este probabil să constituie un model de interfață înșelătoare de tip ***Ascuns la vedere*** sau ***Dirijare emoțională***, care vor fi prezentate detaliat în continuare în cazul de utilizare 1.

3. CICLUL DE VIAȚĂ AL UNUI CONT PE O PLATFORMĂ DE COMUNICARE SOCIALĂ: PUNEREA ÎN APLICARE A PRINCIPIILOR

20. RGPD se aplică întregului proces de prelucrare a datelor cu caracter personal prin mijloace automate.[21] În cazul prelucrării datelor cu caracter personal ca parte a operării platformelor de comunicare socială, prevederile RGPD și principiile acestuia se aplică întregului ciclu de viață al unui cont de utilizator.

3.1 Deschiderea unui cont pe o platformă de comunicare socială

Cazul de utilizare 1: Înregistrarea unui cont

a. Descrierea contextului

21. Primul pas, pe care trebuie să-l facă utilizatorii pentru a obține acces la o platformă de comunicare socială, este înregistrarea prin crearea unui cont. În cadrul acestui proces de înregistrare, utilizatorii sunt solicitați să introducă datele lor cu caracter personal, cum ar fi numele și prenumele, adresa de e-mail sau, uneori, numărul de telefon. Utilizatorii trebuie să fie informați despre prelucrarea datelor lor cu caracter personal și, de obicei, sunt solicitați să confirme că au citit notificarea de confidențialitate și că sunt de acord cu condițiile de utilizare a platformei de comunicare socială. Aceste informații trebuie să fie într-un limbaj clar și simplu, astfel încât utilizatorii să înțeleagă cu ușurință și să fie de acord cu bună știință.

22. La această etapă inițială a procesului de înregistrare, utilizatorii ar trebui să înțeleagă pentru ce anume se înregistrează, adică obiectul acordului dintre platforma de comunicare socială și utilizatori ar trebui descris cât mai clar și simplu posibil.

23. Prin urmare, protecția datelor începând cu momentul conceperii trebuie să fie luată în considerare de către furnizorii platformelor de comunicare socială într-un mod corespunzător pentru a proteja drepturile și libertățile persoanelor vizate.[22]

b. Prevederi legale relevante

24. Furnizorii platformelor de comunicare socială trebuie să implementeze în mod corespunzător principiile prevăzute la articolul 5 din RGPD atunci când își proiectează interfețele. Transparența față de persoanele vizate este esențială întotdeauna, în special la etapa creării unui cont pe o platformă de comunicare socială. Datorită poziției lor de operator sau persoană împuternicită de operator, platformele de comunicare socială ar trebui să prezinte informații utilizatorilor atunci când se înregistrează în mod eficient și clar, precum și informații diferențiate în mod corespunzător de alte informații, care nu sunt legate de protecția datelor.[23] O parte din obligațiile de transparență ale operatorilor constă în informarea utilizatorilor despre drepturile lor, inclusiv

[21] A se vedea articolul 2 alineatul (1) din RGPD.
[22] A se vedea Orientările 04/2019 privind articolul 25 referitor de asigurarea protecției datelor începând cu momentul conceperii și în mod implicit.
[23] A se vedea Orientările privind transparența, p. 8.

despre dreptul lor de a-și retrage consimțământul în orice moment, dacă este un temei legal aplicabil.[24]

i. Consimțământul exprimat în procesul de înregistrare

25. Conform articolului 4 alineatul (11) și articolului 7 din RGPD, clarificat în Considerentul 32, atunci când consimțământul este ales ca temei juridic pentru prelucrare, acesta trebuie să fie *„o manifestare liber exprimată, specifică, în cunoștință de cauză și fără ambiguitate a dorințelor persoanei vizate prin care aceasta, printr-o declarație sau printr-o acțiune afirmativă clară, semnifică acordul pentru prelucrarea datelor cu caracter personal care o privesc”*. Toate aceste cerințe față de consimțământ trebuie îndeplinite cumulativ pentru ca acesta să fie considerat valabil.

26. Pentru furnizorii platformelor de comunicare socială, care solicită consimțământul utilizatorilor pentru diferite scopuri de prelucrare, Orientările 05/2020 ale CEPD privind consimțământul oferă îndrumări utile privind obținerea consimţământului.[25] Platformele de comunicare socială nu trebuie să eludeze condiții, cum ar fi capacitatea persoanelor vizate de a-și exprima liber consimțământul, prin interfețe grafice sau formulare care împiedică persoanele vizate să își exercite voința. În acest sens, articolul 7 alineatul (2) din RGPD prevede că consimțământul trebuie solicitat într-un mod, care să se distingă clar de alte aspecte, într-o formă inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu. Utilizatorii platformelor de comunicare socială pot oferi consimțământul pentru publicitate sau tipuri speciale de analiză în timpul înregistrării și la o etapă ulterioară prin intermediul setărilor de protecție a datelor. În orice caz, după cum este menționat în Considerentul 32 din RGPD, consimțământul trebuie întotdeauna acordat printr-un act afirmativ clar, astfel încât casetele bifate în prealabil sau inactivitatea utilizatorilor să nu constituie consimțământ.[26]

27. După cum s-a menționat deja în Orientările CEPD privind consimțământul, pentru a atinge pragul consimțământului „informat”, trebuie să existe informații minime accesibile utilizatorilor.[27] Dacă nu este cazul, consimțământul obținut în procesul de înregistrare nu poate fi considerat valabil în conformitate cu RGPD, iar prelucrarea este ilegală.

28. Utilizatorii sunt solicitați să își exprime consimțământul pentru diferite scopuri (de exemplu, prelucrarea ulterioară a datelor cu caracter personal). Consimțământul nu este specific și, prin urmare, nu este valabil atunci când utilizatorilor nu le este explicat, de asemenea, într-un mod clar cu ce sunt de acord.[28] După cum prevede articolul 7 alineatul (2) din RGPD, consimțământul ar trebui solicitat astfel încât să-l distingă în mod clar de alte informații, indiferent de modul în care informațiile sunt prezentate persoanei vizate. În special, atunci când consimțământul este solicitat prin mijloace electronice, acesta nu trebuie inclus în condiții.[29] Ținând cont de faptul că un număr tot mai mare de utilizatori accesează platformele de comunicare socială folosind interfața telefoanelor lor mobile inteligente pentru a se înregistra pe platformă, furnizorii platformelor de comunicare socială trebuie să acorde o atenție deosebită modului în care este

[24] Orientările privind transparența, p. 30 și pag. 39.
[25] Orientările 05/2020 ale CEPD privind consimțământul în conformitate cu Regulamentul 2016/679, versiunea 1.1., adoptată la 4 mai 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb guidelines 202005 consent en.pdf.
[26] A se vedea Curtea de Justiție a Uniunii Europene, Hotărârea din 1 octombrie 2019, *Verbraucherzentrale Bundesverband e.V. împotrtiva Planet 49 GmbH,* cauza C-673/17, p. 62-63.
[27] Orientările 05/2020 privind consimțământul, p. 64; a se vedea, de asemenea, mai jos cazul de utilizare 3a în partea 3.3. din aceste Orientări.
[28] A se vedea Orientările 05/2020 privind consimțământul, p. 68.
[29] Orientările privind transparența, p. 8.

solicitat consimțământul, pentru ca acest consimțământul să se deosebească. Utilizatorilor nu trebuie să le fie prezentate informații excesive, care să-i determine să omită citirea acestora. În caz contrar, atunci când utilizatorii sunt „solicitați" să confirme că au citit politica de confidențialitate integral și sunt de acord cu condițiile furnizorului platformei de comunicare socială, inclusiv cu toate operațiunile de prelucrare, pentru a crea un cont, consimțământul exprimat în acest car poate fi calificat drept consimțământ forțat cu condițiile speciale respective. Dacă refuzul consimțământului duce la refuzul serviciului, acesta nu poate fi considerat ca fiind exprimat liber, detaliat și specific, astfel cum prevede RGPD. Consimțământul, care este „combinat" cu acceptarea condițiilor unui furnizor al platformei de comunicare socială nu se califică ca fiind „exprimat în mod liber".[30] Este și cazul în care operatorul, pentru semnarea unui contract sau prestarea unui serviciu, solicită consimțământul, astfel încât să prelucreze datele cu caracter personal care nu sunt necesare pentru îndeplinirea contractului.

29. Dacă consimțământul trebuie exprimat printr-o acțiune pozitivă din partea utilizatorilor, lipsa consimțământului ar trebui să fie considerată o stare implicită până la exprimarea acestuia. Astfel, pentru exprimarea refuzului, nu ar trebui să fie necesară nicio acțiune din partea utilizatorilor sau refuzul ar trebui să fie posibil printr-o acțiune cu același grad de simplitate ca și acțiunea necesară pentru exprimarea consimțământului.[31]

ii. Retragerea consimțământului – articolul 7 alienatul (3) din RGPD

30. În conformitate cu articolul 7 alineatul (3) fraza 1 din RGPD, utilizatorii platformelor de comunicare socială își pot retrage consimțământul în orice moment. Înainte de a-și exprima consimțământul, utilizatorii vor fi, de asemenea, informați că au dreptul să-și retrage consimțământul, conform articolului 7 alineatul (3) fraza 3 din RGPD. În special, operatorii trebuie să demonstreze că utilizatorii au posibilitatea de a refuza să-și acorde consimțământul sau de a-l retrage fără nicio prejudiciu. Utilizatorii platformelor de comunicare socială, care își exprimă consimțământul pentru prelucrarea datelor lor cu caracter personal printr-un singur clic, de exemplu bifând o casetă, îl vor putea retrage într-un mod la fel de simplu.[32] Așa dar consimțământul ar trebui să fie o decizie reversibilă, astfel încât persoana vizată să aibă un grad de control asupra prelucrării respective.[33] Retragerea ușoară a consimțământului constituie o condiție prealabilă a consimțământului valabil în conformitate cu articolul 7 alineatul (3) fraza 4 din RGPD și ar trebui să fie posibilă fără a reduce nivelul de servicii.[34] De exemplu, consimțământul nu poate fi considerat valabil în conformitate cu RGPD dacă este obținut printr-un singur clic, printr-o singură glisare sau apăsare a tastei, dar retragerea necesită mai mulți pași,[35] este mai complicată sau durează mai mult timp.

c. Modele de interfață înșelătoare

31. Mai multe prevederi ale RGPD se referă la procesul de înregistrare. Prin urmare, unele modele de interfață înșelătoare pot apărea atunci când furnizorii platformelor de comunicare socială nu implementează RGPD în mod corespunzător.

i. Modele bazate pe conținut

Supraîncărcarea – Solicitarea continuă (Lista de verificare 4.1.1 din Anexa I)

[30] A se vedea Orientările 8/2020 privind direcționarea utilizatorilor platformelor de comunicare socială, p. 57.
[31] A se vedea Considerentul 42, fraza 5, din RGPD.
[32] A se vedea Orientările privind transparența, p. 113 și următoarele.
[33] Orientările 05/2020 privind consimțământul, p. 10.
[34] Orientările 05/2020 privind consimțământul, p. 114.
[35] A se vedea Orientările 05/2020 privind consimțământul, p. 114.

32. Modelul de interfață înșelătoare ***Solicitare continuă*** există atunci, când utilizatorii sunt împinși să ofere mai multe date cu caracter personal, decât este necesar în scopul prelucrării sau să accepte o altă utilizare a datelor lor, fiind solicitați în mod repetat să ofere date suplimentare sau să-și exprime consimțământul cu un scop de prelucrare. Astfel de solicitări repetate pot apărea prin unul sau mai multe dispozitive. Este posibil ca utilizatorii să fie nevoiți să cedeze, deoarece sunt obosiți să refuze cererea de fiecare dată când folosesc platforma.

Exemplul 1:
Varianta A: La primul pas al procesului de înregistrare, utilizatorii sunt solicitați să aleagă între diferite opțiuni de înregistrare. Ei pot indica o adresă de e-mail sau un număr de telefon. Atunci când utilizatorii aleg să indice adresa de e-mail, furnizorul platformei de comunicare socială încearcă în continuare să convingă utilizatorii să indice numărul de telefon, declarând că acesta va fi folosit pentru securizarea contului, fără a oferi alternative pentru datele, care ar putea fi sau au fost deja acordate de către utilizatori. În mod specific, în procesul de înregistrare apar mai multe ferestre cu un câmp pentru indicarea numărului de telefon, împreună cu explicația *„Vom folosi numărul dvs. de telefon pentru securizarea contului”.* Deși utilizatorii pot închide fereastra, ei se supraîncărcă și renunță indicând numărul lor de telefon.
Varianta B: Un alt furnizor de platformă de comunicare socială solicită în mod repetat utilizatorilor să indice numărul de telefon de fiecare dată când aceștia se loghează în contul lor, în pofida faptului că utilizatorii au refuzat anterior să-l indice, indiferent dacă au fost solicitați în timpul înregistrării sau la ultima logare.

33. Exemplul de mai sus prezintă o situație în care utilizatorii sunt solicitați în mod continuu să ofere anumite date cu caracter personal, cum ar fi numărul lor de telefon. Dacă în varianta A a exemplului, această ***Solicitare continuă*** apare de mai multe ori în timpul înregistrării, varianta B arată că utilizatorii se pot confrunta cu acest model de interfață înșelătoare și după ce s-au înregistrat. Pentru a evita acest model de interfață înșelătoare, este important să acordați atenție în special principiilor de minimizare a datelor în conformitate cu articolul 5 alineatul (1) litera (c) din RGPD și, în astfel de cazuri precum cel descris în exemplul 1 varianta A, principiului de limitare a scopului conform articolului 5 alineatul (1) litera (b) din RGPD. Prin urmare, atunci când furnizorii platformelor de comunicare socială declară că vor folosi numărul de telefon „pentru securizarea contului”, aceștia vor procesa numărul de telefon doar în scopurile de securitate menționate și nu trebuie să proceseze în continuare numărul de telefon depășind acest scop inițial.

34. Pentru a respecta principiul minimizării datelor, furnizorii platformelor de comunicare socială sunt obligați să nu solicite date suplimentare, cum ar fi numărul de telefon, dacă datele deja acordate de utilizatori în timpul procesului de înregistrare sunt suficiente. De exemplu, pentru a asigura securitatea contului, autentificarea îmbunătățită este posibilă fără numărul de telefon prin simpla trimitere a unui cod în conturile de e-mail ale utilizatorilor sau prin alte mijloace.

35. Prin urmare, furnizorii platformelor de comunicare socială ar trebui să se bazeze pe mijloace de securitate, care sunt mai ușor de reinițiat de către utilizatori. De exemplu, furnizorul platformei de comunicare socială poate trimite utilizatorilor un număr de autentificare printr-un canal de comunicare suplimentar, cum ar fi o aplicație de securitate, pe care utilizatorii au instalat-o anterior pe telefonul lor mobil, dar fără a solicita numărul de telefon mobil al utilizatorilor. Autentificarea utilizatorilor prin adrese de e-mail este, de asemenea, mai puțin intruzivă decât prin numărul de telefon, deoarece utilizatorii ar putea pur și simplu să creeze o adresă de e-mail nouă special pentru procesul de înregistrare și să utilizeze această adresă de e-mail în principal în legătură cu rețeaua socială. Cu toate acestea, un număr de telefon nu este

interschimbabil atât de ușor, având în vedere faptul că este foarte puțin probabil ca utilizatorii să cumpere o cartelă SIM nouă sau să încheie un contract de servicii de telefonie nou doar din considerente de autentificare.

36. Trebuie avut în vedere faptul că, dacă scopul unei astfel de solicitări este de a demonstra că utilizatorii posedă legitim dispozitivul utilizat pentru autentificarea în rețeaua de socializare, acest scop poate fi atins prin mai multe mijloace, un număr de telefon fiind doar unul dintre ele. Astfel, un număr de telefon poate constitui doar o opțiune relevantă voluntară pentru utilizatori. În cele din urmă, utilizatorii trebuie să decidă dacă doresc să folosească acest mijloc de autentificare. În special, numerele de telefon ale utilizatorilor nu sunt necesare pentru o verificare unică, deoarece adresa de e-mail este un mijloc obișnuit de contact cu utilizatorii în timpul înregistrării.

37. Practica prezentată în exemplul 1, varianta A, poate induce în eroare utilizatorii și îi poate determina să refuze să ofere astfel de informații, considerând că nu sunt necesare pentru a activa sau a proteja contul. În orice caz, în realitate, utilizatorii nu au primit niciodată alternativă (de exemplu, utilizarea adresei de e-mail pentru activarea contului și în scopuri de securizare). În exemplul 1, varianta B, utilizatorii nu sunt informați care este scopul prelucrării. Totuși, această variație constituie un model de interfață înșelătoare ***Solicitare continuă,*** deoarece furnizorul platformei de comunicare socială ignoră faptul că utilizatorii au refuzat anterior să indice numărul de telefon, și continuă să-l solicite. Atunci când utilizatorii au impresia că pot evita această solicitare repetată doar introducând datele lor, este probabil să cedeze și să-l indice.

38. În următorul exemplu utilizatorii sunt încurajați în mod repetat să acorde platformei de comunicare socială acces la datele lor de contact:

Exemplul 2: O platformă de comunicare socială folosește o informație sau o pictogramă cu semn de întrebare pentru a încuraja utilizatorii să întreprindă acțiunea „opțională” solicitată în prezent. Cu toate acestea, în loc să ofere informații utilizatorilor, care așteaptă ajutor de la aceste butoane, platforma solicită utilizatorilor să accepte importul datelor lor de contact din contul lor de e-mail, afișând în mod repetat o fereastră pop-up, cu mesajul *„Hai să o facem”.*

39. În special în procesul de înregistrare această ***Solicitare continuă*** poate influența utilizatorii să accepte doar cererea platformei pentru a-și finaliza în sfârșit înregistrarea. Efectul acestui model de interfață înșelătoare este sporit atunci când este combinat cu un limbaj motivațional, ca în acest exemplu, creând un sentiment de urgență.

40. Efectele de influență ale textului și elementelor vizuale vor fi abordate în continuare mai jos, în examinarea modelului de interfață înșelătoare, ***Dirijarea emoțională***.[36]

Obstrucționarea – Acțiune înșelătoare (Lista de verificare 4.4.3 din Anexa I)
41. Un alt exemplu de situație, în care furnizorii platformelor de comunicare socială solicită numerele de telefon ale utilizatorilor fără a fi nevoie, se referă la utilizarea aplicației platformei:

Exemplul 3: Când se înregistrează pe o platformă de comunicare socială prin intermediul browserului de desktop, utilizatorii sunt invitați să folosească și aplicația mobilă a platformei. La o altă etapă de înregistrare, utilizatorii sunt invitați să descarce aplicația. Când fac clic pe

[36] A se vedea p. 43 și următoarele, în cazul de utilizare 1, precum și prezentarea generală a exemplelor în lista de verificare a Anexei.

pictogramă, așteptând să fie direcționați către un magazin de aplicații, sunt solicitați în schimb să ofere numărul lor pentru a primi un mesaj textual cu linkul către aplicație.

42. Explicarea utilizatorilor că trebuie să indice numărul de telefon pentru a primi un link de descărcare a aplicației constituie o ***Acțiune înșelătoare*** din mai multe motive: în primul rând, există mai multe modalități prin care utilizatorii pot utiliza o aplicație, de exemplu, scanând un cod QR, folosind un link sau descărcând aplicația din magazinul de aplicații. În al doilea rând, aceste alternative arată că nu există un motiv obligatoriu, pentru care furnizorul platformei de comunicare socială să solicite numărul de telefon al utilizatorilor. După înregistrare, utilizatorii trebuie să poată folosi datele de autentificare (adică, de obicei adresa de e-mail și parola) pentru a se loga indiferent de dispozitivul pe care îl folosesc, fie că folosesc un browser de desktop, un dispozitiv mobil sau o aplicație. Cu atât mai mult este cazul în care, în locul unui telefon inteligent, utilizatorii ar prefera să instaleze aplicația pe tableta lor, care nu este legată de un număr de telefon.

Agitarea – Dirijarea emoțională (Lista de verificare 4.3.1 din Anexa I)

43. Cu modelul de interfață înșelătoare ***Dirijarea emoțională***, formulările sau elementele vizuale (cum ar fi stilul, culorile, pozele sau altele) sunt folosite astfel, ca să transmită informații utilizatorilor fie într-o perspectivă extrem de pozitivă, făcându-i pe utilizatori să se simtă bine, în siguranță sau răsplătiți, fie într-un mod extrem de negativ, făcând utilizatorii să se simtă îngrijorați, vinovați sau pedepsiți. Modul în care informațiile sunt prezentate utilizatorilor le influențează starea emoțională, determinându-i să acționeze împotriva intereselor lor de protecție a datelor. Impactul unor astfel de practici poate fi și mai eficient, dacă se bazează pe datele colectate de platformă. Influențarea deciziilor prin acordarea informațiilor părtinitoare persoanelor fizice poate fi considerată, în general, o practică neloială contrară principiului echității prelucrării prevăzut la articolul 5 alineatul (1) litera (a) din RGPD. Aceasta poate apărea pe parcursul întregii călătorii a utilizatorului în cadrul unei platforme de comunicare socială. Cu toate acestea, la etapa de înregistrare, efectul de direcționare poate fi deosebit de puternic, având în vedere supraîncărcarea informațiilor, cu care ar putea fi nevoiți să se confrunte utilizatorii în afară de pașii necesari pentru a finaliza înregistrarea.

44. În lumina celor menționate mai sus, ***Dirijarea emoțională*** la etapa înregistrării pe o platformă de comunicare socială poate avea un impact și mai mare asupra copiilor, persoanelor în etate și altor grupuri (adică să acorde mai multe date cu caracter personal din cauza neînțelegerii activităților de prelucrare), având în vedere caracterul lor vulnerabil ca persoane vizate.[37] Atunci când serviciile platformei de comunicare socială sunt adresate copiilor sau altor persoane vizate vulnerabile, limbajul folosit, inclusiv tonul și stilul acestuia, trebuie să fie potrivit pentru ca utilizatorii vulnerabili, în calitate de destinatari ai mesajului, să înțeleagă cu ușurință informațiile prezentate.[38] Având în vedere vulnerabilitatea copiilor, a persoanelor în etate și a altor persoane vizate, modelele de interfață înșelătoare pot influența acești utilizatori să prezinte mai multe informații, deoarece expresiile „imperative” le pot crea sentimentul că sunt obligați să le împărtășească, de exemplu sentimentul de popularitate în rândul colegilor sau că acordarea datelor este obligatorie.

45. Atunci când utilizatorii platformelor de comunicare socială sunt îndemnați să ofere rapid datele lor, aceștia nu au timp să „prelucreze” și astfel să înțeleagă cu adevărat informațiile, care

[37] A se vedea, de asemenea, mai sus, p. 7.
[38] Vezi Orientările privind transparența, p. 18.

le sunt prezentate, pentru a lua o decizie conștientă. Limbajul motivațional folosit de platformele de comunicare socială ar putea încuraja utilizatorii să ofere ulterior mai multe date decât este necesar, atunci când consideră că ceea ce propune platforma de comunicare socială este ceea ce vor face majoritatea utilizatorilor și astfel „modul corect" de a proceda.

Exemplul 4: Platforma de comunicare socială solicită utilizatorilor să indice geolocalizarea lor, afirmând: „Hei, ești un lup singuratic? Partajând informații și stabilind relații cu alții vom face lumea mai bună! Împărtășește-ți geolocalizarea! Lasă locurile și oamenii din jur să te inspire!"

46. În timpul înregistrării, scopul utilizatorilor este să finalizeze înregistrarea pentru a putea folosi platforma de comunicare socială. Modelele de interfață înșelătoare, cum ar fi ***Dirijarea emoțională***, au efecte mai puternice în acest context. Acestea riscă să fie mai puternice la mijlocul sau spre sfârșitul procesului de înregistrare spre deosebire de început, deoarece de cele mai multe ori utilizatorii vor parcurge toți pașii necesari „în grabă" sau vor fi mai susceptibili la un sentiment de urgență. În acest context, utilizatorii sunt mai predispuși să die de acord să introducă toate datele solicitate, decât să se întrebe dacă ar trebui să le indice. În acest sens, limbajul motivațional folosit de furnizorul platformei de comunicare socială poate avea o influență asupra deciziei instantanee a utilizatorilor, la fel ca și combinarea limbajului motivațional cu alte forme de accentuare, cum ar fi semnele exclamării, astfel cum este prezentat în exemplul de mai jos.

Exemplul 5: Furnizorul platformei de comunicare socială încurajează utilizatorii să indice mai multe date cu caracter personal decât este necesar, solicitându-i să prezinte o autodescriere: *„Spuneți-ne ceva despre personalitatea dvs. minunată! Așteptăm cu nerăbdare, veniți chiar acum și spuneți-ne!"*

47. Prin această practică, platformele de comunicare socială obțin un profil mai detaliat al utilizatorilor lor. Cu toate acestea, în dependență de caz, acordarea mai multor date cu caracter personal, de exemplu despre personalitatea utilizatorilor, ar putea să nu fie necesară pentru utilizarea serviciului și, prin urmare, ar putea încălca principiul minimizării datelor conform articolului 5 alineatul (1) litera (c) din RGPD. După cum este prezentat în exemplul 5, astfel de tehnici nu cultivă dorința liberă a utilizatorilor să-și comunice datele, deoarece limbajul prescriptiv utilizat poate face utilizatorii să se simtă obligați să prezinte o autodescriere, deoarece au cheltuit deja timp pentru înregistrare și doresc să o finalizeze. Atunci când utilizatorii se înregistrează pentru crearea unui cont, este mai puțin probabil să cheltuiască timp ca să examineze descrierea pe care o oferă sau chiar să se gândească să ofere sau nu o descriere. Acesta este în special cazul atunci, când limbajul folosit creează un sentiment de urgență sau sună ca un imperativ. Dacă utilizatorii au acest sentiment de obligație, chiar și atunci când comunicarea datelor nu este obligatorie, „dorința lor liberă" poate fi influențată. Aceasta înseamnă, de asemenea, că informațiile acordate de platforma de comunicare socială nu au fost clare.

Exemplul 6: Partea procesului de înregistrare, în care utilizatorii sunt rugați să-și încarce fotografia, conține un buton cu semnul „?". Făcând clic pe el, apare următorul mesaj: *„Nu este nevoie să mergeți mai întâi la coafor. Doar alegeți o fotografie personală"*.

48. Chiar dacă propozițiile din exemplul 6 au scopul de a motiva utilizatorii și a simplifica aparent procesul de dragul lor (adică nu este nevoie de o fotografie oficială pentru înregistrare), astfel de

practici pot afecta decizia finală a utilizatorilor, care au decis inițial să nu încarce o poză pentru contul lor. Semnele de întrebare sunt folosite pentru întrebări ca pictograme, iar utilizatorii se pot aștepta să găsească informații utile atunci când fac clic pe ele. Atunci când această așteptare nu este satisfăcută și utilizatorii sunt în schimb îndemnați încă o dată să facă acțiunile pe care ezită să le facă, consimțământul obținut fără a informa utilizatorii despre prelucrarea pozei lor nu ar fi valabil fără respectarea cerințelor de consimțământ „informat" și „exprimat liber" conform articolului 7 din RGPD coroborat cu articolul 4 alineatul (11) din RGPD. Prin urmare, factorul emoțional are o influență puternică asupra legitimității consimțământului.

Obstrucționarea – Mai lungă decât este necesar (Lista de verificare 4.4.2 din Anexa I)

49. Atunci când utilizatorul încearcă să activeze un control legat de protecția datelor, dar în timpul călătoriei utilizatorului, trebuie să parcurgă mai mulți pași, în comparație cu numărul de pași necesari pentru activarea opțiunilor invazive de date, acesta este modelul de interfață înșelătoare ***Mai lungă decât este necesar.*** Acest model ar putea descuraja utilizatorii să activeze controalele de protecție a datelor. În procesul de înregistrare poate apărea o fereastră pop-in sau pop-up, care solicită utilizatorii să-și confirme decizia atunci când aleg o opțiune restrictivă (de exemplu, aleg să-și facă profilurile private). Exemplul de mai jos prezintă un alt caz, în care procesul de înregistrare este ***Mai lung decât este necesar***.

Exemplul 7: În timpul înregistrării, utilizatorilor care fac clic pe butoanele „săriți" pentru a evita introducerea anumitor tipuri de date, li se afișează o fereastră pop-up, care îi întreabă *„Ești sigur/ă?"*. Punându-le la îndoială decizia și, prin urmare, făcându-i să se îndoiască de ea, furnizorul platformei de comunicare socială încurajează utilizatorii să o revizuiască și să prezinte aceste tipuri de date, cum ar fi sexul, lista datelor de contact sau imaginea lor. În schimb, utilizatorii, care decid să introducă direct datele, nu văd niciun mesaj care să le solicite să-și reexamineze alegerea.

Aici, fiind solicitați să confirme că nu doresc să completeze un câmp de date, utilizatorii pot reveni la decizia lor inițială și pot introduce datele solicitate. Acesta este în special cazul utilizatorilor, care nu sunt familiarizați cu funcțiile platformei de comunicare socială. Acest model de interfață înșelătoare ***Mai lungă decât este necesar*** încearcă să influențeze deciziile utilizatorilor, reținându-i și punând la îndoială alegerea lor inițială, în afară de prelungirea inutilă a procesului de înregistrare, ceea ce constituie o încălcare a principiului echității prevăzut în articolul 5 alineatul (1) litera (a) din RGPD. Exemplul arată că modelul de interfață înșelătoare poate determina utilizatorii să dezvăluie (mai multe) date cu caracter personal decât au decis inițial. În aceste cazuri există un dezechilibru de tratare a utilizatorilor, care dezvăluie datele cu caracter personal imediat și a celor care nu le dezvăluie: Doar cei care refuză să prezinte datele, sunt rugați să-și confirme decizia, în timp ce utilizatorii care prezintă datele nu sunt rugați să-și confirme alegerea. Aceasta este o încălcare a principiului echității prevăzut la articolul 5 alineatul (1) litera (a) din RGPD cu privire la utilizatorii, care nu doresc să dezvăluie aceste date cu caracter personal.

ii. Modele bazate pe interfață

Agitarea - Ascuns la vedere (Lista de verificare 4.3.2 din Anexa I)

50. În conformitate cu principiul transparenței, persoanele vizate trebuie să primească informații într-un mod clar ca să înțeleagă cum sunt prelucrate datele lor cu caracter personal și cum le pot controla. De asemenea, aceste informații trebuie să fie ușor de observat pentru persoanele vizate. Cu toate acestea, informațiile legate de protecția datelor, în special link-urile, sunt deseori afișate astfel încât utilizatorii le pot trece cu ușurință cu vederea. Astfel de practici ***Ascunse la vedere*** folosesc un stil vizual pentru informații sau controale de protecție a datelor, care îi

îndepărtează pe utilizatori de la opțiunile avantajoase de protecție a datelor și îi apropie de opțiuni mai puțin restrictive și, prin urmare, mai invazive.

51. Folosirea unei dimensiuni mici a fontului sau a unei culori care nu contrastează suficient pentru o lizibilitate suficientă (de exemplu, culoarea textului gri slab pe fundal alb) poate avea un impact negativ asupra utilizatorilor, deoarece textul va fi mai puțin vizibil, iar utilizatorii fie îl vor trece cu vederea, fie vor avea dificultăți de a-l citi. Acesta este în special cazul când unul sau mai multe elemente atractive sunt plasate lângă informațiile obligatorii legate de protecția datelor. Aceste tehnici de interfață induc în eroare utilizatorii și fac identificarea informațiilor legate de protecția datelor lor mai împovărătoare și consumatoare de timp, deoarece necesită mai mult timp și minuțiozitate pentru identificarea informațiilor relevante.

Exemplul 8: Imediat după înregistrare, utilizatorii pot accesa informațiile privind protecția datelor doar apelând meniul general al platformei de comunicare socială și răsfoind secțiunea sub-meniului, care conține un link către *„setări de confidențialitate și de date”*. Pe această pagină link-ul către politica de confidențialitate nu este vizibil la prima vedere. Utilizatorii trebuie să observe într-un colț al paginii o pictogramă minusculă, care indică politica de confidențialitate, ceea ce înseamnă că utilizatorii cu greu pot observa unde se află informațiile referitoare la politica de protecție a datelor.

52. Este important de remarcat faptul că, chiar și atunci când furnizorii platformelor de comunicare socială pun la dispoziție toate informațiile, care trebuie acordate persoanelor vizate în temeiul articolelor 13 și 14 din RGPD, modul în care sunt prezentate aceste informații poate încălca cerințele generale de transparență prevăzute la articolul 12 alineatul (1) din RGPD. Atunci când informațiile sunt ***Ascunse la vedere*** și, prin urmare, susceptibile de a fi trecute cu vederea, acest fapt duce la confuzie sau dezorientare, iar informațiile nu pot fi considerate inteligibile și ușor accesibile, ceea ce este contrar articolului 12 alineatul (1) din RGPD.

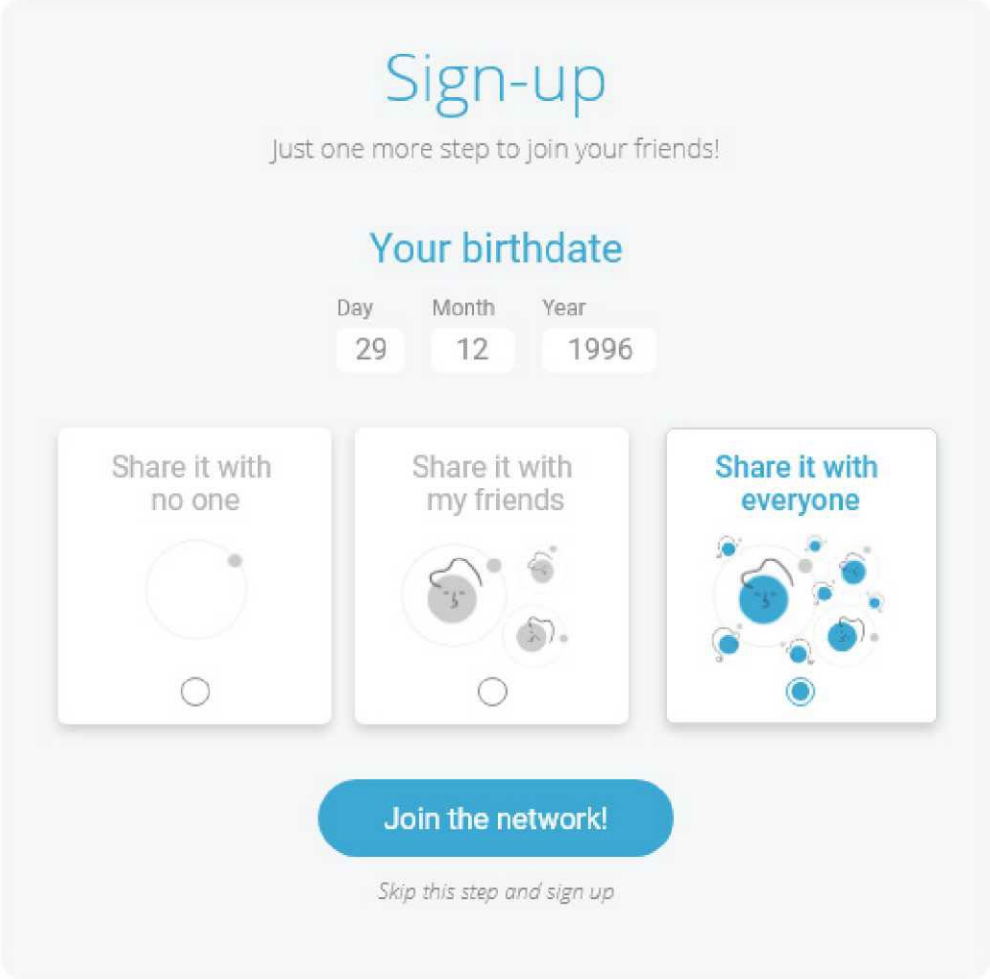
53. Dacă exemplul de mai sus prezintă modelul de interfață înșelătoare după încheierea procesului de înregistrare, acest model apare deja și în timpul înregistrării, astfel cum va fi prezentat în exemplul de mai jos, care combină modelele ***Ascuns la vedere*** și ***Comoditate confortabilă***.

Omiterea – Comoditate înșelătoare (Lista de verificare 4.2.1 din Anexa I)

54. Furnizorii platformelor de comunicare socială trebuie, de asemenea, să aibă în vedere principiul protecției datelor în mod implicit. Când setările de date sunt selectate în prealabil, utilizatorii beneficiază de un anumit nivel de protecție a datelor, determinat de furnizor în mod implicit, și nu de utilizatori. Mai mult, utilizatorilor nu li se oferă întotdeauna imediat opțiunea de a schimba setările cu unele mai stricte, conforme cu cerințele de protecție a datelor. Respectarea prevederilor RGPD în acest sens nu înseamnă că toate opțiunile trebuie să arate exact la fel. Cu toate acestea, dacă furnizorii platformelor de comunicare socială evidențiază una dintre opțiuni și atrag astfel atenția utilizatorilor asupra acesteia, această opțiune trebuie să fie cea mai restrictivă în ceea ce privește datele cu caracter personal, pentru a respecta, printre altele, principiul minimizării datelor prevăzut la articolul 5 alineatul (1) litera (c) din RGPD.

55. Când sunt activate în mod implicit majoritatea caracteristicilor și opțiunilor invazive de date, modelul este ***Comoditate înșelătoare***. Din cauza efectului implicit, care determină utilizatorii să păstreze o opțiune preselectată, este puțin probabil ca utilizatorii să le schimbe chiar dacă au posibilitatea. De obicei, această practică este realizată în procesul de înregistrare, astfel cum este

prezentat în exemplul 9 de mai jos, deoarece este o modalitate eficientă de a activa opțiunile invazive de date, pe care utilizatorii de altfel le-ar refuza. Astfel de modele de interfață înșelătoare sunt contrare principiului protecției datelor în mod implicit prevăzut la articolul 25 alineatul (2) din RGPD, în special atunci când afectează colectarea datelor cu caracter personal, volumul prelucrării, termenul de stocare a datelor și accesibilitatea datelor.[39]



Înregistrare
încă un pas spre alăturarea la prietenii tăi!

Data ta de naștere
Ziua Luna Anul

Nu partaja data cu nimeni | Partajează data cu prietenii mei | Partajează data cu oricine

Alătură-te rețelei!
Omite acest pas și înregistrează

Exemplul 9: În acest exemplu, atunci când utilizatorii introduc data de naștere, sunt invitați să aleagă cui să prezinte aceste informații. În timp ce sunt disponibile opțiuni mai puțin invazive, opțiunea *„partajează-le cu oricine”* este selectată în mod implicit, ceea ce înseamnă că toată

[39] A se vedea și alin. 446 din Decizia finală a Autorității irlandeze pentru protecția datelor cu privire la Instagram (Meta Platforms Ireland Limited) ca urmare a deciziei obligatorii de soluționare a litigiilor a CEPD din 28 iulie 2022, https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention en.

lumea, adică toți utilizatorii înregistrați, precum și orice utilizator al rețelei Internet, vor putea vedea data de naștere a utilizatorilor.

56. **Exemplul 9** prezintă modelul ***Comoditate înșelătoare***, deoarece nu este opțiunea care oferă cel mai înalt nivel de protecție a datelor selectat și, prin urmare, activat în mod implicit. Mai mult, efectul implicit al acestui model îi determină pe utilizatori să păstreze opțiunea preselectată, adică să nu piardă timp pentru examinarea celorlalte opțiuni la această etapă și nici să se întoarcă pentru a schimba setarea la o etapă ulterioară. Modelul ***Ascuns la vedere*** este, de asemenea, utilizat în această interfață. Într-adevăr, introducerea datei de naștere nu este obligatorie, deoarece utilizatorii pot sări peste acest pas de înregistrare făcând clic pe linkul care spune *„Omite acest pas și înregistrează-te”,* care este disponibil sub butonul *„Alătură-te rețelei!”*. Faptul că câmpul pentru data de naștere și butonul de confirmare sunt atât de proeminente ar putea să-i determine pe utilizatori să introducă data de naștere și să o trimită rețelei de socializare, deoarece ei nu observă posibilitatea de a nu partaja aceste informații. Acest efect ar fi și mai puternic, dacă ar fi folosite cercuri animate lângă câmp și buton, care atrag atenția utilizatorilor.

57. Respectarea principiului protecției datelor din momentul conceperii și în mod implicit nu înseamnă că toate opțiunile oferite trebuie să arate exact la fel. Cu toate acestea, dacă operatorii decid să evidențieze o opțiune mai mult decât cealaltă (celelalte), opțiunea evidențiată trebuie să fie cea mai restrictivă în ceea ce privește prelucrarea datelor.

58. În afară de a-i determina pe utilizatori să păstreze o opțiune, care nu se potrivește neapărat cu preferințele lor, este posibil ca furnizorii platformelor de comunicare socială să nu solicite utilizatorilor să verifice sau să modifice setările de protecție a datelor în funcție de preferințele lor după finalizarea procesului de înregistrare. Mai mult, pentru modificarea acestor setări implicite, ar putea fi necesari mai mulți pași. Atunci când utilizatorii nu sunt în niciun fel solicitați să verifice sau să modifice setările de protecție a datelor sau nu sunt direcționați într-un mod clar către orice informație conexă, nivelul lor de protecție a datelor va depinde de propria lor inițiativă. Pentru a facilita controlul utilizatorilor asupra datelor lor, pot fi folosite așa-numitele tablouri de bord pentru confidențialitate, care sunt concepute pentru a centraliza și a ușura controlul respectiv.

59. Este important de reținut că lipsa protecției datelor din momentul conceperii și în mod implicit, combinată cu efectul implicit menționat mai sus, poate avea consecințe negative pentru persoanele vizate, inclusiv pentru securitatea lor cibernetică. Afișarea publică a datelor cu caracter personal, cum ar fi data de naștere, care sunt utilizate pentru procesele de verificare de către alte servicii online, ar putea facilita accesul infractorilor la conturile de cumpărături, conturile bancare și alte conturi ale utilizatorilor. O altă consecință negativă se referă la posibilitățile de contact pe platforma de comunicare socială: atunci când opțiunea implicită de expediere a solicitărilor de contact sau a mesajelor către utilizatori este setată la „oricine”, ceea ce sporește riscul de cybergrooming și fraudă, în special în cazul grupurilor vulnerabile.

60. În sfârșit, atunci când ***Comoditate înșelătoare*** se aplică pentru obținerea consimţământului, ceea ce ar echivala cu considerarea că utilizatorii își exprimă consimțământul în mod implicit, de exemplu prin faptul că utilizează o casetă bifată în prealabil sau că consideră inactivitatea drept aprobare, condițiile pentru exprimarea consimțământului sunt prevăzute la articolul 4 (11) din RGPD nu sunt respectate și prelucrarea ar fi considerată ilegală în conformitate cu articolul 5 alineatul (1) litera (a) și articolul 6 alineatul (1) litera (a) din RGPD.

Obstrucționarea – Fundătură (Lista de verificare 4.4.1 din Anexa I)

61. Este important de menționat faptul că procesul de înregistrare este un moment determinant pentru informarea utilizatorilor. Dacă utilizatorii sunt în căutarea informațiilor și nu le găsesc, deoarece nu este disponibil sau nu funcționează niciun link de redirecționare, există un model de ***Fundătură***, deoarece utilizatorii nu pot atinge acest scop.

Exemplul 10: Utilizatorii nu primesc niciun link către informații despre protecția datelor după ce au început procesul de înregistrare. Utilizatorii nu pot găsi aceste informații, deoarece nu sunt prezentate nicăieri în interfața de înregistrare, nici măcar în subsol.

62. În practică, acest exemplu arată că utilizatorii vor putea fie să oprească înregistrarea și să se întoarcă la pagina de pornire doar dacă aceasta conține un link către notificarea de confidențialitate, fie pentru a finaliza înregistrarea, să se logheze în platforma de comunicare socială și abia apoi să aibă acces la informații legate de protecția datelor. Astfel este încălcat principiul transparenței și al accesului ușor la informațiile pe care persoanele vizate trebuie să le acorde, în conformitate cu articolul 12 alineatul (1) din RGPD. De asemenea, nu sunt îndeplinite cerințele articolului 13 alineatele (1) și (2) din RGPD, deoarece în momentul obținerii datelor cu caracter personal, nu sunt prezentate informații și nu sunt accesibile.

63. Modelul ***Fundătură*** poate apărea și în alt mod, atunci când utilizatorilor li se oferă o acțiune sau o opțiune legată de protecția datelor în procesul de înregistrare, pe care nu o pot regăsi mai târziu, în timpul utilizării serviciului.

Exemplul 11: În procesul de înregistrare, utilizatorii își pot exprima consimțământul cu prelucrarea datelor lor cu caracter personal în scop publicitar și sunt informați că își pot schimba decizia oricând doresc, odată ce s-au înregistrat pe platformele de comunicare socială, accesând politica de confidențialitate. Cu toate acestea, după ce utilizatorii au finalizat procesul de înregistrare și merg la politica de confidențialitate, nu găsesc mijloace sau indicii cum să-și retragă consimțământul cu această prelucrare.

64. În acest exemplu specific, utilizatorii nu au nicio posibilitate să-și retragă consimțământul după ce s-au înregistrat. Aici, modelul de interfață înșelătoare ***Fundătură*** încalcă dreptul persoanelor vizate de a-și retrage consimțământul în orice moment și la fel de ușor ca exprimarea consimțământului, în conformitate cu articolul 7 alineatul (3) frazele 1 și 4 din RGPD.

65. În cele din urmă, direcționarea utilizatorilor către un link, care se presupune că îi conduce către pagini legate de protecția datelor, cum ar fi setările sau informațiile privind protecția datelor, este, de asemenea, un exemplu de model ***Fundătură***, dacă linkul este întrerupt și nu sunt disponibile linkuri de rezervă, care ar ajuta utilizatorii să găsească ceea ce caută. Astfel, utilizatorii nu pot căuta informații relevante, dacă nu le sunt oferite explicații, cum ar fi motivul de ce se întâmplă astfel (de exemplu, probleme tehnice). În asemenea cazuri, apar aceleași probleme legate de transparență și acces ușor la informații, care sunt descrise la p. 58.

d. Cele mai bune practici

Pentru a proiecta interfețele de utilizator, care să faciliteze implementarea eficientă a RGPD, CEPD recomandă implementarea următoarelor celor mai bune practici pentru procesul de înregistrare:

Comenzi rapide: Linkurile către informații, acțiuni sau setări, care pot ajuta practic utilizatorii să-și gestioneze datele și setările de protecție a datelor ar trebui să fie disponibile oriunde găsesc

informații sau experiențe conexe *(de exemplu, linkuri care redirecționează către părțile relevante ale politicii de confidențialitate).*

Informații de contact: Adresa de contact a companiei pentru adresarea solicitărilor de protecție a datelor ar trebui să fie menționată clar în politica de confidențialitate. Ar trebui să fie indicată într-o secțiune, în care utilizatorii se pot aștepta să o găsească, cum ar fi o secțiune despre identitatea operatorului de date, o secțiune legată de drepturi sau o secțiune cu date de contact.

Contactarea autorității de supraveghere: Menționarea identității specifice a autorității de supraveghere și includerea unui link către site-ul său web sau pagina web specifică legată de depunerea unei plângeri. Aceste informații ar trebui să fie indicate într-o secțiune, în care utilizatorii se pot aștepta să le găsească, cum ar fi o secțiune legată de drepturi.

Prezentarea generală a politicii de confidențialitate: La începutul / în partea de sus a politicii de confidențialitate, includeți un cuprins (retractabil) cu titluri și subtitluri, care arată diferite pasaje pe care le conține notificarea de confidențialitate. Denumirile pasajelor individuale conduc în mod clar utilizatorii la conținutul exact și le permit să identifice rapid și să ajungă în secțiunea pe care o caută.

Identificarea modificărilor și compararea: În cazul introducerii modificărilor în notificarea de confidențialitate, faceți accesibile versiunile anterioare cu data lansării și evidențiați modificările.

Formulări coerente: Pe site-ul web aceeași formulare și definiție este utilizată pentru aceeași protecție a datelor. Formularea folosită în politica de confidențialitate ar trebui să se potrivească cu cea folosită pe restul platformei.

Prezentarea definițiilor: Atunci când utilizați cuvinte sau jargon nefamiliare sau tehnice, prezentarea unei definiții într-un limbaj simplu va ajuta utilizatorii să înțeleagă informațiile, care le sunt prezentate. Definiția poate fi inclusă direct în text și apărea atunci când utilizatorii trec cu mouse-ul peste cuvânt, sau poate fi inclusă într-un glosar.

Elemente contrastante de protecție a datelor: Evidențierea vizuală a elementelor sau a acțiunilor legate de protecția datelor într-o interfață, care nu este dedicată direct subiectului. De exemplu, atunci când postați pe platformă un mesaj public, controalele asupra asocierii geolocalizării ar trebui să fie disponibile în mod direct și ar trebui să fie clar vizibile.

Integrarea protecției datelor: Imediat după crearea unui cont, includeți puncte de protecție a datelor în experiența de integrare a furnizorului platformei de comunicare socială pentru ca utilizatorii să-și determine și să-și seteze cu ușurință preferințele. De exemplu, aceasta se poate efectua invitându-i să-și seteze preferințele de protecție a datelor după ce și-au adăugat primul prieten sau după ce au distribuit prima postare.

Utilizarea exemplelor: În afară de informațiile obligatorii, care specifică clar și precis scopul prelucrării, exemple pot fi folosite pentru a prezenta o anumită prelucrare a datelor pentru ca utilizatorii să înțeleagă mai bine.

Informații contextuale: În afară de o politică de confidențialitate exhaustivă, prezentați fragmente succinte de informații la momentul cel mai potrivit pentru ca utilizatorul să aibă o informație specifică și continuă despre modul în care sunt prelucrate datele sale.

3.2 Informarea continuă pe platforma de comunicare socială

Cazul de utilizare 2a: O notificare de confidențialitate stratificată

a. **Descrierea contextului**

66. După cum s-a menționat deja în Orientările privind transparența, principiul transparenței este foarte strâns legat de principiul prelucrării echitabile a datelor cu caracter personal.[40] Cu toate acestea, informațiile despre prelucrarea datelor cu caracter personal îi fac pe operatorii de date să reflecteze asupra propriilor acțiuni, fac prelucrarea datelor mai ușor de înțeles pentru persoanele vizate și, în cele din urmă, abilitează persoanele vizate să aibă control asupra datelor lor, în special prin exercitarea drepturilor lor. Egalizarea abilităților persoanelor implicate care rezultă, generează un sistem echitabil de prelucrare a datelor cu caracter personal. Cu toate acestea, mai multe informații nu înseamnă neapărat informații mai bune. Prea multe informații irelevante sau confuze pot ascunde pasaje importante din conținut sau pot reduce probabilitatea de a le găsi. Prin urmare, echilibrul corect între conținut și prezentarea clară este crucial în acest sens. În lipsa acestui echilibru, pot apărea modele de interfață înșelătoare.

b. **Prevederi legale relevante**

67. Relațiile menționate devin clare pe baza articolului 5 din RGPD. Transparența și corectitudinea sunt deja menționate sistematic una alături de alta la articolul 5 alineatul (1) litera (a) din RGPD, deoarece o componentă o determină pe cealaltă. Faptul că trebuie să existe nu doar transparență externă, ci și internă este prevăzut și de cerința de răspundere prevăzută la articolul 5 alineatul (2) din RGPD. Cea mai importantă parte a transparenței interne este cerința de a păstra evidența activităților de prelucrare în conformitate cu articolul 30 din RGPD. Pentru a asigura transparența externă, în afară de alte mijloace de informare furnizorii platformelor de comunicare socială pot oferi utilizatorilor și o notificare de confidențialitate stratificată.[41] Această necesitate de claritate și procesare echitabilă este corelată cu cerințele articolului 12 alineatul (1) din RGPD, conform cărora orice informații menționate la articolele 13 și 14 din RGPD trebuie acordate într-o formă concisă, transparentă, inteligibilă, ușor accesibilă și într-un limbaj simplu. Astfel, conținutul informațional trebuie să fie accesibil fără obstacole. Dacă cerințele articolului 12 din RGPD nu sunt îndeplinite, nu există informații valabile în sensul articolelor 13 și 14 din RGPD. Astfel, pentru a asigura un control eficient, operatorii și persoanele împuternicite de operatori pot fi trași/trase la răspundere, ceea ce duce la aplicarea cerințelor RGPD în practică.

c. Modele de interfață înșelătoare

i. Modele bazate pe conținut

68. În ceea ce privește acest caz de utilizare, limitele modelelor bazate pe conținut sunt prevăzute la articolul 12 alineatul (1) din RGPD, conform căruia informațiile acordate trebuie să aibă o formă precisă și inteligibilă, precum și un limbaj clar și simplu.

Lăsată în întuneric - Informații conflictuale (Lista de verificare 4.6.2 din Anexa I)

69. Unul dintre cele mai evidente cazuri, în care aceasta se poate întâmpla, este prezentarea ***Informațiilor conflictuale***, motiv pentru care utilizatorii nu sunt siguri cu privire la ceea ce ar trebui să facă și la consecințele acțiunilor lor, prin urmare, nu stabilesc nicio setare sau păstrează setările implicite.

Partajarea informațiilor dvs.

[40] Orientările privind transparența, p. 4-5.

[41] A se vedea cazul de utilizare 2a din secțiunea 3.2 de mai jos.

Pe platforma noastră puteți **partaja totul și orice**! Cu cât mai mult împărtășești, cu atât **mai interesantă** va fi **experiența** dvs. ! În orice moment puteți seta preferința dvs. privind vizibilitatea informațiilor, pe care le distribuiți pe platforma noastră.
De exemplu, puteți decide dacă doriți să Vă **împărtășiți geolicalizarea** sau cine va putea citi postările dvs.
Dacă **modificați publicitatea informațiilor dvs.** după ce acestea sunt postate online, veți pierde vizibilitatea și este posibil ca unele persoane să nu le mai poată vedea.

Exemplul 12: În acest exemplu, informațiile legate de partajarea datelor oferă o perspectivă extrem de pozitivă asupra procesării, evidențiind beneficiile partajării cât mai multor date posibil. Împreună cu imaginea unui animal drăguț, care se joacă cu o minge, această ***Dirijare emoțională*** poate oferi utilizatorilor iluzia de siguranță și confort în ceea ce privește riscurile posibile ale partajării un fel de informații pe platformă. Pe de altă parte, informațiile oferite cu privire la modul de control al publicității datelor cuiva nu sunt clare. În primul rând, se spune că utilizatorii își pot seta preferințele de partajare oricând doresc. Însă ultima propoziție sugerează faptul că aceasta nu este posibil dacă ceva a fost deja postat pe platformă. Din cauza acestor ***Informații conflictuale,*** utilizatorii nu sunt siguri cum își pot controla publicitatea datelor lor.

Schimbător - Lipsa ierarhiei (Lista de verificare 4.5.1 din Anexa I)
71. Efecte similare ca și în cazul ***Informațiilor conflictuale*** și al ***Dirijării emoționale*** pot apărea dacă prezentarea informațiilor nu corespunde unui sistem intern sau unei ierarhii. ***Lipsă de ierarhie*** în informațiile legate de protecția datelor există atunci, când aceste informații apar de mai multe ori și sunt prezentate în mai multe moduri diferite. Utilizatorii ar putea fi confuzi de repetarea lor și ar putea să nu înțeleagă pe deplin cum sunt prelucrate datele lor și cum să exercite controlul asupra acestora. Din cauza unei astfel de arhitecturi, informațiile sunt greu de înțeles, deoarece imaginea completă nu este ușor accesibilă. În cazuri, precum cel descris în exemplul următor, sunt încălcate cerințele de inteligibilitate și ușurință de acces prevăzute de articolul 12 alineatul (1) din RGPD.

Exemplul 13: Informațiile referitoare la drepturile persoanelor vizate sunt indicate în notificarea de confidențialitate. Deși diferite drepturi ale persoanelor vizate sunt explicate în secțiunea *„Opțiunile tale”*, dreptul de a depune o reclamație și adresa exactă de contact sunt menționate doar după mai multe secțiuni și straturi, care se referă la diferite subiecte. Prin urmare, în notificarea de confidențialitate parțial sunt omise date de contact, care apar la etapele, la care specificarea lor ar fi de dorit și recomandabilă.

72. ***Lipsa ierarhiei*** poate apărea și atunci când informațiile date sunt structurate într-un mod, care complică orientarea utilizatorilor, astfel cum este prezentat în următorul exemplu.

Exemplul 14: Politica de confidențialitate nu este divizată în diferite secțiuni cu titluri și conținut. Aceasta are peste 70 de pagini. Totuși, nu există un meniu de navigare în partea laterală sau de sus pentru ca utilizatorii să acceseze cu ușurință secțiunea pe care o caută. Explicația termenului auto-creat *„date de creare”* se conține într-o notă de subsol la pagina 67.

Lăsată în întuneric - Formulare sau informații ambigue (Lista de verificare 4.6.3 din Anexa I)
73. Chiar dacă alegerea cuvintelor nu este în mod evident contradictorie, pot apărea probleme legate de utilizarea unor termeni ambigui și vagi în informațiile oferite utilizatorilor. Cu astfel de informații, utilizatorii ar putea să nu fie siguri de modul în care vor fi procesate datele sau cum

pot controla datele într-o oarecare măsură. Dacă utilizatorii medii nu vor înțelege mesajul autentic al informațiilor fără cunoștințe speciale, condițiile articolului 12 alineatul (1) din RGPD nu vor fi îndeplinite. Utilizarea unei ***Formulări sau informații ambigue*** poate contrazice principiul echității prevăzut la articolul 5 alineatul (1) litera (a) din RGPD, deoarece informațiile nu pot fi considerate transparente, motiv pentru care persoanele vizate nu pot să înțeleagă prelucrarea datelor lor cu caracter personal și să își exercite drepturile.

Exemplul 15: O notificare de confidențialitate descrie o parte a unei prelucrări într-un mod vag și imprecis, ca în această propoziție: *„Datele dvs. ar putea fi folosite pentru a ne îmbunătăți serviciile".* De asemenea, dreptul de acces la datele cu caracter personal este aplicabil prelucrării conform articolului 15 alineatul (1) din RGPD, dar este menționat astfel, încât utilizatorilor să nu fie clar ce le permite să acceseze: *„Puteți vedea o parte din informațiile dvs. din contul dvs. examinând ceea ce ați postat pe platformă".*

74. În exemplu, utilizarea timpului condiționat *(„ar putea")* le creează utilizatorilor sentimentul de nesiguranță cu privire la faptul, dacă datele lor vor fi utilizate pentru prelucrare sau nu. Termenul *„servicii"* ar putea fi prea general pentru a fi calificat drept „clar". În afară de aceasta, nu este clar modul în care vor fi prelucrate datele pentru îmbunătățirea serviciilor. CEPD reamintește că utilizarea timpului condiționat sau a unei formulări vagi nu constituie „un limbaj clar și simplu", după cum prevede articolul 12 alineatul (1) fraza 1 din RGPD, și poate fi utilizat numai dacă operatorii pot demonstra că echitatea prelucrării nu este astfel subminată.[42]

Schimbător – Discontinuitatea limbajului (Lista de verificare 4.5.4 din Anexa I)

75. Atunci când serviciile online sunt oferite și adresate rezidenților anumitor state membre, notificările privind protecția datelor ar trebui, de asemenea, oferite în aceste limbi.[43] În acest context, este important ca alegerea unei anumite limbi să poată fi schimbată și manual și să fie implementată continuu, fără întreruperi. În cazul în care aceste criterii nu sunt îndeplinite, persoanele vizate se confruntă cu o ***Discontinuitate a limbajului***, motiv pentru care nu pot înțelege informațiile legate de protecția datelor. Utilizatorii se vor confrunta cu acest model de interfață înșelătoare atunci când informațiile privind protecția datelor nu sunt prezentate în limbile oficiale ale țării în care locuiesc, în timp ce serviciul este prestat în limba respectivă. Dacă utilizatorii nu cunosc limba în care sunt prezentate informațiile privind protecția datelor, nu o vor putea citi cu ușurință și, prin urmare, nu vor cunoaște cum sunt prelucrate datele lor cu caracter personal. Este important de menționat că ***Discontinuitatea limbajului*** poate deruta utilizatorii și poate crea un mediu de setări pe care nu înțeleg cum să-l folosească. Acest model de interfață înșelătoare poate apărea în diferite moduri, așa cum va fi prezentat în aceste Orientări.

Exemplul 16:

Varianta A: Platforma de comunicare socială este disponibilă în croată ca limbă aleasă de utilizatori (sau în spaniolă ca limbă a țării în care se află), în timp ce toate sau anumite informații despre protecția datelor sunt disponibile doar în limba engleză.

Varianta B: De fiecare dată când utilizatorii apelează anumite pagini, cum ar fi pagina de ajutor, acestea trec automat la limba țării în care se află utilizatorii, chiar dacă au selectat anterior o altă limbă.

[42] A se vedea Orientările privind transparența, p. 12, inclusiv „Exemplele de practici greșită", și p. 13.
[43] A se vedea Orientările privind transparența, p. 13 și nota de subsol 15.

76. Varianta A prezintă cazul, în care nu sunt disponibile informații într-o limbă aparent vorbită de persoana vizată. Aceasta înseamnă că nu pot citi informațiile și, prin urmare, nu pot înțelege cum sunt prelucrate datele lor cu caracter personal. Informațiile nu pot fi considerate inteligibile conform articolului 12 alineatul (1) din RGPD. Din cauza lipsei de informații cu privire la protecția datelor într-o limbă ușor de înțeles, informațiile solicitate în temeiul articolului 13, respectiv 14 din RGPD nu pot fi considerate prezentate persoanelor vizate.

77. Varianta B descrie un caz, în care paginile cu informații privind protecția datelor sunt prezentate în mod implicit în limba țării de reședință a utilizatorilor, în pofida alegerii clare a limbii. Aceasta înseamnă că utilizatorii trebuie să-și reseteze preferința de limbă de fiecare dată când accesează o pagină cu informații privind protecția datelor. Aceasta poate fi considerată o practică neloială față de persoanele vizate și ar putea duce la încălcarea principiului echității prevăzut la articolul 5 alineatul (1) litera (a) din RGPD.

ii. Modele bazate pe interfață

78. În unele cazuri, furnizorii platformelor de comunicare socială folosesc anumite practici pentru a-și prezenta setările de protecție a datelor. În procesul de înregistrare, utilizatorilor li se oferă o mulțime de informații și diferite setări legate de protecția datelor. Pentru ca utilizatorii să-și poată găsi calea către aceste setări și să poată face modificări în orice moment când se utilizează platforma, setările ar trebui să fie ușor accesibile și asociate cu informații relevante pentru ca utilizatorii să ia o decizie în cunoștință de cauză. Elementul „ușor accesibil" înseamnă că persoanele vizate nu ar trebui să caute informațiile. În ceea ce privește politicile de confidențialitate, Grupul de lucru prevăzut la articolul 29 a declarat deja că poziționarea sau schemele de culori, care fac un text sau un link mai puțin vizibil sau greu de găsit pe o pagină web, nu sunt considerate ușor accesibile.[44]

Supraîncărcarea – Labirint de confidențialitate (Lista de verificare 4.1.2 din Anexa I)

79. În conformitate cu Orientările privind transparența, notificarea de confidențialitate ar trebui să fie ușor accesibilă, adică printr-un singur clic pe site-uri web.[45] Utilizarea metodei abordării stratificate poate facilita prezentarea mai clară a notificării de confidențialitate în sensul articolului 12 alineatul (1) din RGPD.[46] Totuși, aceasta nu ar trebui să complice inutil exercitarea funcțiilor sau drepturilor importante prin prezentarea unei politici de confidențialitate complexe, care constă din nenumărate straturi, care ar duce la modelul de interfață înșelătoare ***Labirint de confidențialitate***. Acest model corespunde unui control al informațiilor sau al protecției datelor, care este deosebit de dificil de găsit, deoarece utilizatorii trebuie să navigheze prin multe pagini fără a avea o imagine de ansamblu cuprinzătoare și exhaustivă. Astfel utilizatorii ar putea trece cu vederea informațiile/setarea relevante sau renunța să le caute. Structura stratificată trebuie să faciliteze lizibilitatea și să ofere informații cu privire la modul de exercitare a drepturilor persoanelor vizate, și să nu le complice. Este foarte important ca utilizatorii să poată urma cu ușurință explicațiile.

80. În această privință, ceea ce este cel mai bine pentru utilizatori nu este o abordare universală și depinde de multe criterii, cum ar fi tipul de utilizatori pe platformă sau tipul general de proiect al aplicației. Dacă este posibil, testarea abordării stratificate implementată cu utilizatorii pentru a obține feedback-ul lor ar trebui efectuată pentru a evalua eficacitatea acesteia. Din acest motiv, nu poate fi cuantificat niciun număr concret pentru numărul maxim de straturi de informații

[44] Orientările privind transparența, p. 11.
[45] A se vedea Orientările privind transparența, exemplu la p. 11.
[46] Pentru detalii cu privire la abordarea stratificată într-un mediu digital, a se vedea Orientările privind transparența, p. 35-37.

admise. Prin urmare, trebuie să se stabilească întotdeauna de la caz la caz dacă sunt utilizate prea multe straturi și astfel apar modele de interfață înșelătoare. Cu toate acestea, cu cât mai mare este numărul, cu atât se poate presupune că utilizatorii vor fi descurajați sau induși în eroare. Un număr mare de straturi va fi adecvat doar în cazuri individuale speciale, în care nu este ușor de plasat informații complexe în mod cuprinzător. În același timp, abordarea stratificată nu poate fi folosită greșit pentru a ascunde informații în straturi mai profunde sau adăugând straturi inutile.

81. Cu toate acestea, acest lucru trebuie apreciat diferit atunci când este vorba de exercitarea drepturilor utilizatorilor. Conform RGPD, exercitarea acestor drepturi trebuie să fie asigurată întotdeauna. Acest cadru determină prezentarea informațiilor privind funcțiile conexe și exercitarea drepturilor. Atunci când utilizatorii doresc să-și exercite drepturile, numărul de pași ar trebui să fie cât mai mic posibil. Ca urmare, utilizatorii ar trebui să ajungă la funcția, care le permite să își exercite drepturile cât mai direct posibil. În cele mai multe cazuri, necesitatea de a naviga printr-un număr mare de straturi de informații înainte ca utilizatorii să-și poată exercita efectiv drepturile prin intermediul funcțiilor i-ar putea descuraja să-și exercite aceste drepturi. Dacă sunt implementați un număr mare de pași, furnizorul platformei de comunicare socială ar trebui să poată demonstra beneficiile respective pentru utilizatori ca persoane vizate în conformitate cu RGPD. Pe lângă explicația drepturilor persoanelor vizate în notificarea de confidențialitate, astfel cum este prevăzut la articolul 13 alineatul (2) literele (b), (c) și (d) din RGPD, exercitarea drepturilor ar trebui, de asemenea, să fie accesibilă independent de aceste informații. De exemplu, utilizatorii ar trebui să poată exercita drepturile persoanelor vizate și prin meniul platformei.

Exemplul 17: Pe platforma sa, furnizorul platformei de comunicare socială pune la dispoziție un document numit *„sfaturi utile”*, care conține și informații importante despre exercitarea drepturilor persoanelor vizate. Cu toate acestea, politica de confidențialitate nu conține niciun link sau un alt indiciu către acest document. În schimb, în aceasta se menţionează că mai multe detalii sunt disponibile în secțiunea „Întrebări și răspunsuri” a site-ului web. Prin urmare, utilizatorii care așteaptă să găsească informații despre drepturile lor în politica de confidențialitate nu vor găsi aceste explicații acolo și vor fi nevoiți să navigheze mai departe și să caute prin secțiunea „Întrebări și răspunsuri”.

82. Acest exemplu prezintă clar un model de ***Labirint de confidențialitate,*** care complică găsirea informațiilor suplimentare decât ar trebui cu privire la drepturile persoanelor vizate și, în special, cu privire la modul de exercitare a acestora, ceea ce este contrar articolului 12 alineatul (2) din RGPD. De asemenea, dacă politica de confidențialitate este incompletă, aceasta încalcă și articolul 13 alineatul (2) literele (b), (c) și (d), respectiv articolul 14 alineatul (2) literele (c), (d) și (e) din RGPD. Într-adevăr, în timp ce informații mai detaliate sau modalitatea directă de exercitare a drepturilor ar putea fi la un clic distanță de locul în care sunt menționate în politica de confidențialitate, utilizatorii din exemplu vor trebui să navigheze la secțiunea „Întrebări și răspunsuri” și să o caute pentru a găsi documentul de *„sfaturi utile”.*

83. Este important de reținut că efectele și mai puternice decât cele cauzate de prea multe straturi[47] pot apărea atunci când sunt utilizate nu doar mai multe dispozitive, ci și mai multe aplicații acordate de aceeași platformă de comunicare socială, cum ar fi aplicații speciale de mesagerie. Utilizatorii, care folosesc acest tip de aplicație secundară, s-ar confrunta cu obstacole și eforturi mai mari dacă ar trebui să apeleze la versiunea de browser sau aplicația principală

[47] A se vedea mai sus, p. 81 și 82.

pentru a obține informații legate de protecția datelor. Într-o astfel de situație, care nu este legată doar de dispozitive, ci și de aplicații, informațiile relevante trebuie să fie întotdeauna direct accesibile, indiferent de modul în care utilizatorii folosesc platforma.

Obstrucționarea - Fundătura (Lista de verificare 4.4.1 din Anexa I)

84. Cerințele legale pot fi încălcate și atunci când informațiile privind protecția datelor cerute de RGPD sunt puse la dispoziție prin acțiuni suplimentare, cum ar fi clic pe un link sau pe un buton. În special, navigarea greșită sau interfața incoerentă, care duce la caracteristici ineficiente, nu pot fi clasificate ca fiind corecte în temeiul articolului 5 alineatul (1) litera (a) din RGPD, deoarece utilizatorii sunt induși în eroare atunci când încearcă fie să ajungă la anumite informații, fie își setează preferințele privind protecția datelor. Prin urmare, ***Fundăturile***, în care utilizatorii sunt lăsați singuri fără funcții pentru a-și exercita drepturile, ar trebui evitate în orice caz și încalcă direct prevederile articolului 12 alineatul (2) din RGPD, conform cărora operatorul trebuie să faciliteze exercitarea drepturilor.

Exemplul 18: În politica sa de confidențialitate, un furnizor de platformă de comunicare socială oferă multe hyperlinkuri către pagini cu informații suplimentare despre anumite subiecte. Cu toate acestea, politica de confidențialitate conține mai multe părți doar cu declarații generale că este posibil să accesați mai multe informații, fără a specifica unde sau cum.

85. În general, politica de confidențialitate este privită ca documentul, care centralizează toate informațiile referitoare la protecția datelor, în conformitate cu obligațiile prevăzute la articolele 12, 13 și 14 din RGPD. Prin urmare, trebuie asigurată și redirecționarea către toate locurile relevante de pe platforma de comunicare socială pentru ca utilizatorii să își controleze datele sau să își exercite drepturile. În exemplul 18 de mai sus, acest lucru este implementat doar parțial, deoarece sunt furnizate linkuri către informații suplimentare pentru unele elemente, dar nu și pentru altele. Pentru aceștia, modelul ***Fundătură*** poate duce la o încălcare a articolului 12 alineatul (1) din RGPD, complicând accesul la unele informații de protecție a datelor sau la articolul 12 alineatul (2) din RGPD, prin nefacilitarea exercitării drepturilor.

d. **Cele mai bune practici**

Navigare lipicioasă: În timpul consultării unei pagini legate de protecția datelor, cuprinsul poate fi afișat în mod constant pe ecran, permițând utilizatorilor să fie mereu pe pagină și să navigheze rapid în conținut datorită linkurilor de ancorare.

Înapoi sus: Includeți un buton de revenire în sus în partea de jos a paginii sau ca element lipicios în partea de jos a ferestrei pentru a facilita navigarea utilizatorilor pe o pagină.

Comenzi rapide: găsiți definiția în cazul de utilizare 1 (p. 22) *(de exemplu, în politica de confidențialitate, includeți pentru fiecare informație despre protecția datelor linkuri care redirecționează direct către paginile aferente de protecție a datelor de pe platforma de comunicare socială).*

Informații de contact: găsiți definiția în cazul de utilizare 1 (p. 22).

Contactarea autorității de supraveghere: găsiți definiția în cazul de utilizare 1 (p. 22).

Prezentarea generală a politicii de confidențialitate: găsiți definiția în cazul de utilizare 1 (p. 22).

Identificarea modificărilor și compararea: găsiți definiția în cazul de utilizare 1 (p. 22).

Formulări coerente: găsiți definiția în cazul de utilizare 1 (p. 22).

Prezentarea definițiilor: găsiți definiția în cazul de utilizare 1 (p. 22).

Utilizarea exemplelor: găsiți definiția în cazul de utilizare 1 (p. 22).

Cazul de utilizare 2b: Prezentarea informațiilor persoanei vizate despre controlul comun, articolul 26 alineatul (2) din RGPD

a. Descrierea contextului și a prevederilor legale relevante

86. A doua frază a articolului 26 alineatul (2) din RGPD conține prevederi suplimentare privind transparența în cazul specific de control comun.[48] Acestea asigură accesibilitatea esenței acordului de control comun persoanelor vizate.[49] În Orientările sale 07/2020 privind noțiunile de operator și persoană împuternicită de operator din RGPD, CEPD recomandă ca esența să acopere cel puțin toate elementele informațiilor menționate la articolele 13 și 14 din RGPD, care deja ar trebui să fie accesibile persoanelor vizate și să specifice pentru fiecare element care operator comun este responsabil pentru asigurarea respectării acestora.[50] În esența acordului trebuie să fie indicată și persoana de contact, dacă este desemnată. Operatorii comuni trebuie să stabilească cea mai eficientă modalitate de a pune la dispoziția persoanelor vizate esența acordului.[51]

b. Modele de interfață înșelătoare

Exemplul 19: În ceea ce privește modelele de interfață înșelătoare, provocarea pentru operatori din această constelație este de a integra aceste informații în sistemul online astfel încât să poată fi percepute cu ușurință și să nu-și piardă claritatea și inteligibilitatea, chiar dacă articolul 12 alineatul (1) fraza 1 din RGPD nu se referă direct la articolul 26 alineatul (2) fraza 2 din RGPD.
Cu toate acestea, date fiind principiile de protecție a datelor de corectitudine, transparență și responsabilitate prevăzute la articolul 5 alineatul (1) litera (a) și alineatul (2) din RGPD, cerințe comparabile derivă și în cazul controlului comun. Atunci când operatorii comuni oferă informații despre esența acordului într-o notificare de confidențialitate, aceasta trebuie, de asemenea, să fie clară și transparentă. Prin urmare, prelucrarea nu mai poate fi evaluată ca fiind echitabilă, dacă informațiile despre aceasta sunt greu de înțeles, deoarece nu sunt linkuri sau informațiile sunt prezentate în mai multe locuri. Modelul de interfață înșelătoare ***Labirint de confidențialitate***[52] ar putea fi și mai confuz decât, în general, o notificare de confidențialitate, deoarece utilizatorii se pot aștepta ca informațiile conform articolului 26 alineatul (2) fraza 2 din RGPD să fie prezentate într-un singur loc. Un furnizor de platformă de comunicare socială se referă întotdeauna la *„date de creare”* în cadrul politicii de confidențialitate și nu folosește termenul „date cu caracter personal”. Doar la pagina 90, notificarea de confidențialitate stratificată conține explicația că *„datele de creare ar putea conține date cu caracter personal ale utilizatorilor”*. În acordul operatorilor comuni prezentat persoanelor vizate se folosește și termenul „date de creare” fără explicație. Celălalt operator comun (B) are o definiție a datelor cu caracter personal în politica sa de confidențialitate proprie. Cu toate acestea, în secțiunea din

[48] Găsiți definiția controlului comun în articolul 4 alineatul (7) și în articolul 26 alineatul (1) fraza 1 din RGPD, precum și Orientările 07/2020 ale CEPD privind noțiunile de operator și persoană împuternicită de operator în RGPD, adoptate la 7 iulie 2021, versiunea 2.1, p. 46-49, disponibile la https://edpb.europa.eu/system/files/2021-07/eppb guidelines 202007 controllerprocessor final en.pdf.
[49] A se vedea Orientările 07/2020 ale CEPD privind noțiunile de operator și persoană împuternicită de operator, p. 179.
[50] A se vedea Orientările 07/2020 ale CEPD privind noțiunile de operator și persoană împuternicită de operator, p. 180, de asemenea pentru fraza următoare.
[51] A se vedea Orientările 07/2020 ale CEPD privind noțiunile de operator și persoană împuternicită de operator, p. 181.
[52] A se vedea mai sus, cazul de utilizare 2a, exemplul 17 din aceste Orientări.

politica sa de confidențialitate despre controlul comun cu furnizorul platformei de comunicare socială, operatorul B oferă doar un link către acordul prezentat de furnizorul platformei de comunicare socială, fără alte explicații.

87. Explicațiile conform articolului 26 alineatul (2) fraza 2 din RGPD sunt mai complicat de înțeles atunci când nu mai sunt coerente. Această incoerență este amplificată atunci, când platformele de comunicare socială folosesc terminologie creată independent, pe care de obicei utilizatorii nu o asociază cu prelucrarea datelor cu caracter personal, astfel cum este prezentat în exemplul 19 de mai sus. În acest exemplu, ambii operatori comuni încalcă articolul 26 alineatul (2) fraza (2) din RGPD, precum și articolul 5 alineatul (1) litera (a) din RGPD, deoarece informațiile acordate cu privire la controlul comun nu sunt clare și, prin urmare, nu sunt transparente pentru persoanele vizate.

Cazul de utilizare 2c: Informarea persoanei vizate despre o încălcare a securității datelor cu caracter personal

a. Descrierea contextului și a prevederilor legale relevante

88. Pentru a putea identifica și aborda o încălcare a securității datelor cu caracter personal, un operator trebuie să fie capabil să o recunoască.[53] Conform articolului 4 alineatul (12) din RGPD, „încălcarea securității datelor cu caracter personal" înseamnă „o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod". Când vine vorba despre operatorii platformelor de comunicare socială, încălcările securității datelor cu caracter personal se pot produce în mai multe moduri. De exemplu, un atacator reușește să acceseze datele cu caracter personal și mesajele de chat ale utilizatorilor, sau, din cauza unei erori de programare, o aplicație ar putea accesa date cu caracter personal în afara domeniului de aplicare a permisiunilor acordate de utilizatori. Un alt exemplu ar fi cazul în care utilizatorii partajează poze prin setarea „partajează cu cei mai buni prieteni ai mei", dar pozele lor devin accesibile diferitor persoane. Ca ultim exemplu, din cauza unei erori o platformă de comunicare socială bazată pe înregistrări video în timp real poate partaja conținut în flux, în pofida faptului că utilizatorii au apăsat anterior un buton pentru a opri înregistrarea.

89. În cazul unei încălcări a securității datelor cu caracter personal, un operator trebuie neapărat să notifice autoritatea de supraveghere competentă în conformitate cu articolul 33 din RGPD, cu excepția cazului în care este puțin probabil ca încălcarea dată să genereze un risc pentru drepturile și libertățile persoanelor fizice. Dacă există probabilitatea ca o astfel de încălcare să genereze un risc înalt pentru drepturile și libertățile persoanelor fizice, operatorul va informa, în general, despre încălcare persoanele vizate conform articolului 34 alineatele (1) și (2) din RGPD. În acest caz, operatorul trebuie să informeze persoanele vizate fără întârzieri nejustificate. Aceste informații trebuie să descrie într-un limbaj clar și simplu tipul încălcării securității datelor cu caracter personal, deoarece se aplică și articolul 12 din RGPD. De asemenea, aceste informații trebuie să conțină cel puțin date și măsuri precum (a se vedea și articolul 33 alineatul (3) literele (b)-(d) coroborat cu articolul 34 alineatul (2) din RGPD):

- numele și datele de contact ale responsabilului cu protecția datelor (RPD), dacă este cazul, sau ale unei alte persoane de contact, de la care se pot obține mai multe informații;

[53] A se vedea, de asemenea, Orientările 01/2021 ale CEPD referitoare la exemple de notificare privind încălcarea securității datelor cu caracter personal, adoptate la 14 decembrie 2021, versiunea 2.0, p. 4, disponibile la https://edpb.europa.eu/system/files/2022-01/edpb guidelines 012021 pdbnotification adopted en.pdf.

- o descriere a consecințelor probabile ale încălcării securității datelor cu caracter personal; și
- o descriere a măsurilor luate sau propuse să fie luate de către operator pentru a aborda încălcarea, inclusiv, după caz, măsuri de atenuare a posibilelor efecte adverse ale acesteia.[54]

90. Astfel de comunicări privind încălcarea securității datelor cu caracter personal în conformitate cu articolul 34 din RGPD pot conține și modele de interfață înșelătoare. De exemplu, dacă operatorul respectiv prezintă persoanelor vizate toate informațiile necesare pentru a le informa despre gradul încălcării respective, însă le oferă și informații nespecifice și irelevante, precum și implicațiile și măsurile de precauție pe care operatorul le-a luat sau sugerează să le ia. Aceste informații parțial irelevante pot induce în eroare, iar utilizatorii afectați de încălcare ar putea să nu înțeleagă pe deplin implicațiile încălcării sau să subestimeze efectele (posibile).

b. Modele de interfață înșelătoare

91. Mai jos sunt prezentate câteva exemple negative, practici greșite de notificare a încălcării securității datelor cu caracter personal, prin care este încălcat articolul 34 din RGPD coroborat cu articolul 12 din RGPD, ar putea apărea:

i. Modele bazate pe conținut

Lăsată în întuneric - Informații conflictuale (Lista de verificare 4.6.2 din Anexa I)

Exemplul 20:
• Operatorul se referă doar la acțiunile unui terț, afirmând că încălcarea securității datelor cu caracter personal a fost provocată de un terț (de exemplu, o persoană împuternicită de operator) și că, prin urmare, nu a avut loc nicio încălcare a securității. Operatorul evidențiază, de asemenea, unele bune practici, care nu au nicio legătură cu încălcarea reală.
• Operatorul determină gravitatea încălcării securității datelor cu caracter personal în raport cu el însuși sau cu o persoană împuternicită de operator, mai degrabă decât în raport cu persoana vizată.

Lăsată în întuneric - Formulare sau informații ambigue (Lista de verificare 4.6.3 din Anexa I)

92. În ceea ce privește limba, în care persoana vizată este informată despre încălcare, este esențial ca operatorii să aibă în vedere faptul că majoritatea destinatarilor nu vor fi obișnuiți cu limbajul specific, posibil tehnic sau juridic legat de protecția datelor.

Exemplul 21: Printr-o încălcare a securității datelor cu caracter personal pe o platformă de comunicare socială, accidental mai multe seturi de date de sănătate au devenit accesibile utilizatorilor neautorizați. Furnizorul platformei de comunicare socială informează utilizatorii că accidental au fost făcute publice doar *„categorii speciale de date cu caracter personal”.*

93. Aceasta este o ***Formulare ambiguă***, deoarece utilizatorii medii nu înțeleg termenul *„categorii speciale de date cu caracter personal”* și, prin urmare, nu știu că datele lor de sănătate au fost scurse. Cauza constă în faptul că termenul „special” are un sens foarte diferit în limbajul general decât în limbajul specific legat de RGPD. Utilizatorii medii nu știu că, în conformitate cu articolul 9 alineatul (1) din RGPD, *„categorii speciale de date cu caracter personal”* se referă la date cu

[54] Articolul 29 din Orientările grupului de lucru privind notificarea încălcării securității datelor cu caracter personal, aprobate de CEPD, p. 20 https://ec.europa.eu/newsroom/article29/items/612052/en.

caracter personal, care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice. Astfel, în acest scenariu sintagma *„categorii speciale de date cu caracter personal"* constituie un model de interfață înșelătoare, deoarece induce în eroare utilizatorii din motiv că nu este însoțită de explicații suplimentare. Acesta este un exemplu de situație, în care un operator încearcă să informeze persoanele vizate despre încălcare, dar nu își îndeplinește complet obligația de a comunica încălcarea securității datelor cu caracter personal în conformitate cu articolul 34 din RGPD, deoarece gravitatea incidentului va fi subestimată de către cititorul mediu. Mai mult, informațiile succinte din exemplu nu sunt inteligibile, astfel cum prevede articolul 34 coroborat cu articolul 12 alineatul (1) fraza 1 din RGPD.

94. Un alt exemplu de ***Formulare ambiguă***:

Exemplul 22: Operatorul prezintă doar detalii vagi atunci când identifică categoriile de date cu caracter personal afectate, de exemplu operatorul se referă la documentele transmise de utilizatori fără a specifica ce categorii de date cu caracter personal conțin aceste documente și cât de sensibile au fost.

95. Este important de menționat faptul, că acest model de interfață înșelătoare poate apărea în toate părțile notificării privind încălcarea securității datelor cu caracter personal. Dacă cele două exemple menționate mai sus se referă la o formulare neclară despre categoriile de date afectate, următorul exemplu arată că categoria persoanelor vizate afectate ar putea fi la fel de neclară:

Exemplul 23: Informând despre încălcare, operatorul nu specifică suficient categoria persoanelor vizate, de exemplu, operatorul menționează doar că persoanele vizate au fost studenți, dar nu precizează dacă persoanele vizate sunt minori sau grupuri de persoane vulnerabile.

96. În cele din urmă, gravitatea incidentului poate fi, de asemenea, subestimată atunci când ***informațiile ambigue*** sunt prezentate similar exemplului de mai jos:

Exemplul 24: În notificarea despre încălcare adresată autorității de supraveghere și persoanei vizate, un operator afirmă că datele cu caracter personal au fost făcute publice prin alte surse . Prin urmare, persoana vizată consideră că securitatea nu a fost încălcată.

ii. Modele bazate pe interfață

97. Exemple negative de notificare a încălcării securității datelor cu caracter personal, contrar articolului 34 din RGPD, coroborat cu articolul 12 din RGPD, pot constitui, de asemenea, modele de interfață înșelătoare bazate pe interfață, după cum este prezentat mai jos:

Omiterea - Uită-te acolo (Lista de verificare 4.2.2 din Anexa I)

Exemplul 25:

• Operatorul informează prin texte, care conțin o mulțime de informații irelevante și omite detaliile relevante.

• În cazul încălcărilor de securitate, care afectează datele de acces și alte tipuri de date, operatorul declară că datele sunt criptate sau indexate, deși acest lucru este valabil doar pentru parole.

98. În acest caz, chiar dacă datele relevante figurează în comunicare, persoanele vizate ar putea să le omită din cauza supraîncărcării cu informații irelevante.

c. Cele mai bune practici

Notificări: Notificările pot fi folosite pentru a sensibiliza utilizatorii cu privire la aspectele, schimbarea sau riscurile legate de prelucrarea datelor cu caracter personal *(de exemplu, când a avut loc o încălcare a securității datelor cu caracter personal).* Aceste notificări pot fi transmise în mai multe moduri, cum ar fi prin mesaje primite, ferestre pop-in, bannere fixate în partea de sus a paginii web etc.

Explicarea consecințelor: Atunci când utilizatorii doresc să activeze sau să dezactiveze un control al protecției datelor sau să își exprime sau să își retragă consimțământul, informați-i într-un mod neutru despre consecințele unei astfel de acțiuni.

Comenzi rapide: găsiți definiția în cazul de utilizare 1 (p.22) *(de exemplu, oferiți utilizatorilor un link pentru a-și reseta parola).*

Formulări coerente: găsiți definiția în cazul de utilizare 1 (p. 22).

Prezentarea definițiilor: găsiți definiția în cazul de utilizare 1 (p. 22).

Utilizarea exemplelor: găsiți definiția în cazul de utilizare 1 (p. 22).

3.3 Protejarea continuă pe platforma de comunicare socială

Cazul de utilizare 3a: Gestionarea consimțământului în timpul utilizării unei platforme de comunicare socială

a. Descrierea contextului și a prevederilor legale relevante

99. Utilizatorii platformei de comunicare socială trebuie să-și dea consimțământul respectiv în timpul diferitelor părți ale activităților de prelucrare a datelor, de exemplu înainte de a primi publicitate personalizată. După cum s-a menționat deja în Orientările CEPD privind direcționarea pentru adresarea de conținut personalizat către utilizatorii platformelor de comunicare socială, consimțământul poate fi un temei legal corespunzător doar dacă persoanei vizate i se oferă control și o alegere reală.[55] De asemenea, conform articolului 4 alineatul (11) din RGPD, consimțământul trebuie să fie specific, informat și lipsit de ambiguitate.[56] Este important de menționat faptul că cerințele față de consimțământul valabil conform RGPD nu constituie o obligație suplimentară, ci sunt condiții prealabile pentru prelucrarea legală a datelor cu caracter personal ale utilizatorilor. De asemenea, în ceea ce privește marketingul online sau metodele de urmărire online, se aplică Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice). Cu toate acestea, condițiile prealabile față de consimțământul valabil conform Directivei asupra confidențialității și comunicațiilor electronice sunt identice cu prevederile referitoare la consimțământ din RGPD.[57]

[55] Orientările 08/2020 privind direcționarea utilizatorilor platformelor de comunicare socială, p. 51.
[56] A se vedea, de asemenea, p. 25-29 de mai sus.
[57] A se vedea articolul 2 litera (f) din Directiva 2002/58/CE, precum și Avizul 5/2019 al CEPD privind interacțiunea dintre Directiva privind viața privată și comunicațiile electronice și RGPD, în special în ceea ce privește competența, sarcinile și atribuțiile autorităților de protecție a datelor, adoptat la 12 martie 2019, p. 14, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_ro.

100. Având în vedere principiul răspunderii stabilit la articolul 5 alineatul (2) din RGPD, precum și necesitatea ca operatorul să poată demonstra că persoanele vizate și-au exprimat consimțământul cu prelucrarea datelor lor cu caracter personal în temeiul articolului 7 alineatul (1) din RGPD, este esențial ca furnizorul platformei de comunicare socială să poată demonstra că a obținut în mod corespunzător consimțământul utilizatorilor. Această condiție poate deveni o provocare de demonstrat, de exemplu, dacă utilizatorii ar trebui să-și exprime consimțământul acceptând cookie-uri. De asemenea, persoanele vizate ar putea să nu fie întotdeauna conștiente că își dau consimțământul în timp ce fac clic rapid pe un buton evidențiat sau pe opțiuni prestabilite. Cu toate acestea, după cum este prevăzut în articolul 7 alineatul (1) din RGPD, sarcina probei că utilizatorii și-au dat în mod liber consimțământul o are operatorul.

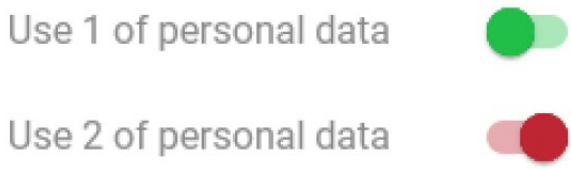
b. Modele de interfață înșelătoare

i. Modele bazate pe conținut

101. În afară de modelele bazate pe conținut deja explicate anterior, care s-ar putea aplica informațiilor legate de o solicitare de consimțământ,[58] mai pot fi găsite două modele de interfață înșelătoare bazate pe conținut în legătură cu consimțământul.

Informații conflictuale - Lăsată în întuneric (Lista de verificare 4.6.2 din Anexa I)

Exemplul 26: Interfața folosește un comutator pentru ca utilizatorii să-și dea sau să-și retragă consimțământul. Cu toate acestea, modul în care este proiectat comutatorul nu arată clar în ce poziție se află și dacă utilizatorii și-au exprimat sau nu consimțământul. Într-adevăr, poziția comutatorului nu se potrivește cu culoarea. Dacă comutatorul este situat în partea dreaptă, ceea ce este de obicei asociat cu activarea funcției („pornire”), culoarea comutatorului este roșie, ceea ce de obicei înseamnă că o funcție este dezactivată. În schimb, când comutatorul este situat în partea stângă, ceea ce de obicei înseamnă că funcția este dezactivată, culoarea de fundal a comutatorului este verde, care în mod normal se asociază cu o opțiune activă.



Utilizarea 1 a datelor cu caracter personal
Utilizarea 2 a datelor cu caracter personal

102. Dacă în procesul de obținere a consimțământului, sunt prezentate ***Informații conflictuale,*** informațiile sunt neclare și neinteligibile. Exemplul de mai sus prezintă un caz, în care informația vizuală este echivocă. Într-adevăr, întâlnind astfel de comutatori, utilizatorii nu vor fi siguri dacă și-au exprimat sau nu consimțământul. Atunci când semnificanții vizuali sunt amestecați în asemenea mod sau sunt prezentați în alte culori, care par contradictorii cu setarea reală (exemplul 26 conținând doar o prezentare a comutatorilor confuzi), consimțământul nu poate fi considerat ca fiind dat fără ambiguitate, în temeiul articolului 7 alineatul (2) din RGPD, coroborat cu articolul 4 alineatul (11) din RGPD. ***Informațiile conflictuale*** pot fi acordate și prin mijloace textuale, astfel cum este prezentat mai jos.

[58] A se vedea cazul de utilizare 1, p. 32-49 sau numerele de exemple UC1 enumerate în Anexă.

Exemplul 27: Furnizorul platformei de comunicare socială oferă utilizatorilor informații conflictuale: Deși informațiile afirmă mai întâi că datele de contact nu sunt importate fără consimțământ, în același timp într-o fereastră informațională pop-up se explică că oricum datele de contact vor fi importate.

Obstrucționarea - Acțiune înșelătoare (Lista de verificare 4.4.3 din Anexa I)

103. În afară de prezentarea ***Informațiilor conflictuale***, operatorii pot oferi informații, care induc în eroare utilizatorii, prin faptul că nu corespund așteptărilor acestora. ***Acțiune înșelătoare*** există atunci, când o diferență între informațiile și acțiunile disponibile utilizatorilor îi determină să facă ceva, ce nu intenționează să facă. Diferența dintre ceea ce utilizatorii așteaptă și ceea ce obțin ar putea să-i descurajeze să meargă mai departe.

Exemplul 28: Utilizatorii își răsfoiesc feed-ul rețelei de socializare. În acest timp, le sunt afișate anunțuri publicitare. Intrigați de un anunț și curioși de motivele pentru care le este afișat, aceștia fac clic pe semnul „?”din colțul din dreapta jos al anunțului. Se deschide o fereastră pop-in, în care se explică de ce văd anume acest anunț și listează criteriile de direcționare. De asemenea, utilizatorii sunt informați că își pot retrage consimțământul pentru afișarea anunțurilor publicitare vizate și apare un link pentru retragere. Când utilizatorii fac clic pe acest link, sunt redirecționați către un site absolut diferit, în care le sunt oferite explicații generale despre ce este consimțământul și cum să-l gestioneze.

104. În cazul prezentat mai sus este exemplificat un conținut, care nu corespunde așteptărilor utilizatorilor. Într-adevăr, atunci când utilizatorii fac clic pe link, aceștia s-ar aștepta să fie redirecționați către o pagină, care le permite să-și retragă consimțământul în mod direct. În schimb, pagina la care ajung nu le permite să o facă și nu precizează concret cum să-și retragă consimțământul pe platforma de comunicare socială. Această diferență între ceea ce utilizatorii ar trebui să găsească și ceea ce găsesc de fapt ar putea să-i deruteze și să-i lase nesiguri cum să procedeze. În cel mai rău caz, ar putea crede că nu își pot retrage consimțământul. O astfel de ***Acțiune înșelătoare*** nu poate fi considerată transparentă, astfel cum prevede articolul 12 alineatul (1) din RGPD. De asemenea, comparând retragerea cu modul în care este obținut consimțământul, această practică ar putea încălca articolul 7 alineatul (3) din RGPD, dacă retragerea consimțământului se dovedește a fi mai dificilă decât acordarea acestuia.

105. Atunci când furnizorii platformelor de comunicare socială informează utilizatorii că o acțiune din partea lor poate avea o anumită consecință și acțiunea duce de fapt la un rezultat diferit, aceasta constituie o ***Acțiune înșelătoare***, astfel cum este prezentat în exemplul următor.

Exemplul 29: În partea din contul rețelei de socializare, în care utilizatorii pot împărtăși gânduri, poze etc., sunt solicitați să confirme că ar dori să partajeze acest conținut după ce l-au introdus sau l-au încărcat. Utilizatorii pot alege să acționeze un buton care spune *„Da, vă rog”*, sau un alt buton *„Nu, mulțumesc”*. Cu toate acestea, dacă utilizatorii decid să nu partajeze conținutul cu alte persoane făcând clic pe al doilea buton, conținutul este publicat în contul lor din rețeaua de socializare.

106. Ca și în exemplul precedent, aceste informații nu sunt transparente și îi privează pe utilizatori de alegere. Chiar dacă utilizatorii ar putea observa rapid publicația și ar șterge-o din nou, datele sunt procesate în pofida refuzului lor și sunt accesibile altor persoane. Un exemplu

mai rău îl găsim atunci când utilizatorii nu conștientizează că datele lor sunt prelucrate sau află despre aceasta cu dificultate sau doar dacă au cunoștințe în domeniul tehnologiilor informaționale, deoarece sunt prelucrate în fundalul platformei de comunicare socială.

ii. Modele bazate pe interfață

107. În afară de cele două modele de interfață înșelătoare menționate de mai sus, în acest caz de utilizare modelele bazate pe interfață sunt cele mai relevante.

Omiterea - Uită-te acolo (Lista de verificare 4.2.2 din Anexa I)

108. Atunci când o acțiune sau o informație legată de protecția datelor este pusă în poziție de concurență cu un alt element legat sau nu de protecția datelor, dacă utilizatorii aleg această altă opțiune, este probabil să uite de cealaltă opțiune, chiar dacă intenționau să o aleagă anume pe ea. Acesta este un model ***Uită-te acolo***, care trebuie evaluat de la caz la caz.

Exemplul 30: Un banner cookie pe platforma de comunicare socială informează „Pentru biscuiți delicioși, aveți nevoie doar de unt, zahăr și făină. Consultați rețeta noastră preferată aici [link]. Folosim și cookie-uri. Citiți mai multe în politica noastră privind cookie-urile [link].” și conține un buton „okay”.

109. Umorul nu trebuie folosit pentru a denatura riscurile posibile și a invalida informațiile reale. În acest exemplu, utilizatorii ar putea fi tentați să facă doar clic pe primul link, să citească rețeta biscuiților *(cookies în engleză)* și apoi să facă clic pe butonul *„okay”*. În afară de faptul că utilizatorilor nu li se oferă un mijloc de a nu-și da consimțământul, acest exemplu prezintă un caz, în care consimțământul ar putea să nu fie informat în mod corespunzător. Într-adevăr, făcând clic pe butonul *„okay”*, utilizatorii ar putea crede că doar resping un mesaj amuzant despre biscuiți ca o gustare coaptă și nu iau în considerare sensul tehnic al termenului *„cookies”*. În acest caz consimțământul nu ar fi informat în sensul articolului 7 alineatul (2) din RGPD coroborat cu articolul 4 alineatul (11) din RGPD.

110. Articolul 7 alineatul (2) din RGPD prevede, de asemenea, că o cerere de consimțământ ar trebui să se distingă în mod clar de alte lucruri. Prin urmare, informațiile privind protecția datelor nu trebuie să fie umbrite de alte contexte. În acest exemplu, jocul de cuvinte bazat pe omonime „cookie-biscuiți” poate induce în eroare cu privire la contextul de protecție a datelor. Pentru ca informațiile să fie distinse clar, informațiile relevante pentru ca utilizatorii să ofere consimțământ valabil ar trebui să fie clare, și nu ***Ascunse la vedere*** și să nu fie amestecate cu alte aspecte sau semnificații. Nu ar trebui să existe confuzii între informațiile privind protecția datelor și alte tipuri de informații. În caz contrar, utilizatorii ar putea fi distrași de la implicațiile reale ale prelucrării datelor lor cu caracter personal. Atunci când implementează aceste cerințe preliminare, proiectanții trebuie să aibă un anumit spațiu de manevră pentru a face informațiile atractive.

Obstrucționarea - Fundătură (Lista de verificare 4.4.1 din Anexa I)

111. Confuzia sau distragerea atenției nu este singurul efect posibil al modelelor de interfață înșelătoare atunci când este vorba de consimțământ. În special, modelul ***Fundătură*** poate interfera în mai multe moduri cu condițiile de obținere a consimțământului prevăzute la articolul 7 din RGPD, coroborat cu articolul 4 alineatul (11) din RGPD.

Exemplul 31: Utilizatorii vor să gestioneze permisiunile acordate platformei de comunicare socială pe baza consimțământului. Trebuie să găsească o pagină în setările legate de aceste acțiuni specifice și vor să dezactiveze partajarea datelor lor cu caracter personal în scopuri de

cercetare. Când utilizatorii fac clic pe casetă pentru a o debifa, nu se întâmplă nimic la nivel de interfață și au impresia că consimțământul nu poate fi retras.

112. În acest exemplu specific, modelul ***Fundătură*** ar putea încălca articolul 7 alineatul (3) din RGPD, deoarece utilizatorii aparent nu pot să-și retragă consimțământul pentru prelucrarea datelor lor cu caracter personal în scopuri de cercetare, deoarece funcția necesară aparent nu funcționează. Dacă acțiunea utilizatorilor nu este înregistrată în mod corespunzător în sistem, poate fi observată o încălcare a articolului 7 alineatul (3) din RGPD. Dacă alegerea este efectiv înregistrată în sistem, faptul că interfața nu reflectă acțiunea utilizatorilor ar putea fi calificat ca o nerespectare a principiului echității prevăzut la articolul 5 alineatul (1) litera (a) din RGPD. Atunci când o interfață pare să ofere mijloace de gestionare corectă a consimțământului, permițând utilizatorilor să-și dea consimțământul sau să retragă un consimțământ dat anterior, dar nu produce niciun efect vizual atunci când interacționează cu aceasta, interfața este înșelătoare pentru utilizatori și le creează confuzie și chiar frustrare. Un astfel de decalaj între starea în care se află sistemul și informațiile transmise de interfață ar trebui evitat, deoarece, în general, poate împiedica utilizatorii să-și controleze datele cu caracter personal.

113. Multe activități de prelucrare implică mai multe părți, adică un alt operator (comun) sau un alt operator implicat în afară de operatorul sau persoana împuternicită de operator, cu care persoana vizată contactează în mod direct.

Exemplul 32: Un furnizor de platformă de comunicare socială lucrează cu terți pentru prelucrarea datelor cu caracter personal ale utilizatorilor săi. În politica sa de confidențialitate, a inclus o listă a acestor terți fără link către fiecare politică de confidențialitate a lor, informând doar utilizatorii să viziteze site-urile web ale terților pentru a obține informații despre modul în care aceste entități prelucrează datele și pentru a-și exercita drepturile.

114. Acest exemplu de model ***Fundătură*** arată cum accesul la informații despre prelucrarea respectivă este complicat pentru utilizatori. Având în vedere faptul că ar putea să nu primească toate informațiile relevante despre prelucrare, se poate considera că o astfel de practică încalcă cerințele articolului 12 alineatul (1) din RGPD privind informațiile ușor accesibile. Dacă o astfel de practică este utilizată cu privire la informațiile acordate pentru a obține consimțământul, aceasta poate încălca cerințele de obținere a consimțământului informat stipulate la articolul 7 alineatul (2) coroborat cu articolul 4 alineatul (11) din RGPD, deoarece accesarea informațiilor ar fi prea complicată, iar persoanele vizate ar putea să nu fie conștiente pe deplin de consecințele alegerii lor.

Obstrucționarea - Mai lungă decât este necesar (Lista de verificare 4.4.2 din Anexa I)

115. Conform articolului 7 alineatul (3) din RGPD, retragerea consimțământului ar trebui să fie la fel de simplă ca și acordarea acestuia. Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679 abordează în continuare subiectul, precizând că acordarea și retragerea consimțământului ar trebui să fie posibile prin același mijloc. Aceasta presupune utilizarea aceleiași interfețe, însă mecanismele de retragere a consimțământului ar trebui să fie ușor accesibile, de exemplu printr-un link sau o pictogramă disponibilă în orice moment în timpul utilizării platformei de comunicare socială.

Exemplul 33: Un furnizor de platformă de comunicare socială nu oferă un mijloc de renunțare directă la publicitate direcționată, chiar dacă pentru acordarea consimțământului (acceptării) este necesar un singur clic.

116. Timpul necesar sau numărul de clicuri necesare pentru retragerea consimțământului poate fi utilizat pentru a evalua dacă este efectiv ușor de obținut. Implementarea modelului de interfață înșelătoare ***Mai lungă decât este necesar*** în timpul călătoriei utilizatorului pentru a-și retrage consimțământul, astfel cum este prezentat în exemplul 33, contravine acestor principii, încălcând astfel articolul 7 alineatul (3) din RGPD.

Supraîncărcarea - Labirint de confidențialitate (Lista de verificare 14.1.2 din Anexa I)

117. După cum este menționat în Orientările 05/2020 privind consimțământul, informațiile privind prelucrarea bazată pe consimțământ trebuie acordate persoanelor vizate pentru ca acestea să ia o decizie în cunoștință de cauză.[59] Fără acestea, consimțământul nu poate fi considerat valabil. Aceleași Orientări abordează în continuare modalitățile de furnizare a informațiilor, specificând că în acest scop pot fi utilizate informații stratificate. Cu toate acestea, astfel cum este prezentat în cazul de utilizare 2a,[60] furnizorii platformelor de comunicare socială trebuie să evite modelul de interfață înșelătoare ***Labirint de confidențialitate*** atunci când prezintă informații legate de o solicitare a consimțământului în mai multe straturi. Dacă unele informații devin prea dificil de găsit, deoarece persoanele vizate ar trebui să navigheze prin mai multe pagini sau documente, consimțământul obținut prin prezentarea unor astfel de informații nu ar putea fi considerat consimțământ informat, deoarece contravine articolului 7 din RGPD coroborat cu articolul 4 alineatul (11) din RGPD. De asemenea, aceasta ar însemna că consimțământul nu este valabil și că furnizorul platformei de comunicare socială ar încălca articolul 6 din RGPD.

Exemplul 34: Informațiile pentru retragerea consimțământului sunt disponibile printr-un link accesibil doar verificând fiecare secțiune a contului lor și informațiile legate de anunțuri publicitare afișate în fluxul de conținut al platformei de comunicare socială.

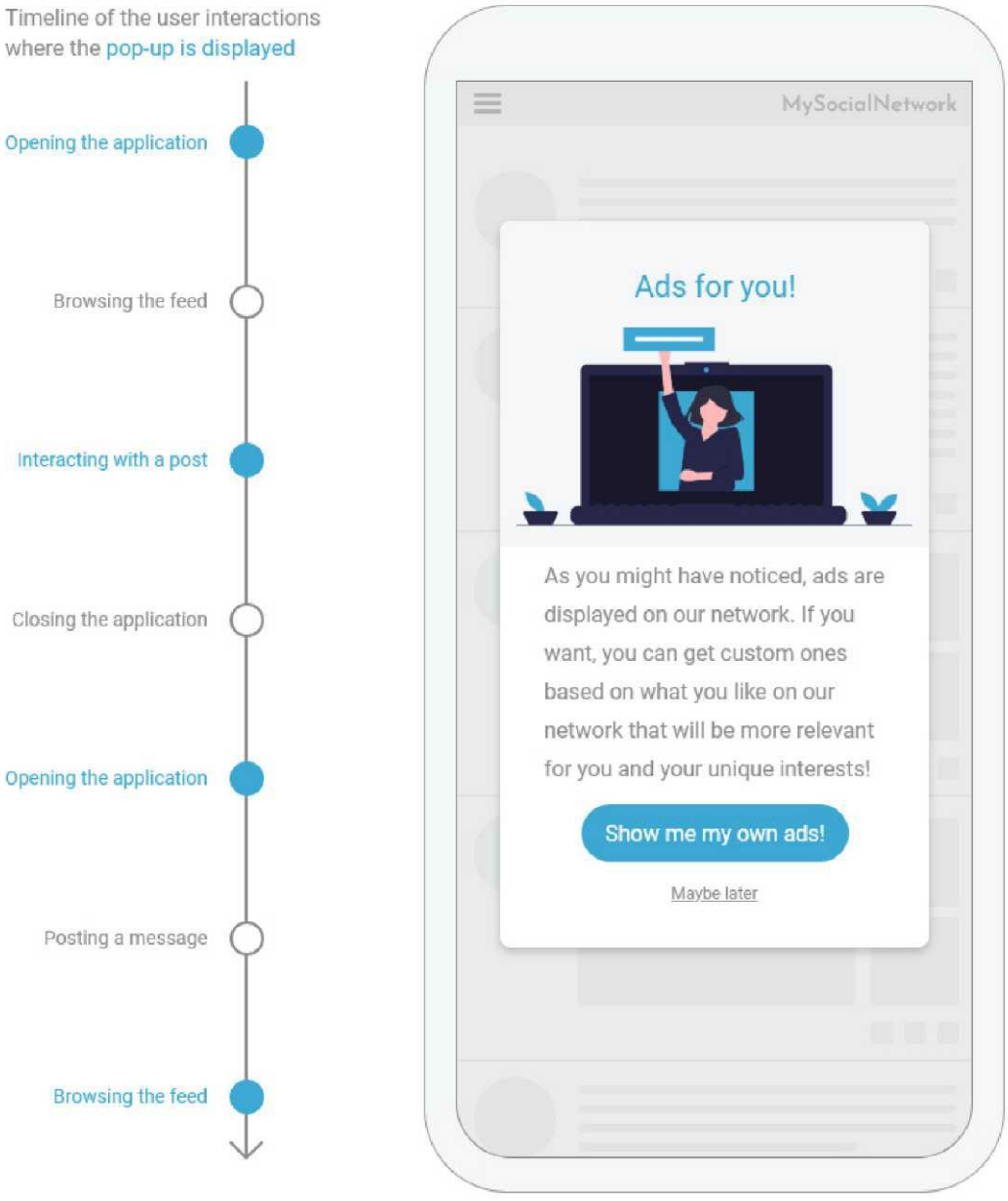
118. După cum arată scenariul descris mai sus, modelul de interfață înșelătoare ***Labirint de confidențialitate*** poate fi, de asemenea, o problemă după obţinerea consimţământului din cauza nerespectării cerinței prevăzute la articolul 7 alineatul (3) fraza 4 din RGPD, care prevede că retragerea consimțământului trebuie să fie la fel de ușoară ca și acordarea acestuia. Problema constă, în special, în faptul că procesul de retragere a consimțământului prevede mai mulți pași decât procesul de acordare a acestuia. Deoarece informațiile furnizate nu sunt, de asemenea, ușor accesibile persoanei vizate, fiind prezentate în diferite părți ale paginii, principiul prevăzut la articolul 12 alineatul (1) din RGPD este încălcat.

Supraîncărcarea – Solicitare continuă (Lista de verificare 4.1.1 din Anexa I)

119. ***Solicitarea continuă***, fiind utilizată pentru utilizatorii, care nu și-au dat consimțământul pentru prelucrarea datelor lor cu caracter personal într-un anumit scop, creează o piedică în utilizarea obișnuită a rețelei de socializare. Aceasta înseamnă că utilizatorii nu pot refuza acordarea consimțământul și, respectiv, nu-l pot retrage fără prejudicii. Aceasta contravine condiției de acordare a consimțământul în mod liber prevăzute la articolul 7 coroborat cu articolul 4 alineatul (11) din RGPD, conform căruia consimțământul înseamnă manifestare de voință liberă

[59] Orientările 05/2020 privind consimțământul, p. 62-64.
[60] A se vedea p. 79-81 mai sus.

a persoanei vizate prin care aceasta acceptă ca datele cu caracter personal care o privesc să fie prelucrate. Considerentul 42, fraza 5 din RGPD prevede, de asemenea, că consimțământul nu poate fi considerat exprimat în mod liber, dacă utilizatorii nu au o alegere reală sau liberă. Acest fapt este susținut și de Orientările CEPD privind consimțământul, conform cărora consimțământul nu va fi valabil dacă persoanele vizate nu au o alegere reală sau se simt obligate să își dea consimțământul de către orice element de presiune sau influență necorespunzătoare exercitată asupra lor, care îi împiedică să își exercite dorința liberă.[61] Deoarece ***Solicitarea continuă*** poate provoca o astfel de presiune, aceasta încalcă principiul consimțământului acordat în mod liber. De asemenea, deoarece este puțin probabil ca, odată ce utilizatorii și-au exprimat consimțământul, furnizorul platformei de comunicare socială să ofere în mod regulat (de exemplu, de fiecare dată când se loghează în contul lor) posibilitatea de a-și retrage consimțământul, acest model de interfață înșelătoare poate încălca articolul 7 alineatul (3) fraza 4 din RGPD, care prevede că retragerea consimțământului trebuie să fie la fel de simplă ca și acordarea acestuia („efect de oglindire").



[61] Orientările 05/2020 privind consimțământul, p. 13-14.

Termenul interacțiunilor utilizatorului în care este afișată fereastra pop-up Deschiderea aplicației Răsfoirea feed-ului Interacționarea cu o postare Închiderea aplicației Deschiderea aplicației Postarea unui mesaj Răsfoirea feed-ului	Rețeaua mea de socializare Anunțuri publicitare pentru tine! După cum ai putut observa, în rețeaua noastră sunt afișate anunțuri publicitare. Dacă dorești, poți personaliza unele pe baza a ceea ce îți place în rețeaua noastră, care vor fi cele mai relevante pentru tine și interesele tale unice! Arată-mi propriile mele anunțuri publicitare! Posibil mai târziu

Exemplul 35: În acest exemplu, atunci când utilizatorii își creează contul, sunt întrebați dacă acceptă ca datele lor să fie prelucrate pentru a primi publicitate personalizată. În cazul în care utilizatorii nu își dau consimțământul în timpul înregistrării pentru această utilizare a datelor lor, văd în mod regulat, în timp ce folosesc rețeaua de socializare, caseta prezentată mai sus, în care sunt întrebați dacă doresc să vizualizeze anunțuri publicitare personalizate. Această casetă îi blochează când utilizează rețeaua de socializare. Fiind afișată în mod regulat, această ***Solicitare continuă*** poate obosi utilizatorii, care în cele din urmă sunt nevoiți să-și exprime consimțământul cu afișarea publicității personalizate. Mai mult, în această interfață este folosit și modelul ***Ascuns la vedere***,[62] deoarece acțiunea de a accepta vizualizarea anunțurilor publicitare este mult mai vizibilă, decât opțiunea de a le refuza.

120. De asemenea, operatorul ar putea încălca principiul echității prevăzut la articolul 5 alineatul (1) litera (a) din RGPD. Având în vedere că, în exemplul de mai sus, utilizatorii nu și-au exprimat consimțământul printr-o acțiune clară pentru prelucrarea datelor lor cu caracter personal în scopul vizualizării publicității direcționate atunci când și-au creat contul, solicitarea repetitivă care pune în mod constant sub semnul întrebării refuzul clar pe care l-au declarat, este împovărătoare. Această acțiune clară a utilizatorilor în timpul înregistrării acum este pusă în mod constant sub semnul întrebării. Degradarea indusă a experienței utilizatorului sporește semnificativ probabilitatea ca utilizatorii să accepte publicitatea direcționată la un moment dat, doar pentru a evita întrebarea care apare de fiecare dată când se loghează în contul lor și doresc să folosească platforma de comunicare socială. În acest caz, neacordarea consimțământului are un impact direct asupra calității serviciului oferit utilizatorilor și condiționează executarea contractului.

c. **Cele mai bune practici**

Consecvența între dispozitive: Atunci când platforma de comunicare socială este disponibilă prin diferite dispozitive (de exemplu, computer, telefoane inteligente etc.), setările și informațiile legate de protecția datelor ar trebui să fie situate în aceleași spații în diferite versiuni și ar trebui să fie accesibile prin aceeași călătorie și elemente de interfață (meniu, pictograme etc.).

[62] A se vedea mai sus p. 49 sau mai jos partea 4.3.2 din Anexă

Identificarea modificărilor și compararea: găsiți definiția în cazul de utilizare 1 (p. 22).

Formulări coerente: găsiți definiția în cazul de utilizare 1 (p. 22).

Prezentarea definițiilor: găsiți definiția în cazul de utilizare 1 (p. 22).

Utilizarea exemplelor: găsiți definiția în cazul de utilizare 1 (p. 22).

Navigare lipicioasă: găsiți definiția în cazul de utilizare 2a (p. 28).

Înapoi sus: găsiți definiția în cazul de utilizare 2a (p. 28).

Notificări: găsiți definiția în cazul de utilizare 2c (p. 32).

Explicarea consecințelor: găsiți definiția în cazul de utilizare 2c (p. 32).

Cazul de utilizare 3b: Gestionarea setărilor de protecție a datelor

a. Descrierea contextului

121. După finalizarea procesului de înregistrare și pe parcursul întregului ciclu de viață al contului pe platforma de comunicare socială, utilizatorii ar trebui să poată ajusta setările de protecție a datelor.

122. Indiferent dacă utilizatorii cunosc deja sau nu despre protecția datelor în general și prevederile RGPD în special și dacă sunt atenți la datele cu caracter personal pe care doresc sau nu să le partajeze și să le vadă alte persoane, toți au dreptul să fie informați despre posibilitățile lor într-un mod transparent în timpul utilizării rețelei de socializare.

123. Utilizatorii partajează o mulțime de date cu caracter personal pe platformele de comunicare socială. Deseori sunt încurajați de aceste platforme să continue să distribuie mai mult conținut în mod regulat. Deși utilizatorii ar putea dori să împărtășească momente din viața lor, să participe la o dezbatere pe un subiect sau să-și lărgească rețelele de contacte, fie din considerente profesionale sau cu caracter personal, trebuie să li se ofere și instrumente pentru a controla cine poate vedea și ce părți ale datelor lor cu caracter personal pot fi văzute. O modalitate de a evita numărul mare de pași necesari pentru a-și schimba setarea ar fi proiectarea unui tablou de bord de confidențialitate, care să permită centralizarea setărilor și să simplifice controlul datelor utilizatorilor.

b. Prevederi legale relevante

124. După cum s-a menționat mai sus,[63] ca unul dintre principiile principale de prelucrare a datelor cu caracter personal, articolul 5 alineatul (1) litera (a) din RGPD prevede că datele cu caracter personal trebuie să fie prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”). În conformitate cu principiul răspunderii prevăzut la articolul 5 alineatul (2) din RGPD, operatorii sunt obligați să arate ce măsuri iau pentru ca activitățile lor de prelucrare să fie nu doar legale și echitabile, ci și transparente. De asemenea, în acest caz de utilizare este relevant principiul minimizării prevăzut la articolul 5 alineatul (1) litera (c) și principiul protecției datelor din momentul conceperii și în mod implicit prevăzut la articolul 25 din RGPD.

[63] A se vedea mai sus p. 1, 9, 10, 14-16.

c. Modele de interfață înșelătoare

i. Modele bazate pe conținut

125. Prima problemă, cu care se confruntă utilizatorii în acest context, se referă la locația setărilor de protecție a datelor. Utilizatorii ar putea citi notificarea privind protecția datelor și apoi decide să introducă modificări legate de prelucrarea datelor lor cu caracter personal. De asemenea, ar putea dori să facă aceste modificări fără să fi citit notificarea, doar utilizând regulat rețelele de socializare, de exemplu atunci când înțeleg că o informație postată pe o platformă de comunicare socială (de exemplu, o fotografie la plajă cu familia) este partajată cu un grup nedorit de oameni (de exemplu, colegi de serviciu). În orice caz, conform principiului transparenței opțiunile de setare trebuie să fie ușor accesibile și disponibile într-un mod ușor de înțeles. Aceasta este posibil prin centralizarea setărilor de date și de confidențialitate într-un singur loc, folosind o adresă URL auto-explicativă, cum ar fi [social-network.com]/data-settings.

126. Există mai multe modele de interfață care creează această problemă, care complică găsirea setărilor pentru utilizatori. Prin urmare, proiectanții platformelor de comunicare socială ar trebui să fie atenți ca să evite aceste modele de interfață înșelătoare.

Supraîncărcare – Prea multe opțiuni (Lista de verificare 4.1.3 din Anexa I)

127. Setările de protecție a datelor trebuie să fie ușor accesibile și ordonate logic. Setările legate de același aspect al protecției datelor ar trebui, de preferință, să fie situate într-un singur loc vizibil. În caz contrar, utilizatorii se vor confrunta cu un număr excesiv de pagini pentru verificare și revizuire, care îi vor supraîncărca în setările preferințelor de protecție a datelor. Într-adevăr, fiind confruntați cu ***Prea multe opțiuni*** din care să aleagă, ar putea să nu poată face o alegere sau ar putea să treacă cu vederea unele setări, renunțând în cele din urmă sau pierzând setările preferințelor lor de protecție a datelor. Astfel este încălcat principiul transparenței și echității. În special, poate fi încălcat articolul 12 alineatul (1) din RGPD, deoarece un control specific legat de protecția datelor devine complicat dacă este răspândit pe mai multe pagini sau diferența între opțiunile oferite utilizatorilor nu este clară.

Exemplul 36: Este posibil ca utilizatorii să nu știe ce să facă atunci când meniul unei platforme de comunicare socială conține mai multe file dedicate protecției datelor: *„protecția datelor”, „siguranță”, „conținut”, „confidențialitate”, „preferințele tale”.*

128. În acest exemplu, titlurile filelor nu indică în mod evident la ce conținut se pot aștepta utilizatorii pe pagina asociată sau că toate se referă la protecția datelor, în special atunci când una dintre file are în mod specific această denumire. Astfel poate apărea riscul că utilizatorii nu vor putea face modificări. De exemplu, dacă ar dori să limiteze sau să extindă numărul de persoane, care pot vedea pozele pe care le-au încărcat, denumirea filelor le-ar putea determina fie să facă clic pe „siguranță”, dacă utilizatorii consideră că există anumite riscuri pentru siguranță atunci când atele lor sunt public accesibile; clic pe „conținut”, dacă utilizatorii doresc să seteze vizibilitatea postării lor; sau pe „confidențialitate”, dacă această noțiune specifică se referă direct la ceea ce utilizatorii doresc să împărtășească. Aceasta înseamnă că aceste titluri de file nu sunt suficient de clare în ceea ce privește acțiunile pe care utilizatorii ar dori să le efectueze. În special, termenii „protecția datelor” și „confidențialitate” sunt deseori folosiți ca sinonime și, prin urmare, sunt deosebit de confuzi dacă sunt prezentați ca secțiuni diferite.

Lăsată în întuneric - Informații conflictuale (Lista de verificare 4.6.2 din Anexa I)

129. După cum este deja prezentat în exemplul 12 și în continuare în exemplul următor, în cadrul setărilor de protecție a datelor utilizatorii pot găsi și informații conflictuale.

Exemplul 37: Utilizatorul X dezactivează utilizarea geolocalizării sale în scopuri publicitare. După ce face clic pe comutatorul, care permite dezactivarea, apare mesajul *„Am dezactivat geolocalizarea ta, însă locația ta va fi în continuare utilizată”.*

Supraîncărcarea - Labirint de confidențialitate (Lista de verificare 4.1.2 din Anexa I)

130. Atunci când utilizatorii modifică o setare de protecție a datelor, conform principiului echității furnizorii platformelor de comunicare socială trebuie, de asemenea, să informeze utilizatorii despre alte setări, care sunt similare. Dacă astfel de setări sunt răspândite pe pagini diferite și neconectate ale platformei de comunicare socială, utilizatorii ar putea rata unul sau mai multe mijloace de a controla un aspect al datelor lor cu caracter personal. Utilizatorii se așteaptă să găsească setări similare una lângă alta.

Exemplul 38: Subiectele conexe, cum ar fi setările privind partajarea datelor de către furnizorul platformei de comunicare socială cu terți și invers, nu sunt disponibile în aceleași spații sau în spații apropiate, ci mai degrabă în file diferite ale meniului de setări.

131. Atunci când este vorba de numărul mediu de pași suportabil pentru modificarea unei setări de către utilizatorii platformelor de comunicare socială, nu există o „abordare unică pentru toți”. În același timp, un număr mai mare de pași poate descuraja utilizatorii să finalizeze modificarea sau aceștia pot rata unele părți, în special dacă doresc să facă mai multe modificări. Complicând astfel realizarea voinței utilizatorilor, sunt încălcate principiile echității prevăzute la articolul 5 alineatul (1) litera (a) din RGPD. Mai mult, modificarea setărilor este strâns legată de exercitarea drepturilor persoanelor vizate.[64] Modificarea unei setări legate de date, precum corectarea numelui sau ștergerea anului de absolvire, poate fi considerată o exercitare a dreptului la rectificare, respectiv a dreptului la ștergere, pentru aceste date specifice. Prin urmare, numărul de pași necesari ar trebui să fie cât mai mic posibil. Deși poate varia, un număr excesiv de pași împiedică utilizatorii și respectiv încalcă principiul echității, precum și articolul 12 alineatele (1) și (2) din RGPD.

Schimbător - Discontinuitatea limbajului (Lista de verificare 4.5.4 din Anexa I)

132. În ceea ce privește informațiile transparente, proiectanții platformelor de comunicare socială trebuie, de asemenea, să fie atenți să evite modelele de interfață înșelătoare bazate pe conținut enumerate în cazul de utilizare 2a, cum ar fi ***Discontinuitatea limbajului***. Din cauza că paginile de setări (sau părțile acestora) nu sunt puse la dispoziție în limba pe care utilizatorii au ales-o pentru platforma de comunicare socială, utilizatorilor le este mai greu să înțeleagă ce pot schimba și, prin urmare, le este complicat să-și stabilească preferințele.

Schimbător - Interfața incoerentă (Lista de verificare 4.5.3 din Anexa I)

133. În acest context, o altă problemă apare atunci când platformele de comunicare socială oferă opțiuni favorabile pentru protecția datelor utilizatorilor, dar nu îi informează despre aceasta în mod clar. Acesta este posibil atunci când platforma de comunicare socială diferă brusc de modelul său obișnuit de proiect de interfață. O astfel de ***Interfață incoerentă*** există atunci când o interfață nu este coerentă în diferite contexte sau nu corespunde așteptărilor utilizatorilor. Din cauza acestor diferențe, utilizatorii ar putea să nu găsească controlul sau informațiile dorite sau să interacționeze cu un element al interfeței neobișnuit pentru ei, chiar dacă această interacțiune determină utilizatorii să facă o agere de protecție a datelor pe care nu o doresc.

[64] A se vedea mai jos, cazurile de utilizare 4 și 5, adică părțile 3.4. și 3.5. din aceste Orientări.

Exemplul 39: Pe toată platforma de comunicare socială, nouă din zece opțiuni de setare a protecției datelor sunt prezentate în următoarea ordine:
– cea mai restrictivă opțiune (adică partajarea datelor cu alte persoane);
– opțiune limitată, dar nu la fel de restrictivă ca prima;
– cea mai puțin restrictivă opțiune (adică partajarea majorității datelor cu alte persoane).
Utilizatorii acestei platforme sunt obișnuiți ca setările lor de protecție a datelor să fie prezentate anume în această ordine. Totuși, această ordine nu este aplicată ultimei setări, în care alegerea vizibilității zilei de naștere a utilizatorilor este afișată în următoarea ordine:
– *Afișează ziua de naștere în întregime: 15 ianuarie 1929* (= cea mai puțin restrictivă opțiune)
– *Afișează doar ziua și luna: 15 ianuarie* (= opțiune limitată, dar nu cea mai restrictivă)
– *Nu afișa altora data mea de naștere* (= cea mai puțin restrictivă opțiune).

134. În acest exemplu, cele trei opțiuni din ultima setare sunt prezentate într-o altă ordine decât cea a setărilor anterioare. Este posibil ca utilizatorii, care și-au modificat anterior celelalte setări, să fie obișnuiți cu ordinea „obișnuită" a setărilor de la prima până la a noua. La ultima setare, sunt atât de obișnuiți cu această ordine încât aleg instinctiv prima opțiune, presupunând că aceasta trebuie să fie cea mai restrictivă. Aranjarea opțiunilor unei setări de protecție a datelor atât de diferită de celelalte din aceeași platformă de comunicare socială este o ***Interfață incoerentă***, deoarece se joacă cu ceea cu ce sunt obișnuiți utilizatorii și cu așteptările lor. Astfel utilizatorii pot să fie confuzi sau pot crede că au făcut alegerea, pe care și-au dorit-o atunci când, în realitate, nu este cazul.

ii. Modele bazate pe interfață

135. A doua problemă, care apare în contextul setărilor de protecție a datelor, este că setările ar putea încălca principiul protecției datelor în mod implicit. Conform articolului 25 alineatul (1) din RGPD, operatorii trebuie să ia măsuri corespunzătoare pentru a implementa principiile de protecție a datelor, cum ar fi minimizarea datelor (articolul 5 alineatul (1) litera (c) din RGPD). Aceste prevederi nu sunt respectate atunci când setările privind partajarea datelor cu caracter personal sunt stabilite în prealabil la una dintre opțiunile mai invazive, mai degrabă decât la cele mai puțin invazive.

Omiterea - Comoditatea înșelătoare (Lista de verificare 4.2.1 din Anexa I)

Exemplul 40: Între opțiunile de vizibilitate a datelor *„vizibile pentru mine"*, *„pentru cei mai apropiați prieteni"*, *„pentru toate conexiunile mele"* și *„publice"*, opțiunea din mijloc *„pentru toate conexiunile mele"* este setată în prealabil. Aceasta înseamnă că toți utilizatorii conectați la ele își pot vedea contribuțiile, precum și toate informațiile introduse pentru înregistrarea pe platforma de comunicare socială, cum ar fi adresa lor de e-mail sau data lor de naștere.

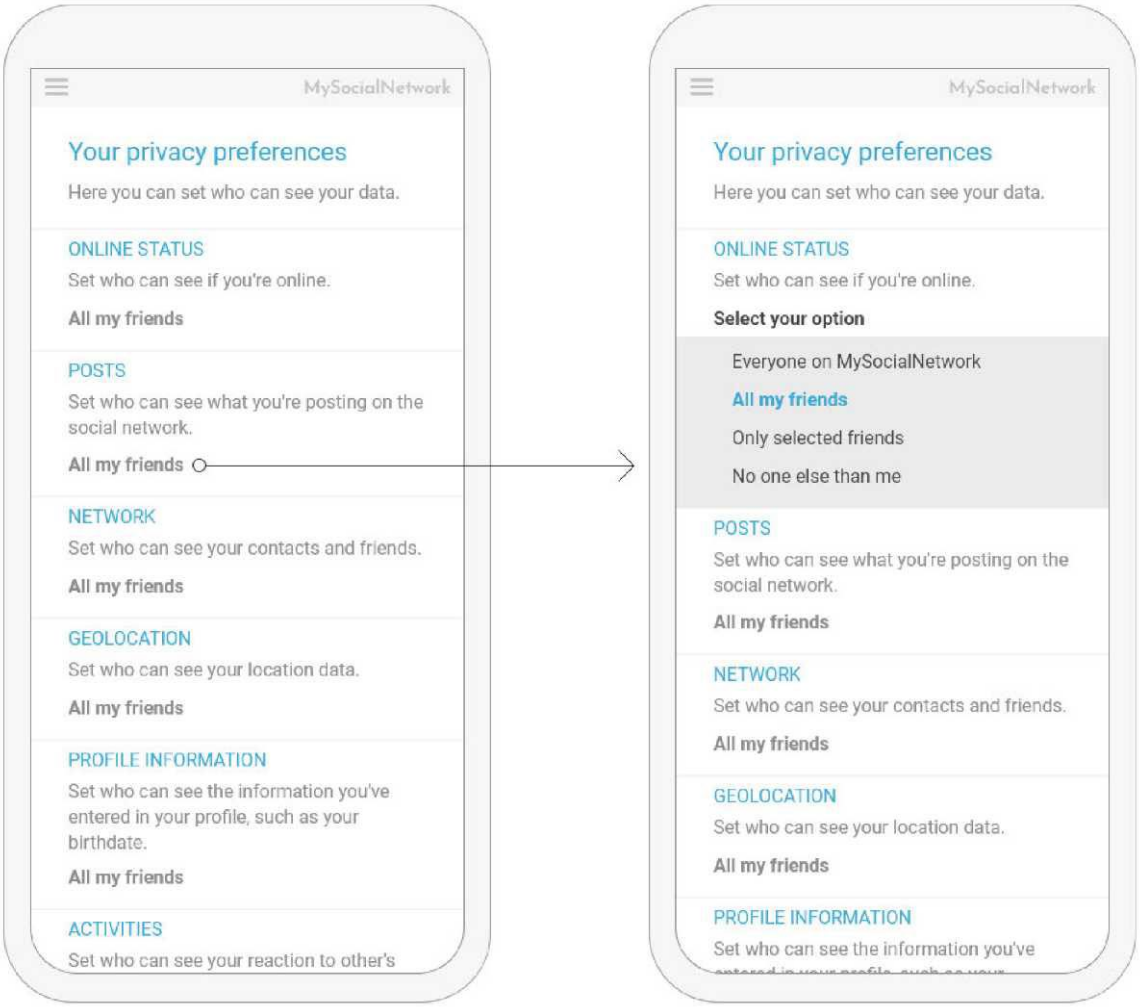
136. Furnizorii platformelor de comunicare socială ar putea argumenta că setarea cea mai puțin invazivă ar putea împiedica realizarea scopului utilizatorilor unei anumite platforme de comunicare socială, de exemplu, scopul de a fi găsiți de persoane necunoscute, care doresc să-și găsească un prieten nou, să stabilească o întâlnire sau să-și găsească un loc de muncă. Deși ar putea fi cazul pentru anumite setări, furnizorii platformelor de comunicare socială trebuie să rețină faptul că încărcarea de către utilizatori a anumitor date în rețea nu constituie consimțământul lor cu partajarea acestor date cu alte persoane.[65] În cazul în care furnizorii platformelor de comunicare socială amână asigurarea protecției datelor în mod implicit, vor

[65] De exemplu data lor de naștere, a se vedea p. 58 de mai sus.

trebui să informeze în mod corespunzător utilizatorii despre aceasta. Astfel utilizatorii trebuie să știe care este setarea implicită, că există opțiuni mai puțin invazive disponibile și unde trebuie să meargă pe platformă pentru a face modificări. În exemplul dat, atunci când opțiunea *„pentru cei mai apropiați prieteni”* este setată în prealabil pentru contribuțiile postate de utilizatori în mod activ pe platforma de comunicare socială, ar trebui să li se indice unde pot modifica această setare. Totuși, setarea prealabilă a vizibilității cu *„pentru toate conexiunile mele”* (sau chiar cu publicul larg) constituie o ***Comoditate înșelătoare***, mai ales atunci când este aplicată datelor solicitate de furnizorul platformei de comunicare socială de la utilizatori pentru a crea un cont, cum ar fi adresa de e-mail sau data nașterii acestora. După cum este descris în cazul de utilizare 1 la p. 55, această practică încalcă articolul 25 alineatul (2) din RGPD.

Agitarea - Dirijarea emoțională (Lista de verificare 4.3.2 din Anexa I)

137. Modelele de interfață înșelătoare ***Ascuns la vedere*** și ***Comoditate înșelătoare*** pot fi combinate cu ușurință atunci când este vorba de selectarea opțiunilor legate de protecția datelor, astfel cum este prezentat în exemplul 9 pentru procesul de înregistrare, și mai jos atunci când utilizatorii doresc să-și schimbe preferințele de protecție a datelor în timp ce folosesc rețelele de socializare.



Rețeaua mea de socializare Preferințele tale de confidențialitate Aici poți seta cine poate vedea datele tale	Rețeaua mea de socializare Preferințele tale de confidențialitate Aici poți seta cine poate vedea datele tale

STATUTUL ONLINE Setează cine te poate vedea online Toți prietenii mei POSTĂRI Setează cine poate vedea postările tale în rețeaua de socializare Toți prietenii mei REȚEAUA Setează cine poate vedea contactele și prietenii tăi. Toți prietenii mei GEOLOCALIZAREA Setează cine poate vedea datele locației tale. Toți prietenii mei IFNORMAȚII DE PROFIL Setează cine poate vedea informațiile pe care le-ai introdus în profilul tău, cum ar fi data ta de naștere. Toți prietenii mei ACTIVITĂȚI Setează cine poate vedea reacția ta la	STATUTUL ONLINE Setează cine te poate vedea online Selectează opțiunea ta Oricine în Rețeaua mea de socializare Toți prietenii mei Doar prietenii selectați Nimeni în afară de mine POSTĂRI Setează cine poate vedea postările tale în rețeaua de socializare Toți prietenii mei REȚEAUA Setează cine poate vedea contactele și prietenii tăi. Toți prietenii mei GEOLOCALIZAREA Setează cine poate vedea datele locației tale. Toți prietenii mei IFNORMAȚII DE PROFIL Setează cine poate vedea informațiile pe care le-ai introdus

Exemplul 41: În acest exemplu, atunci când utilizatorii doresc să gestioneze vizibilitatea datelor lor, trebuie să meargă în fila *„preferință de confidențialitate”*. Aici sunt enumerate informațiile, pentru care își pot seta preferința. Cu toate acestea, modul în care sunt afișate informațiile nu clarifică cum pot fi modificate setările. Într-adevăr, utilizatorii trebuie să facă clic pe opțiunea de vizibilitate curentă pentru a accesa un meniu drop-down, din care pot selecta opțiunea pe care o preferă.

138. Chiar dacă în această filă pot fi modificate preferințele, este un model de interfață ***Ascuns la vedere***, deoarece meniul drop-down nu este direct vizibil pentru utilizatorii, care trebuie să ghicească că făcând clic pe opțiunea curentă se va deschide ceva. Într-adevăr, nu există niciun indiciu vizual obișnuit (text subliniat, săgeată în jos) despre posibilitatea de a interacționa și de a deschide meniul drop-down. Această practică specifică nu este loială față de utilizatori și ar putea face parte din nerespectarea generală a principiului echității prevăzut la articolul 5 alineatul (1) litera (a) din RGPD. De asemenea, dacă opțiunile au fost selectate în prealabil în mod implicit, s-ar putea observa și modelul de interfață înșelătoare ***Comoditate înșelătoare***, astfel cum este descris mai sus la p. 128.

Schimbător - Decontextualizarea (Lista de verificare 4.5.2 din Anexa I)

Decontextualizarea are loc atunci când controlul sau informațiile legate de protecția datelor sunt situate pe o pagină, care este în afara contextului, astfel încât este puțin probabil ca utilizatorii să o găsească, deoarece nu ar fi intuitiv clar că trebuie să le caute pe pagina respectivă.

Exemplul 42: Setările de protecție a datelor sunt greu de găsit în contul utilizatorului, deoarece la primul nivel nu există un capitol de meniu cu o denumire sau un titlu, care să conducă în această direcție. Utilizatorii trebuie să caute alte submeniuri, cum ar fi *„Securitate”*.

140. În acest exemplu, utilizatorii nu sunt îndrumați către setările de protecție a datelor, deoarece nu sunt utilizați termeni semnificativi și clari pentru a indica unde se află pe platforma de comunicare socială. Într-adevăr, termenul *„Securitate”* acoperă doar o parte din ceea ce se poate aștepta de la setările de protecție a datelor. Prin urmare, utilizatorii nu înțeleg că trebuie să caute acest meniu pentru a găsi astfel de setări. Această lipsă de transparență îngreunează accesul la informații mai mult decât ar trebui și poate fi considerat că este încălcat articolul 12 alineatul (1) din RGPD și, eventual, articolul 12 alineatul (2) din RGPD dacă aceste setări se referă la exercitarea unui drept.

Exemplul 43: Modificarea setării este complicată, deoarece în versiunea de desktop a platformei de comunicare socială, butonul *„salvare”* pentru înregistrarea modificărilor acestora nu este vizibil cu toate opțiunile, ci doar în partea de sus a submeniului. Este posibil ca utilizatorii să treacă cu vederea și să considere în mod greșit că setările sunt salvate automat și prin urmare să treacă la o altă pagină fără a face clic pe butonul „salvare”. Această problemă nu apare în versiunile de aplicație și mobilă. Prin urmare, ea creează confuzie suplimentară pentru utilizatorii care trec de la versiunea mobilă/de aplicație la versiunea desktop, și ar putea crede că își pot schimba setările doar în versiunea mobilă sau doar în aplicație.

141. După ce utilizatorii au găsit setările de protecție a datelor și și-au setat alegerile, este posibil să nu fie împiedicați să seteze protecția. După ce utilizatorii au făcut o modificare, modalitatea de salvare a acesteia trebuie să fie evidentă, indiferent dacă are loc imediat ce utilizatorii ajustează o setare sau dacă este nevoie de o confirmare printr-un clic pe un anumit element al interfeței, cum ar fi butonul „salvare”. De asemenea, conform principiului echității stipulat în articolul 5 alineatul (1) litera (a) din RGPD, furnizorii platformelor de comunicare socială trebuie să fie consecvenți pe toată platforma lor, în special pe diferite dispozitive. Acesta nu este cazul când interfața folosește un model de interfață înșelătoare, astfel cum este prezentat în exemplele de mai sus.

d. Cele mai bune practici

Directoriul de protecție a datelor: Pentru a se orienta ușor printr-o secțiune diferită a meniului, oferiți utilizatorilor o pagină ușor accesibilă de unde sunt accesibile toate acțiunile (de exemplu, setările) și informațiile legate de protecția datelor. Această pagină poate fi găsită în meniul de navigare principal al furnizorului platformei de comunicare socială, în contul utilizatorului, prin politica de confidențialitate etc.

Opțiuni în bloc: Plasarea opțiunilor, care au același scop de procesare, astfel încât utilizatorii să le poată schimba mai ușor, lăsând totuși utilizatorilor posibilitatea de a face modificări mai detaliate. Dacă platformele de comunicare socială prezintă opțiuni în bloc, acestea nu ar trebui să conțină elemente neașteptate sau irelevante (de exemplu elemente cu scopuri diferite). Dacă pentru prelucrare este necesar consimțământ, opțiunile în bloc trebuie să fie în conformitate cu Orientările CEPD privind consimțământul, în special p. 42-44.

Comenzi rapide: găsiți definiția în cazul de utilizare 1 (p. 22) *(de exemplu, atunci când utilizatorii sunt informați despre un aspect al prelucrării, aceștia sunt invitați să își stabilească preferințele de date aferente pe pagina setărilor/tabloul de bord corespunzător).*

Adresa URL auto-explicativă: paginile legate de setările sau informațiile de protecție a datelor ar trebui să utilizeze o adresă web, care să reflecte în mod clar conținutul acestora. De exemplu, o

pagină, care centralizează controlul protecției datelor, ar putea avea o adresă URL, cum ar fi [social-network.com]/data-settings.

Formulări coerente: găsiți definiția în cazul de utilizare 1 (p. 22).

Prezentarea definițiilor: găsiți definiția în cazul de utilizare 1 (p. 22).

Utilizarea exemplelor: găsiți definiția în cazul de utilizare 1 (p. 22).

Navigare lipicioasă: găsiți definiția în cazul de utilizare 2a (p. 28).

Notificări: găsiți definiția în cazul de utilizare 2c (p. 32).

Explicarea consecințelor: găsiți definiția în cazul de utilizare 2c (p. 32).

Consecvența între dispozitive: găsiți definiția în cazul de utilizare 3a (p. 39).

3.4 Corectitudinea continuă pe platforma de comunicare socială: drepturile persoanei vizate

Cazul de utilizare 4: Cum sunt furnizate funcții corespunzătoare pentru exercitarea drepturilor persoanelor vizate

a. Descrierea contextului

142. A utiliza de o platformă de comunicare socială înseamnă a beneficia de funcțiile acesteia în conformitate cu scopurile declarate de furnizorul platformei de comunicare socială. Aceasta mai înseamnă că utilizatorii trebuie să își poată exercita drepturile de protecție a datelor. Ele sunt elemente cheie ale protecției datelor și ale controlului propriilor informații, indiferent dacă datele sunt furnizate direct și cu bună știință de persoanele vizate în legătură cu utilizarea serviciului sau a dispozitivului, sau sunt deduse din analiza datelor furnizate de către persoana vizată.[66] Pentru volumul de date cu caracter personal, care circulă pe toată platforma, utilizatorii trebuie să-și poată controla datele cu ajutorul drepturilor conferite de RGPD într-un mod clar și intuitiv. CEPD a explicat aceste noțiuni în mai multe orientări.[67] Exercitarea drepturilor trebuie să fie disponibilă de la începutul până la sfârșitul utilizării platformei și, în unele cazuri, chiar și după ce utilizatorii au decis să părăsească platforma, iar operatorul încă nu a șters datele. Neutilizatorii platformei trebuie, de asemenea, să aibă posibilitatea de a-și exercita drepturile persoanelor vizate legate de prelucrarea datelor lor. Desigur, în unele cazuri nu toate drepturile persoanelor vizate sunt disponibile, în dependență de temeiul juridic al prelucrării datelor. Prin urmare, furnizorul platformei de comunicare socială ar trebui să explice în mod clar de ce anumite drepturi nu sunt aplicabile și de ce unele dintre ele pot fi limitate. După cum s-a menționat mai sus și în capitolele anterioare, utilizarea drepturilor trebuie să fie operativă. Automatizarea, precum și alte funcționalități ale platformelor de comunicare socială, ar trebui utilizate pentru a facilita exercitarea drepturilor.

b. Prevederile legale relevante

[66] Articolul 29 din Orientările grupului de lucru privind dreptul la portabilitatea datelor conform Regulamentului 2016/679, WP242 ed.01, p. 10, https://ec.europa.eu/newsroom/article29/items/611233/en.

[67] Orientările privind dreptul la portabilitatea datelor și Orientările 05/2019 ale CEPD privind criteriile dreptului de a fi uitat în cauzele referitoare la motoarele de căutare în temeiul RGPD (partea 1) - versiune adoptată în urma consultării publice, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines en.

143. RGPD prevede șapte drepturi diferite, pe care persoanele vizate le pot exercita în anumite condiții (de exemplu, temeiul juridici al prelucrării etc.). Conform articolului 15 din RGPD, persoanele vizate au dreptul să știe dacă datele cu caracter personal, care le privesc, sunt prelucrate, și să le acceseze, adică să obțină informații suplimentare despre prelucrarea lor, precum și să primească o copie a datelor respective. Articolul 16 din RGPD prevede detaliat dreptul la rectificare, permițând persoanelor vizate să actualizeze datele cu caracter personal pe care le prelucrează operatorul. Dreptul la ștergerea datelor prevăzut la articolul 17 RGPD permite persoanelor vizate să obțină ștergerea datelor cu caracter personal care le privesc. Dreptul la restricționarea prelucrării conform articolului 18 din RGPD oferă persoanelor vizate posibilitatea de a opri temporar prelucrarea datelor lor cu caracter personal. Articolul 20 din RGPD prevede dreptul la portabilitatea datelor, care permite persoanelor vizate să primească datele lor cu caracter personal și să le transmită altui operator.[68] Persoanele vizate au, de asemenea, dreptul de a se opune prelucrării datelor lor cu caracter personal, conform articolului 21 din RGPD. În cele din urmă, articolul 22 din RGPD oferă persoanelor vizate dreptul de a nu fi obiectul unei decizii bazate exclusiv pe prelucrare automată.[69]

144. CEPD menționează că nu toate aceste drepturi se vor aplica oricărei platforme de comunicare socială, în dependență de temeiul său juridic, de scopurile prelucrării datelor cu caracter personal și de tipurile de servicii prestate. Diferențele ar trebui explicate de către operator în conformitate cu articolul 12 din RGPD. Aceasta înseamnă că informațiile privind drepturile aplicabile ar trebui să fie concise și clare pentru utilizatori, inclusiv de ce anumite drepturi nu se aplică. O astfel de explicație ar putea limita volumul de comunicare cu utilizatorii atunci când aceștia încearcă să-și exercite unele drepturi. Exercitarea dreptului ar trebui să fie simplă și accesibilă în conformitate cu articolul 12 alineatul (2), iar răspunsul ar trebui dat fără întârzieri nejustificate, conform articolului 12 alineatul (3) din RGPD. În mod similar, platforma de comunicare socială ar trebui să explice de ce anumite solicitări nu pot fi îndeplinite și să informeze despre posibilitatea de a depune o plângere la o autoritate de supraveghere desemnată în conformitate cu articolul 12 alineatul (4) din RGPD. Astfel, este posibil ca următoarele modele de interfață înșelătoare să nu fie aplicabile tuturor drepturilor menționate mai sus. Dreptul la ștergere este discutat detaliat în capitolul următor.

c. Modele de interfață înșelătoare

i. Modele bazate pe conținut

Obstrucționarea - Fundătură (Lista de verificare 4.4.1 din Anexa I)

145. Modelul de interfață înșelătoare ***Fundătură*** poate avea un impact direct asupra ușurinței de acces la exercitarea drepturilor. Atunci când linkurile, care redirecționează către mijloacele de exercitare a unui drept, sunt întrerupte sau lipsesc explicații clare cu privire la modul de exercitare a unui drept, utilizatorii nu vor putea să-l exercite în mod corespunzător, ceea ce încalcă articolul 12 alineatul (2) din RGPD.

Exemplul 44: Utilizatorii fac clic pe *„exercit dreptul meu de acces”* din notificarea de confidențialitate, dar în schimb sunt redirecționați către profilul lor, care nu oferă nicio caracteristică legată de exercitarea dreptului.

[68] Acest drept este prezentat detaliat în Orientările privind dreptul la portabilitatea datelor.

[69] Articolul 29 din Orientările privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului 2016/679, wp251 ed.01, p. 19 și următoarele, https://ec.europa.eu/newsroom/article29/items/612053/en.

146. Exemplul de model de interfață înșelătoare menționat mai sus accentuează necesitatea de a oferi utilizatorilor o modalitate clară și intuitivă de a-și exercita drepturile în conformitate cu articolul 12 alineatele (1) și (2) din RGPD, deoarece în caz contrar aceștia nu ar putea să le exercite. Nu este suficient să se confirme utilizatorilor că au drepturi vizate, după cum prevede articolul 12 alineatul (1) din RGPD (inclusiv modul de comunicare) și în special conform articolului 13 alineatul (2) litera (b) și articolului 14 alineatul (2) litera (c) din RGPD. De asemenea, utilizatorii trebuie să le poată exercita cu ușurință, de preferință într-un mod încorporat în interfața platformei, de exemplu prin furnizarea unui formular special. Astfel, de asemenea, experiența utilizatorului cu o platformă ar fi mai pozitivă, dat fiind eforturile furnizorului de a se adapta așteptărilor utilizatorilor de prelucrare și de control asupra datelor lor cu caracter personal în mod legal prin combinarea exercitării drepturilor cu alte funcționalități ale serviciului. Atunci când serviciul platformei de comunicare socială permite o comunicare bidirecțională între utilizatori, precum și între operator și utilizatori, nu există niciun motiv pentru care operatorul să își limiteze canalul de comunicare cu scopul de a facilita solicitările persoanelor vizate ale unui mijloc separat de comunicare precum e-mailul. În același timp, persoanele vizate nu ar trebui să fie nevoite să vină pe platformă pentru a comunica cu operatorul.[70] De asemenea, este posibil ca operatorii să nu limiteze acest drept al persoanei vizate la dreptul de copiere, ci trebuie să asigure, de asemenea, furnizarea informațiilor menționate la articolul 15 alineatul (1) din RGPD utilizatorilor care solicită acces la datele lor.[71]

Schimbător - Discontinuitatea limbajului (Lista de verificare 4.5.4 din Anexa I)

Exemplul 45: Atunci când faceți clic pe un link legat de exercitarea drepturilor persoanei vizate, următoarele informații nu sunt afișate în limba (limbile) oficială (oficiale) a (ale) țării (țărilor) utilizatorilor, iar serviciul este. În schimb, utilizatorii sunt redirecționați către o pagină în limba engleză.

147. Ținând cont de principiul transparenței prevăzut la articolul 5 alineatul (1) litera (a) și articolul 12 alienatul (1) din RGPD, utilizatorii trebuie să primească toate informațiile despre drepturile lor într-un mod clar, simplu și inteligibilă. Acestea trebuie să fie, de asemenea, legate de locația utilizatorilor și de limba folosită în țara sau jurisdicția, în care este oferit serviciul. Faptul că utilizatorii își confirmă capacitatea de a folosi în orice mod o limbă străină nu îl exonerează pe operator de obligațiile sale. Același lucru se aplică atunci când o astfel de cunoaștere a altor limbi înțelese de utilizatori poate fi dedusă din activitățile lor. Informațiile ar trebui să fie relevante și utile pentru utilizatorii, care își exercită drepturile.

Lăsată în întuneric – Formulare sau informații ambigue (Lista de verificare 4.6.3 din Anexa I)

148. În contextul drepturilor persoanelor vizate, utilizatorii se pot confrunta și cu modelul de interfață înșelătoare ***Formulare sau informații ambigue,*** astfel cum este prezentat în exemplul următor.

Exemplul 46: Platforma de comunicare socială nu precizează în mod explicit că utilizatorii din UE au dreptul de a depune o plângere la o autoritate de supraveghere, ci doar menționează că în unele țări, fără a menționa care anume, există autorități de protecție a datelor cu care furnizorul rețelei de socializare cooperează în legătură cu reclamațiile.

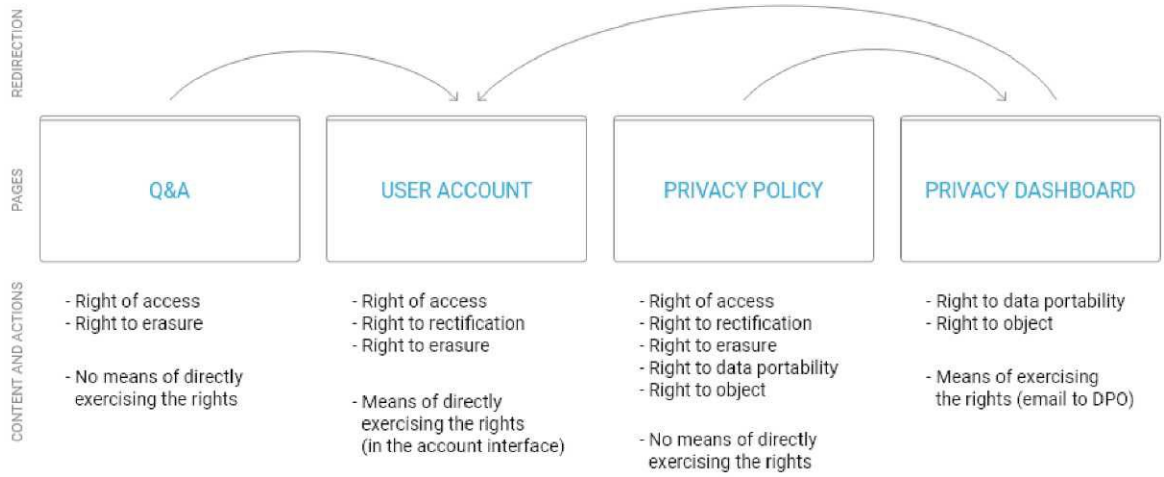
[70] A se vedea Orientările 01/2022 ale CEPD privind drepturile persoanelor vizate – dreptul de acces, p. 136, versiunea 1.0, https://edpb.europa.eu/system/files/2022-01/edpb guidelines 012022 right-of-access O.pdf.
[71] A se vedea Orientările 01/2022, p. 131, 142, 145.

149. Furnizorii platformelor de comunicare socială trebuie, de asemenea, să fie atenți să evite modelul de interfață înșelătoare ***Formulare sau informații ambigue*** atunci când informează persoanele vizate despre drepturile lor. Furnizarea informațiilor utilizatorilor astfel, încât aceștia să nu fie siguri cum vor fi prelucrate datele lor sau cum să dețină un anumit control asupra datelor lor și, prin urmare, cum să-și exercite drepturile, încalcă principiul transparenței. De asemenea, formularea vagă nu este un limbaj concis, astfel cum impune articolul 12 alineatul (1) din RGPD și din acest motiv informațiile furnizate persoanei vizate pot fi incomplete, ceea ce ar putea fi considerat o încălcare a articolului 13 din RGPD. Exemplul menționat mai sus prezintă, de asemenea, o încălcare a articolului 13 alineatul (2) litera (d) din RGPD, care impune operatorilor să ofere persoanelor vizate informații cu privire la dreptul lor de a depune o plângere la o autoritate de supraveghere. Aceasta este, de asemenea, contrar articolului 12 alineatul (2) din RGPD, deoarece furnizorul platformei de comunicare socială nu facilitează exercitarea dreptului de a depune o plângere.

ii. Modele bazate pe interfață

Supraîncărcarea - Labirint de confidențialitate (Lista de verificare 4.1.2 din Anexa I)

150. După cum este menționat mai sus în cazul de utilizare 3b, numărul de pași necesari pentru a primi informațiile relevante privind protecția datelor nu trebuie să fie excesiv, la fel ca și numărul de pași pentru atingerea drepturilor persoanelor vizate.[72] Astfel, utilizatorii ar trebui să poată ajunge întotdeauna rapid la site-ul de exercitare a drepturilor, indiferent de punctul lor de plecare și unde platforma de comunicare socială a localizat această funcție. Prin urmare, furnizorii platformelor de comunicare socială ar trebui să se gândească bine la diferite situații în care utilizatorii ar dori să-și exercite drepturile și să proiecteze accesul la locul în care le pot exercita. Aceasta înseamnă că pe o platformă de comunicare socială pot fi create și disponibile mai multe căi pentru a ajunge la un drept al persoanei vizate. Cu toate acestea, fiecare cale ar trebui să faciliteze accesul la exercitarea drepturilor și să nu interfereze cu o altă cale. În caz contrar, ar fi considerată un model de interfață înșelătoare ***Labirint de confidențialitate***, astfel cum este prezentat în exemplele 47 și 48, ceea ce este contrar articolului 12 alienatul (2) din RGPD.

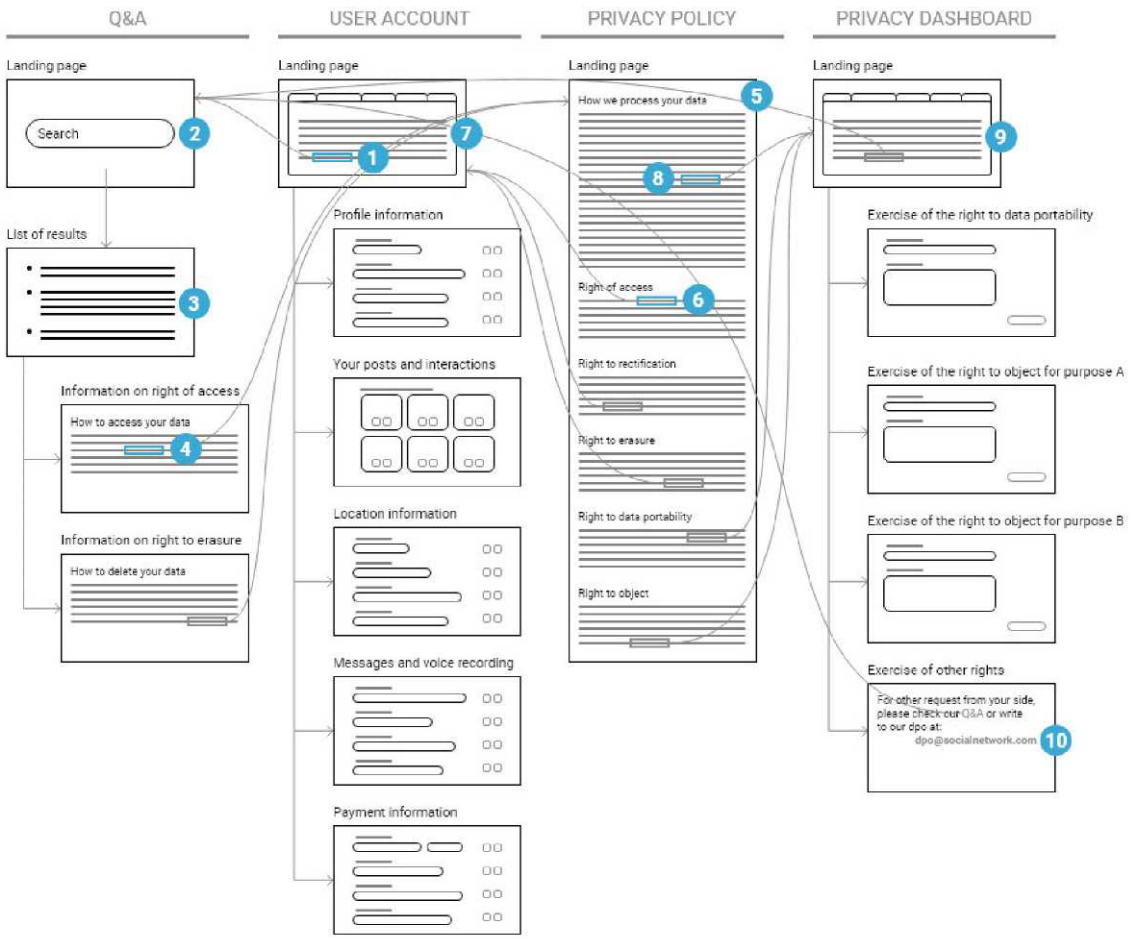


ÎNTREBĂRI ȘI RĂSOUNSURI	CONTUL UTILIZATORULUI	POLITICA DE CONFIDENȚIALITATE	TABLOUL DE BORD DE CONFIDENȚIALITATE
CONȚINUT ȘI ACȚIUNI	PAGINI	REDIRECȚIONAREA	
Dreptul de acces Dreptul la ștergere	Dreptul de acces Dreptul de rectificare Dreptul la ștergere	Dreptul de acces Dreptul de rectificare Dreptul la ștergere	Dreptul la portabilitatea datelor Dreptul de a se opune

[72] A se vedea mai sus p. 123.

		Dreptul la portabilitatea datelor Dreptul de a se opune	
Fără mijloace de exercitare directă a drepturilor	Mijloace de exercitare directă a drepturilor (în interfața contului)	Fără mijloace de exercitare directă a drepturilor	Mijloace de exercitare directă a drepturilor (e-mail către DPO)

Exemplul 47: Aici, informațiile referitoare la drepturile de protecție a datelor sunt disponibile pe cel puțin patru pagini. Chiar dacă politica de confidențialitate informează despre toate drepturile, aceasta nu redirecționează către paginile relevante pentru fiecare dintre ele. În schimb, atunci când utilizatorii își vizitează contul, nu găsesc nicio informație cu privire la unele drepturi, pe care le pot exercita. În acest ***Labirint de confidențialitate*** utilizatorii sunt nevoiți să parcurgă multe pagini pentru a găsi unde să-și exercite fiecare drept și, în dependență de navigarea lor, este posibil să nu cunoască toate drepturile lor.



ÎNTREBĂRI ȘI RĂSOUNSURI	CONTUL UTILIZATORULUI	POLITICA DE CONFIDENȚIALITATE	TABLOUL DE BORD DE CONFIDENȚIALITATE
Pagina de destinație Căutare	Pagina de destinație	Pagina de destinație Cum prelucrăm datele tale	Pagina de destinație
Lista rezultatelor	Informații de profil	Dreptul de acces	Exercitarea dreptului la portabilitatea datelor
Informații despre dreptul de acces	Postările și interacțiunile tale	Dreptul la rectificare	Exercitarea dreptului de a se opune în scopul A

Cum sunt accesate datele tale			
Informații despre dreptul la ștergere Cum se șterg datele tale	Informații despre locație	Dreptul la ștergere	Exercitarea dreptului de a se opune în scopul B
	Mesaje și înregistrarea vocală	Dreptul la portabilitatea datelor	Exercitarea altor drepturi Pentru altă solicitare din partea ta, verifică Întrebări și răspunsuri sau scrie-ne la dpo: dpo@socialnetwork.com
	Informații despre plăți	Dreptul de a se opune	

Exemplul 48: În acest exemplu, utilizatorii doresc să-și actualizeze unele date ale lor cu caracter personal, dar nu găsesc o modalitate de a o face în contul lor. Ei fac clic pe un link (1) care îi redirecționează către pagina „Întrebări și răspunsuri" unde își introduc întrebarea (2). Apar mai multe rezultate (3), unele fiind legate de drepturile de acces și de ștergere. După verificarea tuturor rezultatelor, aceștia fac clic (4) pe linkul disponibil pe pagina „Cum să vă accesați datele". Linkul îi redirecționează către politica de confidențialitate (5). Acolo, ei găsesc informații despre drepturi suplimentare. După ce au citit aceste informații, fac clic pe (6) linkul legat de exercitarea dreptului la rectificare, care îi redirecționează către contul de utilizator (7). Fiind nemulțumiți, revin la politica de confidențialitate și fac clic pe linkul general „Trimite-ne o solicitare" (8). Astfel utilizatorii ajung la tabloul de bord de confidențialitate (9). Deoarece niciuna din opțiunile disponibile nu pare să se potrivească necesităților lor, în cele din urmă utilizatorii merg la pagina „exercitarea altor drepturi" (10) unde în sfârșit găsesc o adresă de contact.

151. Ambele exemple prezintă căi deosebit de lungi și obositoare pentru a-și exercita drepturile. Atunci când mijloace de exercitare a diferitelor drepturi nu se află în același spațiu, dar există o pagină, în care sunt enumerate toate drepturile vizate, ultimul ar trebui să redirecționeze exact către aceste spații diferite, și nu doar către unul sau o parte dintre acestea, astfel cum este prezentat în exemplul 47. Celălalt exemplu arată o călătorie, în care utilizatorii nu găsesc mijlocul de a-și exercita cu ușurință dreptul specific pe care și-l doresc, și anume dreptul la rectificare, deoarece locul în care de obicei este exercitat, și anume contul de utilizator, nu oferă mijlocul necesar în acest scop. Căutând o altă modalitate de a-și exercita acest drept, aceștia nu găsesc unul corespunzător și trebuie să apeleze la un mijloc general oferit în tabloul de bord de confidențialitate.

152. Dacă au fost concepute mai multe căi către exercitarea unui drept, utilizatorilor ar trebui să le fie întotdeauna ușor să găsească o imagine de ansamblu asupra drepturilor persoanelor vizate. Politica de confidențialitate ar trebui să fie clară și ar putea servi drept una din porțile de acces către paginile, în care utilizatorii își pot exercita drepturile. Acest document ar trebui să prevadă toate drepturile aplicabile. Dacă vreunul dintre ele nu ar fi accesibil din cauza limitărilor legale sau tehnice, acest lucru ar trebui explicat astfel încât utilizatorii să fie informați în mod corespunzător. Înțelegerea limitărilor operațiunilor de prelucrare, fie din cauza bazei lor, fie a garanțiilor adoptate de operatori, este utilă nu doar pentru utilizatori. Aceasta limitează, de asemenea, cazurile în care un furnizor de platformă de comunicare socială trebuie să explice de ce nu poate respecta o solicitare de drepturi ale persoanei vizate primită din partea utilizatorilor.

Agitarea - Ascuns la vedere (Lista de verificare 4.3.2 din Anexa I)

153. Capacitatea utilizatorilor de a ajunge la locul, în care își exercită dreptul, poate fi afectată și de vizibilitatea slabă a informațiilor sau linkurilor conexe, fiind folosit modelul de interfață înșelătoare ***Ascuns la vedere.***

Exemplul 49: În punctul situat sub subtitlul „dreptul de acces" din politica de confidențialitate se explică că utilizatorii au dreptul la informare în temeiul articolului 15 alineatul (1) din RGPD. Cu toate acestea, se menționează doar posibilitatea utilizatorilor de a primi o copie a datelor lor cu caracter personal. Nu există un link direct vizibil pentru exercitarea componentei de copiere a dreptului de acces conform articolului 15 alineatul (3) din RGPD. Mai degrabă, sunt ușor accentuate primele trei cuvinte din „Puteți avea o copie a datelor dvs. cu caracter personal". Când treceți cursorul peste aceste cuvinte cu mouse-ul, apare o casetă mică cu un link către setări.

154. Completând secțiunea anterioară, orice mijloc creat de operator pentru exercitarea drepturilor ar trebui să fie ușor accesibil. Această regulă nu poate fi subestimată. O acțiune a operatorului, astfel cum este descrisă mai sus, poate fi percepută doar ca un efort de a împiedica exercitarea drepturilor de către utilizatori, ceea ce încalcă articolul 12 alineatul (2) din RGPD. Operatorii, indiferent de considerentele lor, nu ar trebui să inhibe o astfel de solicitare. După o examinare mai atentă a unui caz specific, o autoritate de supraveghere ar putea stabili că astfel este încălcat RGPD, pentru care operatorul este sancționat.

Schimbător - Interfața incoerentă (Lista de verificare 4.5.3 din Anexa I)

Exemplul 50: Platforma de comunicare socială oferă diferite versiuni (desktop, aplicație, browser mobil). În fiecare versiune, setările (care duc la acces/obiecție etc.) sunt afișate cu un simbol diferit, lăsând utilizatorii care trec de la o versiune la alta confuzi.

155. Întâlnind interfețe pe diferite dispozitive, care transmit aceeași informație prin diferiți semnificanți vizuali, este posibil ca utilizatorii să cheltuiască mai mult timp sau să întâmpine dificultăți în încercarea de a găsi instrumentele de control, pe care le cunosc de pe un dispozitiv pe altul. În exemplul de mai sus, sunt utilizate diferite simboluri sau pictograme, prin care utilizatorii sunt direcționați către setări. Faptul că astfel utilizatorii sunt confuzi ar putea fi considerat contrar facilitării exercitării drepturilor persoanelor vizate, astfel cum este menționat la articolul 12 alineatul (2) din RGPD.

Obstrucționarea - Mai lungă decât este necesar (Lista de verificare 4.4.2 din Anexa I)

156. În sfârșit, orice încercare de a face exercitarea unui drept ***Mai lungă decât este necesar*** poate fi considerată contrară prevederilor RGPD.

Exemplul 51: Când utilizatorii decid să șteargă numele și locul liceului lor sau referința la un eveniment, la care au participat și pe care l-au partajat, apare o a doua fereastră, în care se solicită confirmarea alegerii *(„Într-adevăr vrei să faci aceasta? De ce?").*

157. În mod similar cu numărul de straturi dintr-o politică de confidențialitate (cazul de utilizare 2a) și numărul de pași spre o setare sau de modificare a unei setări (cazul de utilizare 3b), numărul de pași sau clicuri, pe care utilizatorii trebuie să le facă pentru a-și exercita un drept, nu ar trebui să fi excesiv. Aceasta depinde, desigur, de complexitatea operațiunilor efectuate de operator, luând în considerare contextul specific. Ar fi însă nerezonabil ca utilizatorii să fie solicitați să efectueze multe acțiuni inutile pentru a încheia exercitarea dreptului lor. De exemplu, utilizatorii

nu ar trebui să fie descurajați prin întrebări suplimentare, cum ar fi dacă doresc cu adevărat să își exercite acest drept sau care sunt motivele unei astfel de solicitări. În majoritatea cazurilor, aceștia ar trebui să își poată exercita doar dreptul lor, fără ca motivația lor să fie pusă în discuție. Astfel de practici, prezentate în exemplul de mai sus, pot fi considerate contrare articolului 12 alineatul (2) din RGPD, deoarece operatorul împiedică exercitarea drepturilor prin pași inutili. Desigur, aceasta nu împiedică operatorul să primească feedback adresând ulterior întrebări suplimentare cu scopul de a îmbunătăți serviciul. Dacă această întrebare este adresată mai târziu, răspunsul la aceasta ar depinde doar de voința utilizatorilor și nu ar fi confundat cu o cerință de exercitare a unui drept.

d. Cele mai bune practici

Formularul de exercitare a drepturilor: pentru a facilita exercitarea de către utilizatori a drepturilor lor prevăzute în RGPD, furnizați un formular dedicat care să ajute utilizatorii să-și înțeleagă drepturile și care să-i îndrume să îndeplinească acest tip de solicitări.

Comenzi rapide: găsiți definiția în cazul de utilizare 1 (p. 22) (de exemplu, *furnizați un link către ștergerea contului din contul utilizatorului*).

Formulări coerente: găsiți definiția în cazul de utilizare 1 (p. 22).

Prezentarea definițiilor: găsiți definiția în cazul de utilizare 1 (p. 22).

Utilizarea exemplelor: găsiți definiția în cazul de utilizare 1 (p. 22).

Navigare lipicioasă: găsiți definiția în cazul de utilizare 2a (p. 28).

Explicarea consecințelor: găsiți definiția în cazul de utilizare 2c (p. 32).

Consecvența între dispozitive: găsiți definiția în cazul de utilizare 3a (p. 39).

Directoriul de protecție a datelor: găsiți definiția în cazul de utilizare 3b (p. 45).

Relația controalelor de protecție a datelor: găsiți definiția în cazul de utilizare 3b (p. 45).

3.5 Adio: închiderea unui cont pe platforma de comunicare socială

Cazul de utilizare 5: suspendarea contului/ștergerea tuturor datelor cu caracter personal

a. Descrierea contextului și a prevederilor legale relevante

158. Sfârșitul ciclului de viață al unui cont este situația în care utilizatorii decid să părăsească rețeaua de socializare. În această situație, de obicei utilizatorii decid să părăsească platforma de comunicare socială definitiv. Cu toate acestea, deseori există și opțiunea de a dezactiva contul doar temporar și de a suspenda deservirea. Implicațiile legale ale ambelor decizii diferă și sunt descrise mai jos.

i. Ștergerea permanentă a contului

159. Decizia de a părăsi definitiv platforma de comunicare socială este însoțită de dreptul la ștergere prevăzut la articolul 17 alineatul (1) litera (a) din RGPD. În acest context, cuvântul „deletion” (ștergere) este folosit mai des decât erasure (ștergere).

160. Cuvântul „erasure” nu este definit legal în articolul 17 din RGPD și este menționat doar ca formă de prelucrare în articolul 4 alineatul (2) din RGPD. Cuvântul „erasure” poate fi înțeles în general ca o imposibilitate (de fapt) de a accesa informațiile despre o persoană vizată incluse anterior în datele care urmează să fie șterse. După ștergere (erasure), nimeni nu trebuie să mai poată accesa informațiile în cauză fără un efort disproporționat.

161. Anonimizarea este o altă modalitate de a șterge definitiv relația cu o persoană. Cu alte cuvinte, utilizarea tehnicilor de anonimizare are scopul de a se asigura că persoana vizată nu mai poate fi identificată. Anonimizarea înseamnă, de asemenea, că principiile legislației privind protecția datelor, cum ar fi principiul limitării scopului, nu mai sunt aplicabile (a se vedea Considerentul 26, frazele 4 și 5).

162. Conform articolului 12 alineatul (2) din RGPD, operatorul va facilita exercitarea drepturilor persoanelor vizate în temeiul articolelor 15-22. În conformitate cu această cerință, nu pot fi create obstacole substanțiale sau formale în afirmarea drepturilor persoanelor vizate. Prin urmare, dacă exercitarea dreptului de ștergere este complicată fără un motiv real, aceasta constituie o încălcare a RGPD. Deși există un motiv valabil pentru ca furnizorii platformelor de comunicare socială să explice în mod obiectiv consecințele, cum ar fi ștergerea tuturor datelor cu caracter personal și să solicite persoanelor vizate să confirme această alegere,[73] obstacolele inutile trebuie, de asemenea, evitate în acest caz de utilizare. Astfel rezultă, de exemplu, că orice perioadă de grație între solicitările de ștergere a contului utilizatorului și ștergerea efectivă a acestuia trebuie să fie proporțională. Respectiv, această perioadă de timp ar putea să nu fie prea lungă, ținând cont de motivele tehnice ale întârzierilor de la ștergerea imediată, precum și perioada scurtă de timp pentru (re)examinarea de către utilizator a deciziei de a-și șterge contul după declanșarea procesului de ștergere a contului. În timp ce dorința liberă a utilizatorului de a se răzgândi trebuie respectată, este posibil ca furnizorii platformelor de comunicare socială să nu încerce să declanșeze o astfel de schimbare de părere încurajând utilizatorii să revină, ceea ce ar constitui, de asemenea, un obstacol în realizarea dreptului utilizatorului la ștergere. În perioada de grație, procesul de ștergere ar putea fi întrerupt în unele cazuri, de exemplu atunci când utilizatorul se loghează din nou. Dacă ștergerea nu poate fi finalizată, utilizatorul trebuie să fie informat cum se finalizează ștergerea.

163. Decizia de a părăsi platforma de comunicare socială declanșează consecințele ștergerii, astfel cum prevede articolul 17 alineatul (1) din RGPD. Dacă o persoană vizată solicită ștergerea contului respectiv, operatorul platformei de comunicare socială trebuie să șteargă datele. Cu toate acestea, unele date pot rămâne pe platformă o anumită perioadă de timp dacă este aplicabil articolul 17 alienatul (3) din RGPD. Excepțiile enumerate la articolul 17 alineatul (3) din RGPD trebuie interpretate în mod restrâns și se aplică doar în cazurile menționate în mod explicit în această parte a dispoziției. Orice excepție, pe care se bazează un operator în temeiul articolului 17 alineatul (3) din RGPD, și păstrarea datelor respective trebuie să fie justificată de operator, de exemplu prin faptul că conform legislației naționale operatorul este obligat să stocheze informații legate de persoana vizată din considerente imperative de interes public, pentru exercitarea dreptului fundamental la libertatea de exprimare și informare sau din considerente fiscale. Este clar că aceste date rămase ar trebui să fie stocate doar intern de către furnizorul platformei de comunicare socială și nu ar trebui să fie vizibile public pentru alți utilizatori. Cu toate acestea, o derogare în temeiul articolului 17 alineatul (3) din RGPD nu permite în niciun caz furnizorului

[73] Spre deosebire de celelalte drepturi ale persoanelor vizate, a se vedea p. 154 de mai sus.

platformei de comunicare socială să păstreze statutul activ al contului persoanei vizate mai mult decât intenționează utilizatorul după solicitarea sa de ștergere.

164. Independent de o solicitare de ștergere a contului, dacă utilizatorii își retrag consimțământul în temeiul articolului 7 alineatul (3) din RGPD, prelucrarea datelor lor acordate pe baza consimțământului conform articolului 6 alineatul (1) litera (a) din RGPD nu mai poate avea loc. În acest caz, alte operațiuni de prelucrare, în care furnizorul platformei de comunicare socială se bazează pe alte temeiuri juridice în conformitate cu articolul 6 alineatul (1) din RGPD, în anumite circumstanțe, încă mai pot avea loc.

165. Dacă totuși utilizatorii solicită ștergerea contului, nu ar trebui să aibă loc nicio prelucrare ulterioară, indiferent de temeiul juridic care stă la bază, cu excepția cazului în care se aplică una din excepțiile enumerate în mod exhaustiv la articolul 17 alineatul (3) din RGPD. În acest context, este important să rețineți că păstrarea datelor se limitează la stocarea minimă menționată mai sus.

166. Conform articolului 25 alineatul (1) din RGPD, operatorul va implementa măsuri tehnice și organizatorice adecvate pentru a pune în aplicare principiile de protecție a datelor. Conform Orientărilor 04/2019 privind articolul 25 – Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, măsurile tehnice și organizatorice pot fi înțelese în sens larg ca orice metodă sau mijloc, pe care un operator le poate folosi în prelucrare. A fi adecvate înseamnă că măsurile ar trebui să fie corespunzătoare pentru atingerea scopului vizat, adică trebuie să implementeze în mod eficient principiile de protecție a datelor. Astfel cerința de adecvare este strâns legată de cerința de eficacitate.[74]

ii. Suspendarea contului

167. Alternativ, utilizatorilor li se oferă posibilitatea de a-și dezactiva temporar contul, ceea ce le permite să părăsească rețeaua de socializare pe o perioadă de timp fără a-și șterge contul definitiv. În acest caz, contul este dezactivat temporar, iar profilul, pozele, comentariile și reacțiile vor fi ascunse până când utilizatorii își vor reactiva contul, de exemplu printr-o logare nouă. Principala diferență față de ștergere este că datele cu caracter personal rămân în rețeaua de socializare și contul poate fi reactivat de către utilizatori fără să se înregistreze din nou.

168. Utilizatorii, care încep procesul de ștergere a contului, pot afla că opțiunea de suspendare a contului este preselectată. Deși ar putea fi util pentru utilizatorii, care nu ar dori să-și șteargă definitiv contul, să li se ofere o opțiune de suspendare, furnizorii platformelor de comunicare socială ar putea să nu ofere utilizatorilor astfel de perioade de dezactivare, în special prin preselectare. Oferind această posibilitate de dezactivare, furnizorul platformei de comunicare socială satisface așteptările rezonabile ale utilizatorilor că datele lor cu caracter personal nu vor fi prelucrate în același mod ca în timpul utilizării active a contului și că furnizorul platformei de comunicare socială va reduce prelucrarea datelor la un nivel strict necesar în această perioadă. Utilizatorii s-ar putea aștepta ca datele lor să nu fie prelucrate deloc sau să nu fie prelucrate integral în anumite scopuri, de exemplu prin îmbunătățirea profilului lor cu vizite pe site-uri web terțe, care utilizează instrumente corespunzătoare de direcționare sau de urmărire. Pe lângă informarea utilizatorilor într-un mod transparent despre consecințele suspendării contului lor, orice prelucrare a datelor în timpul acestei suspendări trebuie să se bazeze pe un temei juridic valabil.

[74] Orientările 04/2019 privind articolul 25 – Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, pag. 6, p. 8.

169. În ceea ce privește prelucrarea datelor, care se bazează pe consimțământ în conformitate cu articolul 6 alineatul (1) litera (a) din RGPD, furnizorul platformei de comunicare socială trebuie să ia în considerare faptul că utilizatorii consideră ca consimțământul, pe care îl acordă în timpul înregistrării sau ulterior, se refere doar la prelucrarea datelor în timpul utilizării active a contului. CEPD recunoaște că termenul consimțământului depinde de context, de domeniul de aplicare al consimțământului inițial și de așteptările persoanei vizate.[75] Deși RGPD nu prevede o limită de timp specifică a termenului consimțământului, valabilitatea acestuia depinde de context, domeniul de aplicare al consimțământului inițial și așteptările persoanei vizate.[76] Dacă operațiunile de prelucrare se schimbă sau evoluează considerabil, atunci consimțământul inițial nu mai este valabil.[77] CEPD recomandă, ca cea mai bună practică, ca consimțământul să fie reîmprospătat la intervale corespunzătoare.[78] Furnizarea tuturor informațiilor din nou contribuie la asigurarea informării corespunzătoare a persoanelor vizate cum sunt utilizate datele lor și cum își exercită drepturile.[79] Dacă acesta este cazul, consimțământul trebuie obținut din nou[80] și toate cerințele corespunzătoare trebuie să fie îndeplinite.

170. Așteptările rezonabile ale persoanei vizate ar trebui, de asemenea, luate în cont atunci când se aplică articolul 6 alineatul (1) litera (f) din RGPD (a se vedea Considerentul 47). În special, trebuie să se ia în considerare dacă persoana vizată se poate aștepta în mod rezonabil la momentul și în contextul colectării datelor cu caracter personal că prelucrarea în acest scop ar putea avea loc. Cu toate acestea, utilizatorii se așteaptă în mod rezonabil ca în timpul dezactivării să fie prelucrate doar datele necesare. De asemenea, furnizorul platformei de comunicare socială se poate referi la interesul legitim doar dacă sunt îndepliniți toți pașii testului interesului legitim, inclusiv exercițiul de echilibrare. Orice interes primordial sau drepturi și libertăți fundamentale ale persoanei vizate ar trebui evaluate de la caz la caz.

171. Deoarece obligațiile contractuale sunt, de asemenea, suspendate în mare măsură în timpul dezactivării, operațiunile de prelucrare a datelor sunt necesare doar într-o măsură limitată în conformitate cu articolul 6 alineatul (1) litera (b) din RGPD. Poate fi considerată necesară doar stocarea datelor utilizatorilor până la decizia finală de reactivare sau ștergere.
172. Având în vedere faptul că toate prelucrările anterioare ale datelor erau legate de un cont activ, în timpul perioadei de dezactivare trebuie prezentate informații suplimentare despre prelucrare, dacă nu sunt incluse în informațiile generale conform articolelor 13 și 14 din RGPD. Aceasta decurge din principiile transparenței și echității prevăzute la articolul 5 alineatul (1) litera (a) din RGPD și din principiul limitării scopului prevăzut la articolul 5 alineatul (1) litera (b) din RGPD. Prelucrarea datelor în urma dezactivării trebuie să fie însoțită de informații suficiente ale persoanei vizate. Prin urmare, furnizorul platformei de comunicare socială va informa în mod cuprinzător utilizatorii despre prelucrarea reală și scopurile acesteia în timpul suspendării și, dacă este necesar, va obține un consimțământ nou.

b. Modele de interfață înșelătoare
i. Modele bazate pe conținut
Supraîncărcarea - Labirint de confidențialitate (Lista de verificare 4.1.2 din Anexa I)

[75] Orientările 5/2020 privind consimțământul, p. 110.
[76] Orientările 5/2020 privind consimțământul, p. 110.
[77] Orientările 5/2020 privind consimțământul, p. 110.
[78] Orientările 5/2020 privind consimțământul, p. 111.
[79] Orientările 5/2020 privind consimțământul, p. 111.
[80] Orientările 5/2020 privind consimțământul, p. 110.

173. În acest caz de utilizare, modelul de interfață înșelătoare ***Labirint de confidențialitate*** apare atunci când utilizatorii se confruntă cu o avalanșă de informații răspândite în mai multe locuri, pentru a-i împiedica să-și șteargă contul, astfel cum este prezentat în exemplul de mai jos. Deși unele informații suplimentare înainte de acest pas sunt destul de dezirabile, cum ar fi indicația că utilizatorii au acces la datele lor înainte de ștergere, informațiile generale irelevante nu mai sunt esențiale. Utilizatorii nu ar trebui să întârzie în mod inutil acest pas.

Exemplul 52: Utilizatorii caută dreptul la ștergere. Trebuie să apeleze setările contului, să deschidă un submeniu numit „confidențialitate" și trebuie să ruleze până la capăt pentru a găsi un link pentru ștergerea contului.

Agitarea - Dirijarea emoțională (Lista de verificare 4.3.1 din Anexa I)

Exemplul 53: La primul nivel de informare, informațiile sunt oferite utilizatorilor subliniind doar consecințele negative și descurajatoare ale ștergerii conturilor lor (de exemplu, *„vei pierde totul pentru totdeauna"* sau *„prietenii tăi te vor uita"*).

174. În timp ce regretul pentru încetarea relației contractuale pare corespunzător din punct de vedere social și respectiv dificil de sesizat din punct de vedere juridic, o descriere cuprinzătoare a consecințelor negative presupuse cauzate de ștergerea contului de către utilizatori constituie un impediment pentru realizarea deciziei lor, dacă este cazul exemplificat mai sus, în care se joacă cu frica de a rata ceva important (FOMO), făcând alegerea de a-și șterge contul să pară deosebit de pedepsitoare. O astfel de ***Dirijare emoțională***, care amenință utilizatorii că vor rămâne singuri, dacă își vor șterge contul, este o încălcare a obligației de a facilita exercitarea drepturilor persoanelor vizate prevăzute la articolul 12 alineatul (2) din RGPD, precum și a principiului echității prevăzut la articolul 5 alineatul (1) litera (a) din RGPD.

Lăsată în întuneric - Formulare sau informații ambigue (Lista de verificare 4.6.3 din Anexa I)

175. În contextul ștergerii unui cont în rețeaua de socializare, utilizatorii se pot confrunta și cu modelul de interfață înșelătoare ***Formulare sau informații ambigue***, astfel cum este prezentat în exemplul următor.

Exemplul 54: Când utilizatorii își șterg contul, aceștia nu sunt informați cât timp vor fi păstrate datele lor după ștergerea contului. Și mai rău, în tot procesul de ștergere, utilizatorii nu sunt informați despre faptul că *„unele date cu caracter personal"* ar putea fi stocate chiar și după ștergerea contului. Ei trebuie să caute informațiile singuri, în diferite surse de informații disponibile.
Exemplul 55: Utilizatorii își pot șterge contul doar prin linkurile numite *„La revedere"* sau *„Dezactivează"* disponibile în contul lor.

176. În aceste exemple, formularea folosită pentru linkuri nu sugerează clar faptul că utilizatorii vor fi redirecționați către procesul de ștergere a contului. În schimb, utilizatorii s-ar putea gândi la alte funcționalități, cum ar fi delogarea până la următoarea utilizare sau dezactivarea contului lor. Ca atare, acest lucru ar putea fi interpretat ca o încălcare a articolului 12 alineatul (2) din RGPD, care prevede că operatorii de date ar trebui să faciliteze exercitarea drepturilor persoanelor vizate. Creând confuzie cu privire la așteptările utilizatorilor legate de link, platforma de comunicare socială nu facilitează pe deplin exercitarea dreptului la ștergere. Utilizarea unor

astfel de cuvinte echivoce în alt context ar putea încălca prevederile RGPD, cum ar fi articolul 7 din RGPD și respectiv articolul 17 alineatul (1) litera (b) din RGPD.

ii. Modele bazate pe interfață
Omiterea - Comoditatea înșelătoare (Lista de verificare 4.2.1 din Anexa I)

Exemplul 56: În procesul de ștergere a contului, utilizatorilor li se oferă două opțiuni la alegere: Să-și șteargă contul sau să-l suspende. În mod implicit, este selectată opțiunea de suspendare.

177. Dacă este aleasă prima opțiune de ștergere a contului, sunt șterse toate datele cu caracter personal ale utilizatorilor, ceea ce înseamnă că platforma de comunicare socială nu mai deține aceste date, cu excepția datelor, care sunt obiectul excepției temporare prevăzute la articolul 17 alineatul (3) din RGPD. În schimb, cu a doua opțiune de suspendare a contului, toate datele cu caracter personal sunt păstrate și potențial procesate de furnizorul platformei de comunicare socială. Aceasta neapărat creează mai multe riscuri pentru persoana vizată, de exemplu dacă are loc o încălcare a securității datelor cu caracter personal și datele încă stocate de furnizorul platformei de comunicare socială sunt accesate, dublate, transferate sau prelucrate în alt mod. Selectarea implicită a opțiunii de suspendare probabil va determina utilizatorii să o selecteze în loc să-și șteargă contul după cum s-a intenționat inițial. Prin urmare, practica prezentată în acest exemplu poate fi considerată o încălcare a articolului 12 alineatul (2) din RGPD, deoarece în acest caz nu facilitează exercitarea dreptului la ștergere și chiar încearcă să-i îndepărteze pe utilizatori de la exercitarea acestuia.

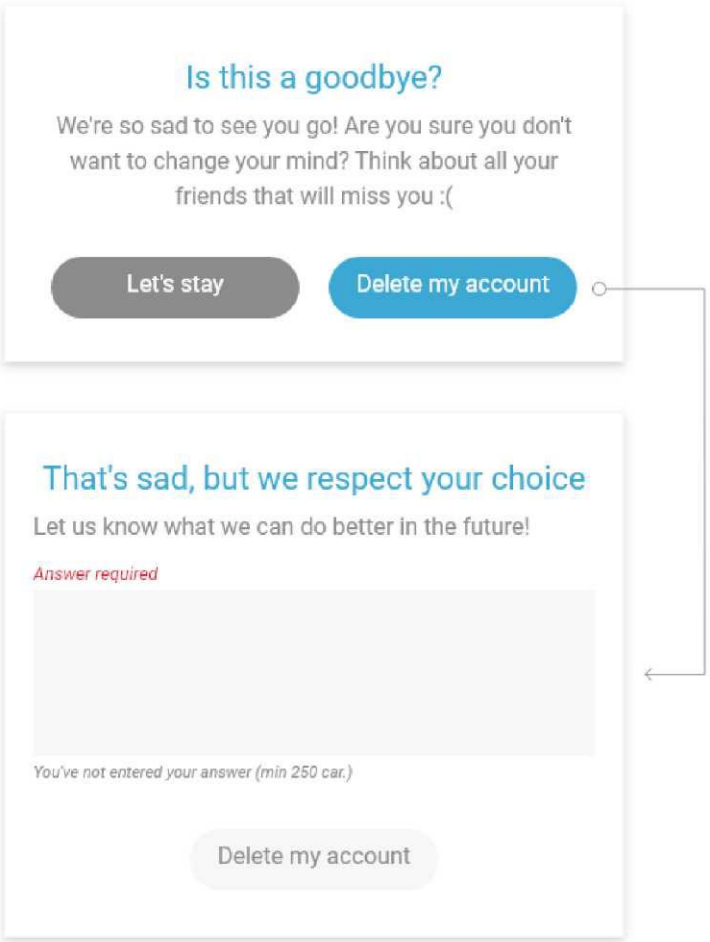
Omiterea - Uită-te acolo (Lista de verificare 4.2.2 din Anexa I)
178. Oferirea utilizatorilor a unui mijloc pentru a-și descărca datele atunci când își exprimă dorința de a-și șterge contul poate fi o opțiune relevantă care trebuie oferită. Într-adevăr, odată ce contul lor este șters, datele lor cu caracter personal vor fi șterse peste o anumită perioadă de timp. Aceasta înseamnă că, dacă nu obțin o copie a datelor lor cu caracter personal, le vor pierde complet. Cu toate acestea, prezentarea acestei opțiuni poate constitui un model de interfață înșelătoare ***Uită-te acolo***, astfel cum este prezentat în exemplul următor.

Exemplul 57: După ce fac clic pe „Șterge contul meu”, utilizatorilor li se prezintă opțiunea de a-și descărca datele, implementată ca drept la portabilitate, înainte de a șterge contul. Când fac clic pentru a-și descărca informațiile, utilizatorii sunt redirecționați către o pagină cu informații despre descărcare. Cu toate acestea, odată ce utilizatorii au ales care date anume și cum să le descarce, aceștia nu sunt redirecționați către procesul de ștergere.

179. În exemplul de mai sus, s-ar putea considera că modul în care este implementată opțiunea de descărcare nu facilitează exercitarea dreptului la ștergere asociat cu ștergerea contului. Într-adevăr, odată ce utilizatorii și-au descărcat datele, aceștia nu sunt readuși la procesul de ștergere. Pentru a reveni la el, vor trebui să facă clic de mai multe ori. Complicarea în acest mod a exercitării unui drept încalcă articolul 12 alineatul (2) din RGPD. Mai mult, oferirea unui mijloc de a ajunge cu ușurință la procesul de ștergere după descărcarea datelor este o funcție simplă de implementat. În această privință, s-ar putea considera că obligația de a pune în aplicare măsuri tehnice și organizatorice adecvate, care sunt prevăzute la articolul 25 alineatul (1) din RGPD, nu este îndeplinită, deoarece utilizatorii nu pot continua să își exercite drepturile în mod efectiv.

Obstrucționarea - Mai lungă decât este necesar (Lista de verificare 4.4.2 din Anexa I)

180. După cum este prezentat mai detaliat în cazul de utilizare 4, orice pași irelevanți adăugați la procesul de exercitare a unui drept ar putea contraveni prevederilor RGPD, în special articolului 12 alineatul (2). Acesta este cazul în care utilizatorii intenționează să-și șteargă contul, deoarece ar interfera cu dreptul la ștergere asociat cu o astfel de solicitare.



E adio?

Ne pare atât de rău că ne părăsești! Ești sigur(ă) că nu te vei răzgândi? Gândește-te la toți prietenii, cărora le vei lipsi :(

Rămân Șterge contul meu

Ne pare rău, dar respectăm alegerea ta

Spune-ne ce putem îmbunătăți în viitor!

Răspunsul este obligatoriu

Nu ai introdus răspunsul tău (min. 250 car.)

Șterge contul meu

Exemplul 58: În acest exemplu, utilizatorii văd mai întâi o casetă de confirmare a ștergerii contului după ce au făcut clic pe linkul sau butonul corespunzător din contul lor. Chiar dacă în această

casetă există o ***Dirijare emoțională***, acest pas poate fi văzut ca o măsură de securitate pentru ca utilizatorii să nu-și șteargă contul făcând un clic greșit în contul lor. Cu toate acestea, atunci când utilizatorii fac clic pe butonul „Șterge contul meu", apare o a doua casetă, care solicită să descrie textual motivul, pentru care doresc să șteargă contul. Atât timp cât nu au introdus ceva în casetă, nu își pot șterge contul, deoarece butonul asociat acțiunii nu este activ și este de culoare gri. Din cauza acestei practici ștergerea unui cont este ***Mai lungă decât este necesar***, mai ales că solicitarea utilizatorilor să introducă un text în care să explice de ce doresc să șteargă contul necesită efort și timp suplimentar și nu ar trebui să fie obligatorie pentru ștergerea contului.

181. După cum s-a menționat anterior, atunci când își exercită un drept, utilizatorii nu ar trebui să fie nevoiți să răspundă la întrebări, care nu sunt legate de exercitarea dreptului în sine. Necesitatea de a-și justifica alegerea sau de a explica cum platforma de comunicare socială ar trebui să se îmbunătățească nu se încadrează în această categorie. În exemplul prezentat, această problemă este accentuată, deoarece persoanele vizate trebuie să scrie un răspuns în loc să selecteze o propunere există dintr-o listă prestabilită, ceea ce este și mai împovărător pentru ei, deoarece răspunsul trebuie creat. Din cauza unui astfel de mecanism unii utilizatori ar putea să nu-și exercite dreptul în totalitate dacă nu le este suficient de comod să scrie un răspuns.

182. Totuși, aceasta nu înseamnă că o listă de răspunsuri prestabilite este un pas acceptabil de adăugat la procesul de ștergere a contului cuiva. Acesta este cazul în special dacă aceste răspunsuri sunt asociate cu pași și acțiuni suplimentare impuse utilizatorilor, astfel cum este prezentat în exemplul de mai jos.

Exemplul 59: Furnizorul platformei de comunicare socială cer utilizatorilor să răspundă la o întrebare despre motivele pentru care doresc să-și șteargă contul, printr-o selecție de răspunsuri într-un meniu derulant. Utilizatorii consideră că răspunsul la această întrebare (aparent) le permite să efectueze acțiunea pe care o doresc, adică să șteargă contul. Odată ce este selectat un răspuns, apare o fereastră pop-up, care arată utilizatorilor o modalitate de a soluționa problema menționată în răspunsul lor. Prin urmare, din cauza procesului întrebare- răspuns, ștergerea contului utilizatorilor durează mai mult timp.

183. Pe lângă faptul că ștergerea contului este deosebit de lungă, un mecanism ***Uită-te acolo*** are scopul să distragă utilizatorii de la ștergerea contului, oferind o soluție de descurajare a părăsirii platformei de comunicare socială. Aceasta împiedică exercitarea dreptului la ștergere și respectiv descurajează persoanele vizate să-și exercite dreptul.

Schimbător - Decontextualizarea (Lista de verificare 4.5.2 din Anexa I)

184. În cele din urmă, modelul de interfață înșelătoare ***Decontextualizare*** poate fi găsit și atunci când utilizatorii doresc să-și șteargă contul.

Exemplul 60: Pe platforma de comunicare socială XY, linkul de dezactivare sau ștergere a contului se găsește în fila *„Datele tale XY"*.

185. În general, termenii folosiți pentru a întitula o pagină sau o secțiune a platformei de comunicare socială dedicată aspectelor de protecție a datelor ar trebui să reflecte clar tipul de informații sau control inclus. Este puțin probabil ca utilizatorii medii să vadă legătura dintre acțiunile de ștergere sau dezactivare a contului lor și gestionarea datelor. În exemplul de mai sus, utilizatorii nu s-ar aștepta la funcționalitatea de ștergere a contului lor într-o pagină numită

„Informațiile tale XY”, care face aluzie la vizualizarea și eventual revizuirea informațiilor cuiva. În schimb, ar căuta o pagină „Informații generale” sau o pagină „Șterge contul meu”. Prin urmare, din punctul de vedere al utilizatorilor, opțiunile sunt plasate într-o setare, care se află în afara contextului și nu corespunde așteptărilor utilizatorilor.

Exemplul 61: Fila pentru ștergerea unui cont se găsește în secțiunea *„șterge o funcție a contului tău”.*

186. În acest exemplu, utilizatorii ar putea înțelege din greșeală titlul secțiunii ca fiind locul unde pot ajusta funcții individual. Prin urmare, utilizatorii nu s-ar aștepta să găsească acolo opțiunea de ștergere a contului în întregime. Din această cauză utilizatorilor le este dificil să găsească linkul corect pentru ștergerea întregului cont.

187. Modelul de interfață înșelătoare ***Decontextualizare***, astfel cum este prezentat în cele două exemple de mai sus, ar putea fi considerat o încălcare a articolului 12 alineatul (2) din RGPD, având în vedere că utilizatorii ar întâmpina dificultăți să găsească locul potrivit în care să-și exercite dreptul la ștergere.

c. Cele mai bune practici

Formulări coerente: găsiți definiția în cazul de utilizare 1 (p. 22).

Prezentarea definițiilor: găsiți definiția în cazul de utilizare 1 (p. 22).

Utilizarea exemplelor: găsiți definiția în cazul de utilizare 1 (p. 22).

Explicarea consecințelor: găsiți definiția în cazul de utilizare 2c (p. 32).

Consecvența între dispozitive: găsiți definiția în cazul de utilizare 3a (p. 39).

Pentru Comitetul european pentru protecția datelor
Președintele

(Andrea Jelinek)

4 ANEXA I: LISTA CATEGORIILOR ȘI TIPURILOR DE MODELE DE INTRERFAȚĂ ÎNȘELĂTOARE

Următoarea listă oferă o prezentare generală a categoriilor de modele de interfață înșelătoare și a tipurilor de modele de interfață înșelătoare din fiecare categorie. De asemenea, sunt enumerate prevederile RGPD cele mai relevante pentru tipurile de modele de interfață înșelătoare. Cititorii ar trebui să țină cont de faptul că, după cum s-a menționat mai sus, principiul prelucrării echitabile prevăzut la articolul 5 alineatul (1) litera (a) din RGPD este un punct de plecare pentru evaluarea existenței modelelor de interfață înșelătoare. Acesta are o funcție tip umbrelă și toate modelele de interfață înșelătoare nu ar fi conforme cu acesta, chiar dacă ar fi conforme cu alte principii de protecție a datelor.[81]
Pentru fiecare model, lista mai conține numărul exemplului și cazului de utilizare corespunzător (CU) pentru ca cititorii să le găsească rapid.
Este important de menționat că această listă nu este exhaustivă și că, prin urmare, modelele de interfață înșelătoare pot apărea și în cazuri de utilizare, care nu conțin un exemplu pentru acest tip de model de interfață înșelătoare în textul Orientărilor.

4.1 Supraîncărcarea

Îngroparea utilizatorilor sub o masă de solicitări, informații, opțiuni sau posibilități pentru a-i descuraja să meargă mai departe și a-i determina să păstreze sau să accepte anumite practici legate de date.

4.1.1 Solicitare continuă[82]

Determinarea utilizatorilor să furnizeze mai multe date cu caracter personal decât este necesar în scopul prelucrării sau să fie de acord cu o altă utilizare a datelor lor, solicitând în mod repetat utilizatorilor să prezinte date sau să consimtă cu un scop de prelucrare nou. Astfel de solicitări repetitive pot apărea prin unul sau mai multe dispozitive. Este posibil ca în cele din urmă utilizatorii să cedeze, fiind obosiți de a fi nevoiți să refuze cererea de fiecare dată când folosesc platforma care îi deranjează în procesul de utilizare a acesteia.

Prevederile relevante ale RGPD:
- *Limitarea scopului: articolul 5 alineatul (1) litera (b);*
- *Consimțământul liber: articolul 7* coroborat cu articolul 4 alineatul (11);
- *Consimțământul specific: articolul 7 alineatul (2).*

Exemple: CU 1 exemplele 1, 2; CU 3a exemplul 34 (ilustrare).

4.1.2 Labirintul de confidențialitate

Atunci când utilizatorii doresc să obțină anumite informații sau să utilizeze un anumit control sau să exercite un drept al persoanei vizate, le este deosebit de dificil să le găsească, deoarece trebuie să navigheze prin prea multe pagini pentru a obține informațiile sau controlul relevant, fără a

[81] A se vedea mai sunt p. 9 din Orientări.
[82] Acest model este strâns legat de un tip de model numit „Sâcâială ” găsit în literatura academică.

avea o prezentare generală cuprinzătoare și exhaustivă disponibilă. Utilizatorii ar putea să renunțe sau să rateze informațiile sau controlul relevant.

Prevederile relevante ale RGPD:
- Principiul transparenței: articolul 5 alineatul (1) litera (a) și informații transparente: articolul 12 alineatul (1);
- Principiul echității: articolul 5 alineatul (1) litera (a);
- Informații ușor accesibile: articolul 12 alineatul (1);
- Acces simplu la drepturi: Articolul 12 (2);
- Consimțământ informat: articolul 7 coroborat cu articolul 4 alineatul (11).

Exemple: CU 2a exemplul 17; CU 3a exemplul 33; CU 3b exemplul 37; CU 4 exemplele 47 (ilustrare) și 48 (ilustrare); CU 5 exemplul 51.

4.1.3 Prea multe opțiuni

Oferirea utilizatorilor a (prea) multor opțiuni la alegere. Din cauza numărului de opțiuni, utilizatorii nu pot face nicio alegere sau pot trece cu vederea unele setări, mai ales dacă informațiile nu sunt disponibile. În cele din urmă îi poate determina să renunțe sau să rateze setările preferințelor sau drepturilor lor de protecție a datelor.

Prevederile relevante ale RGPD:
- Principiile transparenței și echității: articolul 5 alineatul (1) litera (a);
- Informații transparente: articolul 12 alineatul (1).

Exemplu: CU 3b exemplul 35.

4.2 Omiterea

Proiectarea interfeței de utilizator sau a călătoriei utilizatorului astfel încât utilizatorii să uite sau să nu se gândească la toate sau la unele aspecte ale protecției datelor.

4.2.1 Comoditate înșelătoare

În mod implicit, sunt activate majoritatea funcțiilor și opțiunilor invazive de date. Bazându-se pe efectul implicit, care determină utilizatorii să păstreze o opțiune preselectată, este puțin probabil ca utilizatorii să o schimbe, chiar dacă au posibilitatea.

Prevederile relevante ale RGPD:
- Protecția datelor din momentul proiectării și în mod implicit: articolul 25 alineatul (1);
- Consimțământul: articolul 4 alineatul (11) și articolul 6 (practică ilegală de a activa o prelucrare bazată pe consimțământ în mod implicit).

Exemple: CU 1 exemplul 9; CU 3b exemplele 39 şi 40 (ilustrare); CU 5 exemplul 55.

4.2.2 Uită-te acolo

O acțiune sau o informație legată de protecția datelor este pusă într-o poziție de competiție cu un alt element care poate fi legat sau nu de protecția datelor. Atunci când utilizatorii aleg această

opțiune, care distrage atenția, este probabil să uite de cealaltă, chiar dacă ea a fost intenția lor principală.

Prevederile relevante ale RGPD:
- *Principiile transparenței și echității:* articolul 5 alineatul (1) litera (a);
- *Informații transparente:* articolul 12 alineatul (1);
- *Exercitarea drepturilor:* articolul 12 alineatul (2).

Exemple: CU 2c exemplul 25; CU 3a exemplul 29; CU 5 exemplele 56 și 58.

4.3 Agitarea

Afectarea alegerii, pe care utilizatorii ar face-o, apelând la emoțiile lor sau folosind ghionturi vizuale.

4.3.1 Dirijarea emoțională[83]

Utilizarea formulării sau a elementelor vizuale (cum ar fi stilul, culorile, pozele sau altele) într-un mod care prezintă utilizatorilor informațiile într-o perspectivă extrem de pozitivă, făcându-i pe utilizatori să se simtă bine, în siguranță sau recompensați, sau într-un mod extrem de negativ, făcând utilizatorii să se simtă speriați, vinovați sau pedepsiți. Influențarea stării emoționale a utilizatorilor într-un astfel de mod îi poate determina să facă o acțiune împotriva intereselor lor de protecție a datelor.

Prevederile relevante ale RGPD:
- *Principiile transparenței și echității:* articolul 5 alineatul (1) litera (a);
- *Informații transparente:* articolul 12 alineatul (1);
- *Exercitarea drepturilor:* Articolul 12 alineatul (2);
- *Consimțământul copilului:* articolul 8;
- *Consimțământ informat*: articolul 7 coroborat cu articolul 4 alineatul (11);

Exemple: UC1 exemplele 4, 5, 6; CU 5 exemplul 52.

4.3.2 Ascuns la vedere

Utilizarea unui stil sau tehnici vizuale pentru controalele de protecție a informațiilor sau a datelor, care împing utilizatorii către opțiuni mai puțin restrictive și, prin urmare, mai invazive.

Prevederile relevante ale RGPD:
- *Principiul echității:* articolul 5 alineatul (1) litera (a);
- *Consimțământul liber:* articolul 7 coroborat cu articolul 4 alineatul (11);
- *Informații clare:* articolul 12 alineatul (1);
- *Exercitarea drepturilor:* articolul 12 (2)

[83] Acest model este strâns legat de un tip de model numit *„Jocul cu emoțiile”* găsit, printre altele, în rapoartele organizațiilor interguvernamentale precum Comisia Europeană, Direcția Generală Justiție și Consumatori, Lupiânez-Villanueva, F., Boluda, A. , Bogliacino, F., și alții, *Behavioural study on unfair commercial practices in the digital environment : dark patterns and manipulative personalisation : final report*, Oficiul pentru Publicații al Uniunii Europene, 2022 https://data.europa.eu/doi/10.2838/859030 și OCDE (2022), „Dark commercial patterns”, *Documents de travail de l'OCDE sur l'économie numérique*, nr. 336, Éditions OCDE, Paris, https://doi.org/10.1787/44f5e846-en.

Exemple: UC1 exemplul 8, CU 3a exemplul 34 (ilustrare); CU 3b exemplul 40 (ilustrare); CU 4 exemplul 48.

4.4 Obstrucționarea[84]

Împiedicarea sau blocarea utilizatorilor în procesul lor de obținere a informațiilor sau de gestionare a datelor lor, făcând acțiunea greu sau imposibil de realizat.

4.4.1 Fundătură

În timp ce utilizatorii caută informații sau un control, ajung să nu le găsească, deoarece un link de redirecționare fie nu funcționează, fie nu este disponibil deloc. Utilizatorii nu pot îndeplini această sarcină.

Prevederile relevante ale RGPD:
- *Informații ușor accesibile:* articolul 12 alineatul (1);
- *Exercitarea drepturilor:* articolul 12 (2);
- *Protecția datelor din momentul proiectării și în mod implicit*: articolul 25 alineatul (1).

Exemple: UC1 exemplele 10, 11; CU 2a exemplul 18; CU 3a exemplele 30, 31; CU 4 exemplul 43.

4.4.2 Mai lungă decât este necesar

Atunci când utilizatorii încearcă să activeze un control legat de protecția datelor, călătoria utilizatorului prevede mai mulți pași din partea utilizatorilor, decât numărul de pași necesari pentru activarea opțiunilor invazive de date. Aceasta ar putea să-i descurajeze să activeze un astfel de control.

Prevederile relevante ale RGPD:
- *Informații ușor accesibile:* articolul 12 alineatul (1);
- *Exercitarea drepturilor:* articolul 12 alineatul (2);
- *Dreptul de a se opune:* articolul 21 alineatul (1);
- *Retragerea consimțământului*: articolul 7 alineatul (3);
- *Protecția datelor din momentul proiectării (și în mod implicit):* articolul 25 alineatul (1).

Exemple: CU 1 exemplul 7; CU 3a exemplul 32; CU 4 exemplul 50; CU 5 exemplele 57 (ilustrare) și 58.

4.4.3 Acțiune înșelătoare

O discrepanță între informațiile și acțiunile disponibile utilizatorilor îi determină să facă ceva ce nu intenționează să facă. Diferența dintre ceea ce așteaptă utilizatorii și ceea ce obțin ar putea să-i descurajeze să meargă mai departe.

Prevederile relevante ale RGPD:
- *Informații transparente:* articolul 12 alineatul (1);

[84] Această categorie este strâns legată de strategia numită *„Obstrucționare”* definită și descrisă Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph, and Toombs Austin L. 2018. The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (Montreal QC, Canada) (CHI '18). ACM, New York, NY, USA, articolul 534, 14 pagini. https://doi.org/10.1145/3173574.3174108.

- *Echitatea prelucrării:* articolul 5 alineatul (1) litera (a).
- *Consimțământ informat*: articolul 7 alineatul (2) coroborat cu articolul 4 alineatul (11).

Exemple: CU 1 exemplul 3; CU 3a exemplul 28.

4.5 Schimbător

Proiectul interfeței este instabil și inconsecvent, motiv pentru care utilizatorilor le este dificil să conștientizeze tipul procesării, să facă o alegere corectă cu privire la datele lor și să găsească unde se află diferitele controale.

4.5.1 Lipsa ierarhiei

Informațiile legate de protecția datelor sunt lipsite de ierarhie, din care cauză apar de mai multe ori și sunt prezentate în mai multe moduri. Este posibil ca utilizatorii să fie confuzi de această redundanță și să nu poată înțelege pe deplin cum sunt prelucrate datele lor și cum să exercite controlul asupra acestora.

Prevederile relevante ale RGPD:
- *Informații ușor accesibile:* articolul 12 alineatul (1);
- *Exercitarea drepturilor:* articolul 12 alienatul (2).

Exemple: CU 2a exemplele 13 și 14.

4.5.2 Decontextualizarea

O informație sau un control privind protecția datelor se află pe o pagină, care este în afara contextului. Este puțin probabil ca utilizatorii să găsească informațiile sau controlul, deoarece nu ar fi intuitiv să le caute pe această pagină specifică.

Prevederile relevante ale RGPD:
- *Informații ușor accesibile*: articolul 12 alineatul (1);
- *Informații transparente*: articolul 12 alineatul (1);
- *Exercitarea drepturilor*: articolul 12 alineatul (2).

Exemple: CU 3b exemplele 41, 42; CU 5 exemplele 59 și 60.

4.5.3 Interfață incoerentă

O interfață nu este coerentă în diferite contexte (de exemplu, un meniu legat de protecția datelor nu afișează aceleași elemente pe telefon mobil și la calculator) sau nu corespunde așteptărilor utilizatorilor (de exemplu, o opțiune, a cărei locație a fost schimbată cu cea a unei alte opțiuni). Aceste diferențe pot determina utilizatorii să nu găsească controlul sau informațiile dorite sau să interacționeze cu un element al interfeței cu care nu sunt obișnuiți, chiar dacă această interacțiune duce la o alegere de protecție a datelor, pe care utilizatorii nu o doresc.

Prevederile relevante ale RGPD:
- *Informații ușor accesibile*: articolul 12 alineatul (1);
- *Exercitarea drepturilor*: articolul 12 alineatul (2).

Exemple: CU 3b exemplul 39; CU 4 exemplul 50.

4.5.4 Discontinuitatea limbajului

Informațiile referitoare la protecția datelor nu sunt furnizate în limbile oficiale ale țării în care locuiesc utilizatorii, în timp ce serviciul este. Dacă utilizatorii nu cunosc limba în care sunt prezentate informațiile privind protecția datelor, nu o vor putea citi cu ușurință și, prin urmare, nu vor cunoaște cum sunt prelucrate datele lor cu caracter personal.

Prevederile relevante ale RGPD:
- *Echitatea prelucrării:* articolul 5 alineatul (1) litera (a);
- *Informații inteligibile:* articolul 12 alineatul (1), articolul 13 și articolul 14;
- *Utilizarea unui limbaj clar și simplu pentru informații*: articolul 12 alineatul (1), articolul 13 și articolul 14.

Exemple: CU 2a exemplul 16; CU 3a exemplele 26 (ilustrare) şi 27; CU 4 exemplul 44.

4.6 Lăsată în întuneric

Interfața este concepută astfel încât să ascundă informațiile sau instrumentele de control legate de protecția datelor sau să lase utilizatorii nesiguri cu privire la modul de prelucrare a datelor lor și tipul de control, pe care ar putea să-l aibă asupra acesteia.

4.6.1 Informații conflictuale

Oferirea utilizatorilor a informațiilor, care într-un mod se contrazic unele pe altele. Este posibil ca utilizatorii să rămână nesiguri cu privire la ceea ce ar trebui să facă și la consecințele acțiunilor lor, prin urmare probabil să nu facă nimic și să păstreze doar setările implicite.

Prevederile relevante ale RGPD:
- *Echitatea prelucrării*: articolul 5 alineatul (1) litera (a);
- *Informații transparente*: articolul 12 (1);
- *Consimțământ informat*: articolul 7 alineatul (2) coroborat cu articolul 4 alineatul (11). Exemple: CU 2a exemplu 12; CU 2c exemplu 20; CU 3b exemplu 36.

4.6.2 Formulare sau informații ambigue

Utilizarea de termeni ambigui și vagi atunci când oferiți informații utilizatorilor. Este posibil ca aceștia să rămână nesiguri cu privire la modul în care vor fi prelucrate datele sau la modul în care își exercită controlul asupra datelor lor cu caracter personal.

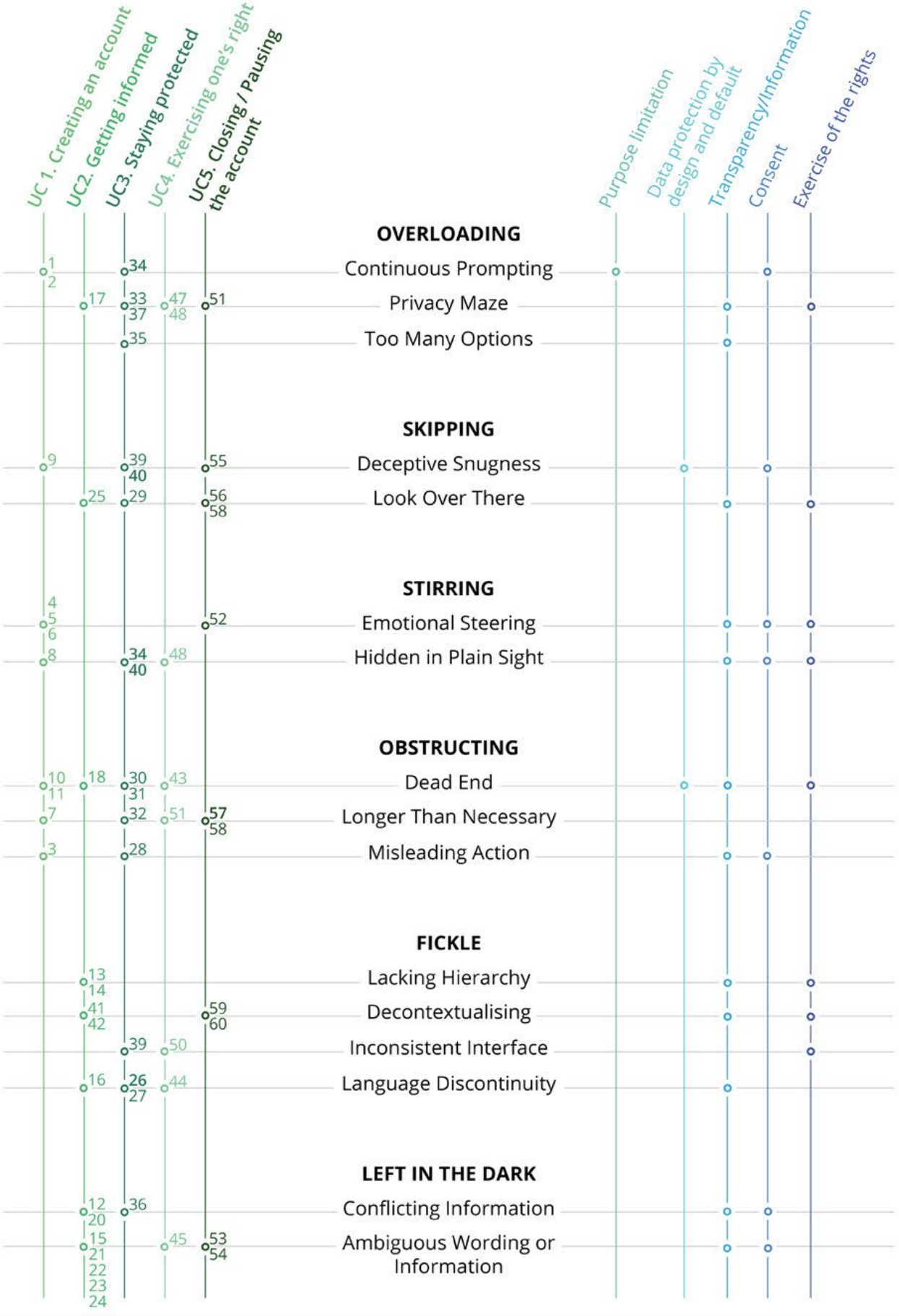
Prevederile relevante ale RGPD:
- *Echitatea prelucrării*: articolul 5 alineatul (1) litera (a);
- *Informații transparente*: articolul 12 (1);
- *Utilizarea unui limbaj clar și simplu pentru informații*: articolul 12 alineatul (1);
- *Consimțământ informat*: articolul 7 alineatul (2) coroborat cu articolul 4 alineatul (11);
- *Informații incomplete*: articolul 13
- *Prevederi specifice în dependență de cazul de utilizare particular, de exemplu*, articolul 34 pentru *CU 2c.*

Exemple: CU 2a exemplul 15; CU 2c exemplele 21, 22, 23, 24; CU 4 exemplul 45; CU 5 exemplele 53 și 54.

DECEPTIVE DESIGN OVERVIEW

LIFECYCLE

GDPR PROVISIONS
All deceptive design go against the fairness principle



CICLUL DE VIAȚĂ

PREZENTARE GENERALĂ A INTERFEȚELOR ÎNȘELĂTOARE

PREVEDERILE RGPD

Toate interfețele înșelătoare contravin principiului echității

CU1. Crearea unui cont	Limitarea scopului
CU2. Informarea	Protejarea datelor din momentul conceperii și în mod implicit
CU3. Protejarea continuă	Transparența/Informarea
CU4. Exercitarea dreptului	Consimțământul
CU5. Închiderea/Suspendarea contului	Exercitarea drepturilor

SUPRAÎNCĂRCAREA

Solicitare continuă

Labirint de confidențialitate

Prea multe opțiuni

OMITEREA

Comoditate înșelătoare

Uită-te acolo

AGITAREA

Dirijarea emoțională

Ascuns la vedere

OBSTRUCȚIONAREA

Fundătură

Mai lungă decât este necesar

SCHIMBĂTOR

Lipsa ierarhiei

Decontextualizarea

Interfața incoerentă

Discontinuitatea limbajului

LĂSATĂ ÎN ÎNTUNERIC

Informații conflictuale

Formulare sau informații ambigue

5 ANEXA II: CELE MAI BUNE PRACTICI

Următoarea listă oferă o privire de ansamblu asupra celor mai bune practici descrise în Orientări de la sfârșitul fiecărui caz de utilizare. Acestea pot fi folosite pentru a proiecta interfețe ale utilizatorului, care facilitează implementarea eficientă a RGPD. Astfel de cele mai bune practici pot oferi un prim pas către o modalitate standardizată pentru utilizatori de a-și controla în mod eficient datele și de a-și exercita drepturile.

Comenzi rapide: Linkurile către informații, acțiuni sau setări, care pot ajuta practic utilizatorii să-și gestioneze datele și setările de protecție a datelor ar trebui să fie disponibile oriunde găsesc informații sau experiențe conexe *(de exemplu, linkuri care redirecționează către părțile relevante ale politicii de confidențialitate*; *de exemplu, în politica de confidențialitate, includeți pentru fiecare informații despre protecția datelor linkuri care redirecționează direct către paginile aferente de protecție a datelor de pe platforma de comunicare socială; oferiți utilizatorilor un link pentru a-și reseta parola; atunci când utilizatorii sunt informați despre un aspect al prelucrării, sunt invitați să-și seteze preferințele de date aferente pe pagina setărilor/tabloul de bord corespunzător; oferiți un link către ștergerea contului din contul de utilizator).*

Opțiuni în bloc: Plasarea opțiunilor, care au același scop de procesare, astfel încât utilizatorii să le poată schimba mai ușor, lăsând totuși utilizatorilor posibilitatea de a face modificări mai detaliate. Dacă platformele de comunicare socială prezintă opțiuni în bloc, acestea nu ar trebui să conțină elemente neașteptate sau irelevante (de exemplu elemente cu scopuri diferite). Dacă pentru prelucrare este necesar consimțământ, opțiunile în bloc trebuie să fie în conformitate cu Orientările CEPD privind consimțământul, în special p. 42-44.

Informații de contact: Adresa de contact a companiei pentru adresarea solicitărilor de protecție a datelor ar trebui să fie menționată clar în politica de confidențialitate. Ar trebui să fie indicată într-o secțiune, în care utilizatorii se pot aștepta să o găsească, cum ar fi o secțiune despre identitatea operatorului de date, o secțiune legată de drepturi sau o secțiune cu date de contact.

Contactarea autorității de supraveghere: Menționarea identității specifice a autorității de supraveghere și includerea unui link către site-ul său web sau pagina web specifică legată de depunerea unei plângeri. Aceste informații ar trebui să fie indicate într-o secțiune, în care utilizatorii se pot aștepta să le găsească, cum ar fi o secțiune legată de drepturi.

Prezentarea generală a politicii de confidențialitate: La începutul / în partea de sus a politicii de confidențialitate, includeți un cuprins (retractabil) cu titluri și subtitluri, care arată diferite pasaje pe care le conține notificarea de confidențialitate. Denumirile pasajelor individuale conduc în mod clar utilizatorii la conținutul exact și le permit să identifice rapid și să ajungă în secțiunea pe care o caută.

Identificarea modificărilor și compararea: În cazul introducerii modificărilor în notificarea de confidențialitate, faceți accesibile versiunile anterioare cu data lansării și evidențiați modificările.

Formulări coerente: Pe site-ul web aceeași formulare și definiție este utilizată pentru aceeași protecție a datelor. Formularea folosită în politica de confidențialitate ar trebui să se potrivească cu cea folosită pe restul platformei.

Prezentarea definițiilor: Atunci când utilizați cuvinte sau jargon nefamiliare sau tehnice, prezentarea unei definiții într-un limbaj simplu va ajuta utilizatorii să înțeleagă informațiile, care

le sunt prezentate. Definiția poate fi inclusă direct în text și apărea atunci când utilizatorii trec cu mouse-ul peste cuvânt, sau poate fi inclusă într-un glosar.

Elemente contrastante de protecție a datelor: Evidențierea vizuală a elementelor sau a acțiunilor legate de protecția datelor într-o interfață, care nu este dedicată direct subiectului. De exemplu, atunci când postați pe platformă un mesaj public, controalele asupra asocierii geolocalizării ar trebui să fie disponibile în mod direct și ar trebui să fie clar vizibile.

Integrarea protecției datelor: Imediat după crearea unui cont, includeți puncte de protecție a datelor în experiența de integrare a furnizorului platformei de comunicare socială pentru ca utilizatorii să-și determine și să-și seteze cu ușurință preferințele. De exemplu, aceasta se poate efectua invitându-i să-și seteze preferințele de protecție a datelor după ce și-au adăugat primul prieten sau după ce au distribuit prima postare.

Utilizarea exemplelor: În afară de informațiile obligatorii, care specifică clar și precis scopul prelucrării, exemple pot fi folosite pentru a prezenta o anumită prelucrare a datelor pentru ca utilizatorii să înțeleagă mai bine.

Navigare lipicioasă: În timpul consultării unei pagini legate de protecția datelor, cuprinsul poate fi afișat în mod constant pe ecran, permițând utilizatorilor să fie mereu pe pagină și să navigheze rapid în conținut datorită linkurilor de ancorare.

Înapoi sus: Includeți un buton de revenire în sus în partea de jos a paginii sau ca element lipicios în partea de jos a ferestrei pentru a facilita navigarea utilizatorilor pe o pagină.

Înapoi sus: Includeți un buton de revenire în sus în partea de jos a paginii sau ca element lipicios în partea de jos a ferestrei pentru a facilita navigarea utilizatorilor pe o pagină.

Notificări: Notificările pot fi folosite pentru a sensibiliza utilizatorii cu privire la aspectele, schimbarea sau riscurile legate de prelucrarea datelor cu caracter personal *(de exemplu, când a avut loc o încălcare a securității datelor cu caracter personal).* Aceste notificări pot fi transmise în mai multe moduri, cum ar fi prin mesaje primite, ferestre pop-in, bannere fixate în partea de sus a paginii web etc.

Explicarea consecințelor: Atunci când utilizatorii doresc să activeze sau să dezactiveze un control al protecției datelor sau să își exprime sau să își retragă consimțământul, informați-i într-un mod neutru despre consecințelor unei astfel de acțiuni.

Consecvența între dispozitive: Atunci când platforma de comunicare socială este disponibilă prin diferite dispozitive (de exemplu, computer, telefoane inteligente etc.), setările și informațiile legate de protecția datelor ar trebui să fie situate în aceleași spații în diferite versiuni și ar trebui să fie accesibile prin aceeași călătorie și elemente de interfață (meniu, pictograme etc.).

Directoriul de protecție a datelor: Pentru a se orienta ușor printr-o secțiune diferită a meniului, oferiți utilizatorilor o pagină ușor accesibilă de unde sunt accesibile toate acțiunile (de exemplu, setările) și informațiile legate de protecția datelor. Această pagină poate fi găsită în meniul de navigare principal al furnizorului platformei de comunicare socială, contul de utilizator, prin politica de confidențialitate etc.

Informații contextuale: În afară de o politică de confidențialitate exhaustivă, prezentați fragmente succinte de informații la momentul cel mai potrivit pentru ca utilizatorul să aibă o informație specifică și continuă despre modul în care sunt prelucrate datele sale.

Adresa URL auto-explicativă: paginile legate de setările sau informațiile de protecție a datelor ar trebui să utilizeze o adresă web, care să reflecte în mod clar conținutul acestora. De exemplu, o pagină care centralizează controlul protecției datelor ar putea avea o adresă URL, cum ar fi [social-network.com]/data-settings.

Formularul de exercitare a drepturilor: pentru a facilita exercitarea de către utilizatori a drepturilor lor prevăzute de RGPD, furnizați un formular dedicat care să ajute utilizatorii să-și înțeleagă drepturile și care să-i îndrume să îndeplinească acest tip de solicitări.