

Suport de curs pentru dezvoltarea educației social media în școală

Ce este GDPR?

Ce sunt datele cu caracter personal?

Ce este prelucrarea?

Cine trebuie să respecte normele GDPR?

Regulile GDPR

Publicitatea direcționată/comportamentală

Ce trebuie făcut în cazul încălcărilor?

MODULUL 6



GDPR, legislație, proceduri și politici de utilizare a social media

Cofinanțat prin
programul Erasmus+
al Uniunii Europene



Erasmus+ ref.no. 2019-1-R001-KA201-063996

Conținutul prezentului material reprezintă responsabilitatea exclusivă a autorilor, iar Agenția Națională și Comisia Europeană nu sunt responsabile pentru modul în care va fi folosit conținutul informației.

Scopul modulului

Atunci când se apelează la rețelele de socializare, trebuie luată în discuție, în mod inevitabil confidențialitatea și protecția datelor.

Lumea digitală de astăzi ne permite să împărtășim totul cu toată lumea. Toate tipurile de persoane, organizații, companii și chiar și guvernul prelucrează informații despre dvs., gândiți-vă la școala dvs., la comuna sau orașul dvs., la clubul dvs. sportiv, la angajatorul dvs. etc. Cu toate acestea, cele mai multe informații despre dvs. sunt colectate prin intermediul internetului. În special pe rețelele de socializare, cum ar fi Facebook și Instagram, sunt distribuite o mulțime de informații personale. O concepție greșită frecventă este aceea că serviciile platformelor de socializare sunt gratuite: în realitate, plătiți, dar în loc să plătiți cu bani, plătiți cu datele dvs. personale. Deși aceasta poate fi o modalitate plăcută de a interacționa cu prietenii și chiar un mijloc amuzant de a-ți face noi prieteni, împărtășirea informațiilor personale prezintă și riscuri. Tot ceea ce distribuiți online poate lăsa amprente digitale. Odată ce o fotografie, un videoclip, un status, un tweet etc. este postat pe internet (de exemplu, pe profilul dvs. de socializare), nu mai aveți control asupra acestuia: oricine poate copia, reposta sau salva fotografia, făcând imposibilă ștergerea completă a acesteia de pe internet. Aceste amprente digitale pot fi „date cu caracter personal” (de exemplu, numele dumneavoastră, adresa (de e-mail), data nașterii, fotografiile dumneavoastră). Împărtășirea acestui tip de date vă poate expune la tot felul de riscuri (de exemplu, furt de identitate, hărțuire, conținut personalizat, publicitate direcționată și multe altele). Prin urmare, este important să știți ce date cu caracter personal despre dvs. sunt colectate, în ce mod, pentru cât timp și ce se face pentru a vă proteja datele personale. Acesta este punctul în care a intervenit legiuitorul.

Datele dvs. personale nu pot fi pur și simplu folosite de alții și nici dvs. nu puteți folosi datele personale ale altor persoane. De ceva timp deja, există legi privind confidențialitatea care limitează utilizarea datelor cu caracter personal. Datorită creșterii rețelelor de socializare, a altor platforme online, a aplicațiilor mobile etc. - toate bazându-se pe prelucrarea unor cantități mari de date cu caracter personal - aceste legi au devenit depășite și nu mai erau de actualitate, pentru a oferi o protecție suficientă pentru persoanele fizice și datele lor personale. Prin urmare, aceste legi naționale au fost înlocuite de Regulamentul general privind protecția datelor (GDPR), care se aplică în întreaga Uniune Europeană.

GDPR obligă orice persoană care prelucrează date cu caracter personal să respecte normele regulamentului, inclusiv școlile și profesorii. Având în vedere că copiii își petrec o parte semnificativă a timpului pe rețelele de socializare, iar școlile sunt colectori importanți de date cu caracter personal (despre personalul și despre elevii lor și atât online, cât și offline), acest modul este de mare importanță. Viața privată și protecția datelor sunt drepturi fundamentale pentru toată lumea. Este important ca tinerii să cunoască GDPR și să fie conștienți de drepturile și obligațiile lor în această privință. Deoarece profesorii sunt adesea un prim punct de contact pentru elevi, aceștia se află într-o poziție cheie pentru a informa și a sensibiliza elevii cu privire la GDPR.

Număr de ore: 2

Rezultatele învățării

- Conștientizarea și familiarizarea atât a elevilor, cât și a profesorilor cu GDPR, cu scopul și importanța acestuia;
- Cunoașterea obligațiilor care revin companiilor și organizațiilor în ceea ce privește prelucrarea datelor cu caracter personal în conformitate cu GDPR;
- Cunoașterea propriilor drepturi în ceea ce privește prelucrarea datelor lor personale;
- Înțelegerea conceptului și a valorii „datelor cu caracter personal” și a „prelucrării”;
- Crearea unui reflex natural la elevi de a reflecta, înainte de a împărtăși date cu caracter personal, dacă informațiile pe care intenționează să le împărtășească nu sunt prea personale și nu constituie un risc pentru viața lor privată;
- Ce se poate/trebuie să se regăsească într-o politică de confidențialitate;
- Capacitatea de a utiliza setările de confidențialitate ale platformei lor de socializare pentru a se asigura că numai persoanele pe care le aleg pot vedea informațiile de pe profilul lor;
- Înțelegerea publicității direcționate;

- Cunoștințe din partea școlilor și a cadrelor didactice cu privire la modul de utilizare legală a rețelelor sociale;
- Cunoștințe despre ce trebuie făcut în cazul utilizării ilegale a datelor cu caracter personal.

Material de formare

Context

1.1. Ce este GDPR-ul?

Regulamentul general privind protecția datelor a intrat în vigoare la 25 mai 2018 și se aplică oricărei organizații stabilite în UE sau în afara UE, dar care prelucrează date cu caracter personal de la persoane din UE - aceasta include școlile sau orice alte instituții de învățământ. Prin introducerea de noi reguli, GDPR urmărește să redea indivizilor controlul asupra datelor lor personale prin limitarea modului în care alte persoane și organizații pot utiliza datele dvs. personale.

GDPR protejează datele dvs. personale din momentul în care împărtășiți aceste date cu alte persoane. Altor nu li se permite pur și simplu să partajeze aceste date, să le salveze, să le copieze, să dea link-uri.... GDPR stabilește reguli pe care companiile, organizațiile și guvernele trebuie să le respecte în cazul în care doresc să utilizeze datele personale ale persoanelor fizice: prelucrarea trebuie să se facă în mod legal, corect și transparent. În plus, GDPR stabilește o serie de drepturi pentru a ajuta persoanele fizice să dețină în continuare controlul asupra datelor lor personale.

Deoarece partajarea informațiilor personale pe rețelele de socializare sau schimbul de date personale pentru accesul la aplicații și alte servicii bazate pe web este ceva obișnuit în zilele noastre, acest modul se va concentra pe GDPR și pe protecția datelor în lumina acestor servicii.

1.2. Ce sunt datele cu caracter personal?

1.2.1. Generalități

Datele cu caracter personal reprezintă orice fel de informații care dezvăluie ceva despre dumneavoastră personal.

De exemplu, numele, numărul de identificare, data nașterii, adresa, datele de localizare, fotografiile sau videoclipurile unei persoane, religia, adresa IP, istoricul de navigare, mărcile, biletele de comportament, profilurile de socializare (inclusiv like-urile, share-urile și prietenii) etc.

Acest lucru trebuie interpretat în sens foarte larg: dacă este posibil să se identifice o persoană în mod direct sau indirect din informațiile în cauză, atunci aceste informații sunt date cu caracter personal.

- **Identificare directă:**

Informațiile vă permit în sine să identificați persoana la care se referă aceste informații.

De exemplu, numele, numărul de telefon, numărul de identificare, adresa de domiciliu, adresa de e-mail, date de localizare, înregistrări vocale etc.

- **Identificare indirectă:**

Informațiile, ca atare, nu sunt suficiente pentru a identifica o persoană, însă luarea în considerare a unor informații suplimentare - care sunt deja disponibile sau care trebuie obținute dintr-o altă sursă - vă permite să identificați persoana în cauză.

De exemplu, plăcuțele de înmatriculare pot fi considerate date cu caracter personal, indiferent de faptul că dumneavoastră nu aveți acces la bazele de date care leagă plăcuțele de înmatriculare de proprietarii de mașini. Faptul că alte persoane pot face această conexiune este suficient pentru a califica aceste informații drept date cu caracter personal. Același raționament se aplică și în cazul informațiilor colectate prin cookie-uri, ID-uri digitale și adrese MAC și IP (care sunt unice pentru un dispozitiv).

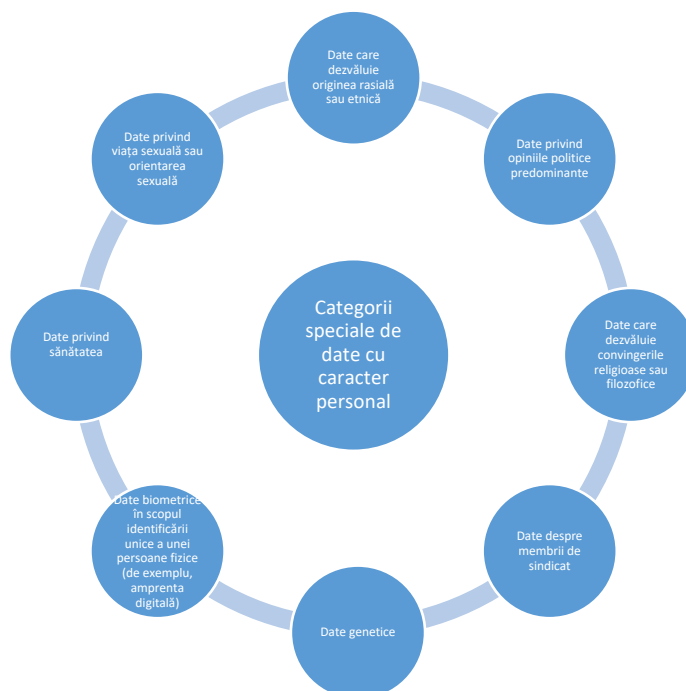
Este posibil ca o singură informație (de exemplu, culoarea părului, ocupația, mașina...) să nu fie capabilă să identifice o persoană fizică ca atare, dar acest lucru poate fi diferit atunci când aceste date sunt combinate cu alte date. Companiile care colectează mai multe tipuri de date despre persoane (de exemplu, rețelele de socializare) ar trebui să țină cont de acest lucru.

Date cu caracter personal
<p>Informații referitoare la o <u>persoană fizică</u>.</p> <p>Nu sunt informații despre companii și alte organizații, persoane decedate, animale de</p>

companie, obiecte etc.
<u>Formatul este irelevant</u> : text, imagine, video, sunet etc.
Informațiile permit identificarea unei singure persoane, <u>fie direct, fie indirect</u> (prin luarea în considerare a unor informații suplimentare).

1.2.2. Categoriile speciale de date cu caracter personal

GDPR face distincție între datele cu caracter personal „obișnuite” și categoriile speciale de date. Din cauza naturii sensibile a acestora din urmă și a potențialului mare de a afecta în mod negativ viața privată a unei persoane și alte drepturi și libertăți fundamentale (de exemplu, dreptul de a nu fi discriminat) atunci când sunt utilizate, acest tip de date cu caracter personal este, în principiu, interzis de a fi prelucrate.



1.2.3. De ce sunt valoroase datele personale?

Datele cu caracter personal sunt adesea numite „petrolul internetului” și noua monedă a lumii digitale de astăzi. Cu alte cuvinte, datele cu caracter personal sunt considerate extrem de valoroase.

Multe companii își oferă gratuit serviciile online, în timp ce își câștigă banii din publicitate. Publicitatea este cea care beneficiază în mod predominant de prelucrarea datelor cu caracter personal.

Atunci când intrați online, lăsați urme digitale. Tehnologia actuală permite companiilor să utilizeze și să stocheze datele personale pe care le generați atunci când cumpărați anumite bunuri sau servicii, sau pur și simplu când căutați anumite lucruri sau informații (numele dumneavoastră, interesele dumneavoastră, dorințele dumneavoastră, stilul dumneavoastră etc.). Un număr de clicuri și like-uri pe rețelele de socializare (de exemplu, Facebook) sunt suficiente pentru ca societățile să efectueze o analiză pentru a vă determina preferințele exacte. Combinând toate aceste informații din diferite surse, companiile sunt capabile să își facă o imagine clară despre dumneavoastră. Aici se vede valoarea datelor cu caracter personal: dacă o companie știe ce căutați sau ce vă interesează, poate să vă trimită reclame specifice pentru aceste produse sau servicii. *(Mai multe despre acest lucru la punctul 4. Publicitatea direcționată)*

Datele cu caracter personal nu sunt interesante doar pentru companii, ci și pentru hackeri! În ultimii ani, mai multe companii mari au ajuns la știri în lumina unor scandaluri de hacking, în cazul cărora au fost furate date personale ale clienților lor (de exemplu, Cambridge Analytica, Facebook, Mastercard).

În cele din urmă, datele cu caracter personal oferă, de asemenea, informații interesante pentru autoritățile publice, deoarece le pot permite să obțină noi informații despre persoane sau grupuri de persoane.

Cu toate acestea, o utilizare necontrolată a datelor cu caracter personal ar putea plasa companiile private, hackerii și autoritățile publice într-o poziție de putere.

1.3. Ce este prelucrarea?

Normele din GDPR se aplică numai prelucrării datelor cu caracter personal.

Prelucrare = orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra unor seturi de date cu caracter personal, fie că este sau nu efectuată prin mijloace automatizate.

De exemplu, colectarea, înregistrarea, organizarea (de exemplu, întocmirea unei liste de distribuție), structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în alt mod (de exemplu, postarea unui mesaj sau a unei imagini pe pagina de Facebook a unei organizații), alinierea sau combinarea, restricționarea, ștergerea sau distrugerea datelor cu caracter personal.

În cazul în care una dintre acțiunile menționate mai sus este efectuată asupra datelor dvs. personale, se aplică GDPR.

Important de reținut este faptul că prelucrarea pentru activități pur personale sau casnice nu intră sub incidența GDPR. (de exemplu, părinții care își fotografiază copilul și colegii de școală la un eveniment școlar pentru a fi păstrate acasă într-un album foto).

1.4. Cine trebuie să respecte regulile GDPR?

GDPR se aplică unei companii sau entități (adică persoană fizică sau juridică, autoritate publică, agenție sau alt organism), indiferent de mărimea, sectorul, numărul de angajați sau cifra de afaceri, care:

- prelucrează date cu caracter personal ca parte a activităților uneia dintre sucursalele sale stabilite în UE (indiferent de locul în care sunt prelucrate datele);
- este stabilit în afara UE și prelucrează date cu caracter personal în vederea oferirii de bunuri/servicii persoanelor fizice din UE sau în vederea monitorizării comportamentului persoanelor fizice din UE.

Astfel de companii sau entități sunt considerate controlori ai datelor dumneavoastră cu caracter personal și trebuie să se asigure că este respectat GDPR.

Regulile

2.1. Principiile GDPR

Orice companie sau entitate care prelucrează date cu caracter personal va trebui să respecte anumite reguli.

2.1.1. Legalitate, corectitudine și transparență

(a) Legalitate

Atunci când o companie sau o organizație dorește să prelucreze datele dumneavoastră cu caracter personal, înainte de a face acest lucru, trebuie să se asigure că prelucrarea sa se poate baza pe un motiv justificat - **un temei legal** - în conformitate cu RGPD. Un temei legal este un motiv pentru prelucrare care este determinat și acceptat de GDPR (a se vedea articolul 6 din GDPR).

Cele mai relevante dintre aceste temeiuri legitime în lumina social media sunt: prelucrarea datelor cu caracter personal este necesară **pentru a executa un contract**, compania sau organizația a obținut **consimțământul** dvs. sau compania sau organizația are (un) **interes(e) legitim(e)** în prelucrarea datelor dvs. cu caracter personal.

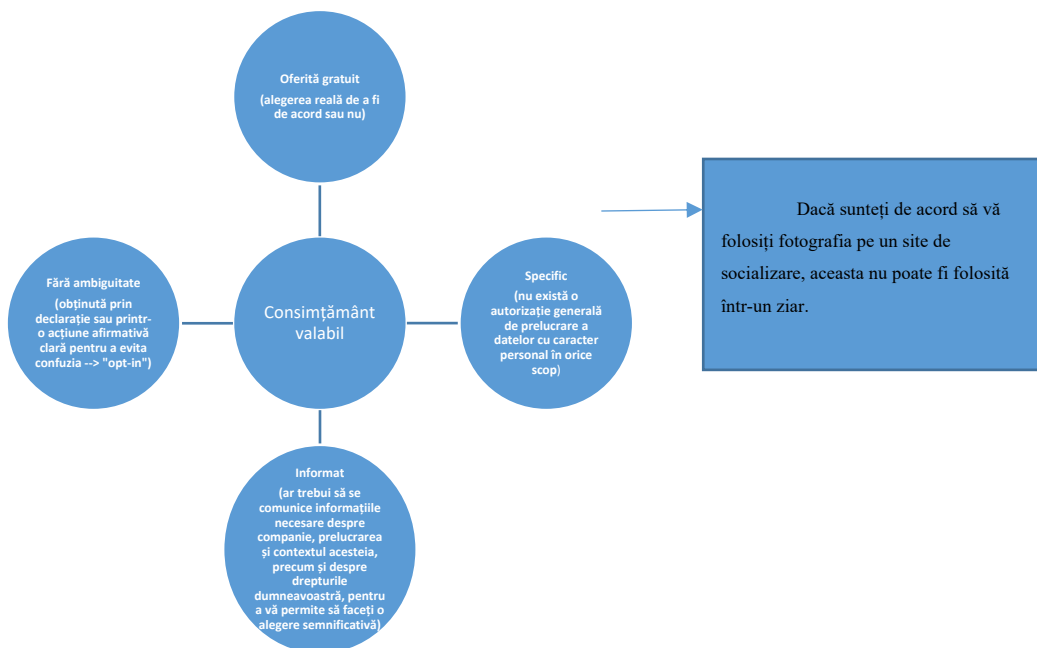
Necesitatea contractuală

Atunci când o companie sau o organizație trebuie să prelucreze date cu caracter personal pentru a respecta obligațiile contractuale dintre ea și dvs. sau pentru a da curs unor solicitări precontractuale din partea dvs., aceasta se poate baza pe temeiul legal „contract”. Unele obligații contractuale pur și simplu nu pot fi îndeplinite fără colectarea și prelucrarea anumitor date cu caracter personal. Prelucrarea care este utilă, dar care nu este necesară în mod obiectiv, pentru a efectua serviciul contractual sau pentru a întreprinde demersuri precontractuale relevante nu este acoperită de acest temei legal.

Exemplu: Twitter prelucrează datele dumneavoastră cu caracter personal - cum ar fi numele și adresa de e-mail - pentru a vă crea un cont, în scopul autentificării și pentru a permite crearea de conținut.

Consimțământ

Consimțământul are un înțeles special în conformitate cu GDPR. Pentru a fi valabil, consimțământul trebuie să fie:



Ar trebui să aveți posibilitatea de a vă retrage consimțământul în orice moment. Informațiile privind modul în care puteți face acest lucru ar trebui să vă fie furnizate în momentul în care vi se solicită consimțământul pentru o anumită activitate de prelucrare. Modalitatea de retragere a consimțământului ar trebui să fie la fel de ușoară ca și cea de acordare a consimțământului și nu ar trebui să aibă consecințe negative pentru dumneavoastră (de exemplu, o taxă sau niveluri de servicii mai scăzute).

Exemplu: Facebook are o funcție de recunoaștere facială care permite rețelei de socializare să vă recunoască în fotografiile sau videoclipurile de pe platforma sa. Utilizarea unei astfel de funcții implică prelucrarea datelor cu caracter personal, și anume fotografii sau videoclipuri cu dumneavoastră. Pentru a o activa, Facebook vă solicită consimțământul.

Același lucru este valabil și pentru funcția „istoric de localizare” pe care Facebook o oferă. Atunci când vă dați consimțământul cu privire la utilizarea acestei funcții, datele dvs. de localizare

sunt prelucrate pentru a explora ceea ce se întâmplă în jurul dvs., pentru a vă arăta reclame relevante, pentru a căuta prieteni în zonă.

Exemplu: Twitter prelucrează informațiile pe care le colectează de la dvs. pe Twitter, alte activități online ale dvs. și date de la partenerii săi pentru a vă afișa publicitate personalizată pe Twitter și în afara acestuia, pe baza consimțământului dvs.

O companie sau o organizație poate prelucra datele cu caracter personal ale unui copil pe baza consimțământului doar cu **acordul explicit al părintelui sau al tutorelui** acestuia până la o anumită vârstă. Pragul de vârstă pentru obținerea consimțământului copiilor direct de la aceștia poate varia de la 13 până la 16 ani în fiecare țară din UE. (Puteți verifica acest lucru la autoritatea națională de protecție a datelor din țara dumneavoastră)

Interes legitim

Interesele legitime pentru care este **necesară** prelucrarea datelor cu caracter personal pot fi interesele dumneavoastră sau interesele unor terțe părți (de exemplu, interese comerciale, interese individuale sau beneficii societale mai largi). Acest interes trebuie să fie specificat în politica de confidențialitate.

Pentru a se baza în mod valabil pe acest motiv de prelucrare, companiile sau organizațiile trebuie să prelucreze datele dvs. într-un mod la care vă așteptați în mod rezonabil, fără a vă cauza prejudicii nejustificate. În caz contrar, este probabil ca interesele dumneavoastră să prevaleze asupra celor ale companiei sau organizației, ceea ce înseamnă că acestea nu au voie să vă prelucreze datele cu caracter personal (pe acest temei legal), cu excepția cazului în care există o justificare imperioasă pentru prelucrare.

Exemplu: Twitter face deducții cu privire la contul dvs. - cum ar fi interesele, vârsta și sexul - pentru a vă oferi funcții precum sugestii de conturi, publicitate, recomandări, clasament în cronologie etc.

Exemplu: YouTube (Google) prelucrează datele dumneavoastră cu caracter personal în interesul legitim al acestora și al unor terțe părți, aplicând în același timp garanții adecvate care să

vă protejeze confidențialitatea. Acesta este, de exemplu, cazul personalizării serviciilor lor pentru a vă oferi o experiență de utilizare mai bună, marketing pentru a informa utilizatorii despre serviciile lor, dar și pentru a vă oferi publicitate, ceea ce face ca multe dintre serviciile lor să rămână gratuite. (Atunci când reclamele sunt personalizate, aceștia solicită consimțământul).

Categorii speciale de date

Este important de adăugat faptul că, pentru categoriile speciale de date cu caracter personal, există 10 excepții de la interdicția generală de a prelucra astfel de date (a se vedea articolul 9 din GDPR). Dacă este îndeplinită una dintre aceste condiții, categoriile speciale de date pot fi prelucrate în mod legal. Cea mai importantă excepție, având în vedere social media, este atunci când există un **consimțământ explicit** din partea persoanei ale cărei date cu caracter personal sunt vizate.

Aceste excepții formează un strat suplimentar de condiții pe lângă regulile obișnuite. În practică, acest lucru înseamnă că, atunci când doriți să prelucrați categorii speciale de date, trebuie să existe un temei legal (art. 6) și trebuie să se aplice o excepție (art. 9).

Exemplu: Google vă solicită consimțământul înainte de a partaja informații personale în afara companiei. Să presupunem că faceți o rezervare la restaurant prin intermediul „Google Home”, vi se va cere permisiunea înainte de a partaja datele personale (de exemplu, numele, numărul de telefon) cu restaurantul. Atunci când este vorba de informații personale sensibile (de exemplu, alergii), se angajează să ceară consimțământul explicit.

(b) Corectitudine

Compania sau entitatea care prelucrează datele dumneavoastră cu caracter personal ar trebui să facă acest lucru într-un mod corect, ceea ce înseamnă că trebuie să procedeze în mod rezonabil și nu într-un mod care să aibă efecte negative nejustificate sau care să vă inducă în eroare.

(c) Transparență

Acesta este un principiu foarte important, care este legat de corectitudine! Încă de la început, companiile sau organizațiile trebuie să fie clare, deschise și oneste cu dvs. cu privire la modul în care vor utiliza datele dvs. personale. Acest lucru presupune ca informațiile să fie furnizate într-un limbaj ușor accesibil și ușor de înțeles. Aici intervine politica de confidențialitate. Politicile de confidențialitate lungi și complicate ar trebui evitate, potrivit GDPR.

O politică de confidențialitate

Politica de confidențialitate este locul unde trebuie să mergeți atunci când doriți să obțineți informații despre modul în care sunt colectate, utilizate și protejate datele dumneavoastră personale de către rețelele de socializare (sau orice alt site web). Fiecare politică de confidențialitate trebuie să conțină un număr mare de mențiuni obligatorii:

- numele și datele de contact ale societății/organizației;
- datele de contact ale responsabilului cu protecția datelor, dacă acesta are unul;
- scopul (scopurile) pentru care prelucrează datele cu caracter personal și pe ce bază legală se bazează pentru a prelucra datele;
- interesul legitim pentru prelucrare (dacă este cazul) ;
- (categoriile de) date cu caracter personal obținute (dacă nu sunt obținute direct de la dumneavoastră);
- destinatarii (categoriile de destinatari) datelor cu caracter personal (vor fi datele cu caracter personal partajate cu alte părți?);
- detaliile privind transferurile de date cu caracter personal către orice țări terțe sau organizații internaționale (dacă este cazul);
- cât timp sunt păstrate datele (perioada de păstrare);
- drepturile pe care le puteți exercita (de exemplu, dreptul de acces, dreptul la uitare, dreptul de rectificare etc.);
- dreptul de retragere a consimțământului (dacă este cazul);
- dreptul dvs. de a depune plângeri la autoritatea pentru protecția datelor;
- sursa datelor cu caracter personal (în cazul în care datele cu caracter personal nu sunt obținute direct de la dumneavoastră);
- Detaliile privind existența procesului decizional automatizat, inclusiv crearea de profiluri (dacă este cazul).

2.1.2. Limitarea scopului

Principiul limitării scopului înseamnă că societățile sau organizațiile trebuie să definească în mod clar un scop specific pentru fiecare dintre activitățile lor de prelucrare, înainte de a începe. Această cerință urmărește să ofere transparență, previzibilitate și control din partea utilizatorilor. Orice prelucrare a datelor cu caracter personal trebuie să se facă într-un scop specific bine definit

sau în scopuri suplimentare, specificate, compatibile cu cel inițial. Astfel, prelucrarea datelor cu caracter personal în scopuri nedefinite și/sau nelimitate este ilegală.

Fiecare scop nou pentru prelucrarea datelor cu caracter personal care nu este compatibil cu scopul inițial trebuie să aibă propriul său temei juridic special și nu se poate baza pe faptul că datele au fost inițial obținute sau prelucrate în alt scop legitim.

Exemplu: Dacă acordați consimțământul Facebook pentru utilizarea funcției de recunoaștere facială pentru a repera pe platformă imagini și videoclipuri în care apăreți dumneavoastră, acest lucru nu înseamnă că Facebook poate utiliza aceste date în scopul de a vă oferi reclame targetate pe baza acestor date personale. Va avea nevoie de un temei legal separat (de exemplu, consimțământul) pentru acest lucru.

2.1.3. Minimizarea datelor

Companiile și organizațiile pot prelucra doar datele cu caracter personal de care au nevoie efectiv pentru a-și atinge scopul specificat, nu mai mult. Aceasta înseamnă că vor trebui să revizuiască periodic datele pe care le stochează pentru a șterge tot ceea ce nu le este necesar.

2.1.4. Precizie

Companiile și organizațiile trebuie să ia măsuri rezonabile pentru a se asigura că datele cu caracter personal pe care le dețin sunt corecte și nu induc în eroare. Acest lucru implică faptul că vor trebui să mențină datele cu caracter personal actualizate, prin corectarea sau ștergerea datelor, dacă este necesar.

2.1.5. Limitarea stocării

Datele cu caracter personal nu pot fi păstrate la nesfârșit. Companiile și organizațiile trebuie să șteargă sau să anonimizeze datele cu caracter personal de îndată ce nu mai au nevoie de ele pentru a atinge scopul (scopurile) pentru care au fost colectate. Companiile și organizațiile trebuie să se gândească din timp la cât timp doresc să păstreze datele dumneavoastră cu caracter personal și dacă această perioadă de timp este justificată, ceea ce va depinde de scopurile pentru care le prelucrează. Informațiile în acest sens ar trebui să fie incluse în politicile de confidențialitate.

2.1.6. Integritatea și confidențialitatea (securitatea datelor)

Protecția datelor cu caracter personal împotriva prelucrării neautorizate sau ilegale, a pierderii, distrugerii sau deteriorării accidentale reprezintă un element central al acestui principiu de integritate și confidențialitate (securitatea datelor). Principiul securității datelor are ca scop evitarea efectelor negative pentru dumneavoastră prin obligarea implementării unor măsuri tehnice (de exemplu, criptarea, pseudonimizarea) și/sau organizatorice (de exemplu, asigurarea faptului că datele cu caracter personal nu sunt disponibile pentru toată lumea din cadrul unei organizații, ci doar pentru cei care trebuie să lucreze cu datele).

2.1.7. Responsabilitate

Principiul responsabilității impune ca întreprinderile sau organizațiile să își asume responsabilitatea pentru ceea ce fac cu datele dumneavoastră cu caracter personal și pentru modul în care respectă GDPR. Având în vedere acest lucru, acestea trebuie să instituie măsuri și înregistrări care să le permită să demonstreze conformitatea atunci când li se solicită acest lucru.

Drepturile dumneavoastră

În societatea digitalizată de astăzi, este important să vă cunoașteți drepturile din punctul de vedere al protecției datelor.

3.1. Dreptul de a fi informat

Comaniile și organizațiile trebuie să vă informeze cu privire la colectarea și utilizarea datelor dumneavoastră cu caracter personal. Acest lucru este legat de principiul transparenței care stă la baza GDPR. A se vedea punctul 2.1.1.(c) cu privire la informațiile care trebuie furnizate.

Informațiile ar trebui să fie comunicate:

- în momentul în care colectați datele cu caracter personal de la aceștia;
- cel târziu la o lună de la obținerea datelor, în cazul în care au primit datele dvs. cu caracter personal de la altcineva.

Informațiile trebuie să fie concise, transparente, inteligibile, ușor accesibile și trebuie să utilizeze un limbaj clar și simplu. Aceste informații sunt furnizate în principal prin intermediul unei politici de confidențialitate.

3.2. Dreptul de acces

Aveți dreptul de a vă accesa propriile date cu caracter personal, deținute de o companie sau organizație. În practică, acest lucru înseamnă că veți primi următoarele informații:

- dacă societatea sau organizația prelucrează sau nu datele dumneavoastră cu caracter personal;
- o copie a datelor respective (în general, gratuit);
- informații suplimentare: companiile sau organizațiile trebuie să vă furnizeze aceleași informații care trebuie să se regăsească într-o politică de confidențialitate (a se vedea 2.1.1.(c)).

Exercitarea acestui drept vă ajută să înțelegeți cum și de ce folosesc companiile sau organizațiile datele dvs. și să verificați dacă acestea procedează în conformitate cu GDPR.

Este posibil ca societatea sau organizația să refuze accesul atunci când cererea este vădit nefondată (de exemplu, este clar că este făcută doar pentru a hărțui societatea) sau excesivă (de exemplu, se suprapune cu alte cereri). Motivele refuzului trebuie să vă fie comunicate în mod clar. Companiile și organizațiile au la dispoziție o lună pentru a răspunde la cerere.

3.3. Dreptul la ștergere (dreptul de a fi uitat)

GDPR vă acordă dreptul de a vă șterge datele cu caracter personal. Acest drept este legat de principiile minimizării și acurateței datelor, obligând companiile și organizațiile să ia în considerare ștergerea datelor cu caracter personal în anumite ocazii. Vă puteți exercita dreptul la ștergere atunci când:

- datele dvs. cu caracter personal nu mai sunt necesare în scopul pentru care au fost colectate de către companie sau organizație;

- atunci când compania sau organizația se bazează pe consimțământul dvs. ca bază legală pentru a deține datele, iar dvs. doriți să vă retrageți consimțământul;
- atunci când compania sau organizația se bazează pe interese legitime ca bază legală pentru prelucrare, vă puteți opune prelucrării datelor dumneavoastră și, dacă nu există un interes legitim superior pentru a continua această prelucrare, datele dumneavoastră vor fi șterse;
- atunci când compania sau organizația prelucrează datele cu caracter personal pentru a vă trimite marketing direct și vă opuneți acestei prelucrări;
- atunci când datele dvs. cu caracter personal au fost prelucrate în mod ilegal (= fără a se baza în mod corect pe un temei legal valabil);
- atunci când există o obligație legală care obligă la ștergerea datelor dvs. personale;
- atunci când datele dvs. personale au fost colectate de la dvs. când erați copil pentru a vă oferi servicii online.

Se pune un accent deosebit pe dreptul la ștergere în cazul în care cererea se referă la date colectate de la copii. În cazul în care consimțământul pentru prelucrarea datelor cu caracter personal a fost dat inițial când erați copil (fără să fiți pe deplin conștient de riscuri), poate fi foarte important să vă puteți retrage consimțământul și să obțineți ștergerea datelor cu caracter personal. (Probabil că fiecare elev se poate gândi la ceva ce a postat online în trecut, cu care nu mai este de acord sau pe care îl consideră jenant astăzi).

Compania sau organizația nu este obligată să dea curs întotdeauna (în totalitate) solicitării dumneavoastră, deoarece în unele cazuri dreptul la ștergere nu se aplică (de exemplu, dacă prelucrarea este necesară pentru a respecta legea sau atunci când prelucrarea are loc în scopuri de arhivare în interes public sau pentru cercetare științifică sau istorică, în cazul în care ștergerea ar duce la afectarea gravă a cercetării). O societate sau o organizație poate, de asemenea, să refuze exercitarea dreptului dumneavoastră la ștergere atunci când cererea este în mod vădit nefondată sau excesivă (a se vedea punctul 3.2).

O observație care trebuie făcută aici este că, chiar și cu acest drept la uitare, va fi foarte dificil (poate chiar imposibil) să vă ștergeți complet datele cu caracter personal de pe internet. Acest lucru se datorează faptului că datele sunt deseori partajate (ne)legal de către companii și organizații cu alte părți, care apoi partajează din nou aceste date cu alte părți și așa mai departe.

3.4. Dreptul la rectificare

Pe baza dreptului la rectificare, puteți corecta orice erori în datele dumneavoastră personale deținute de companii sau organizații: datele personale inexacte pot fi rectificate și datele incomplete pot fi completate. Acest drept este în mod clar legat de principiul exactității, de care companiile și organizațiile trebuie să țină cont.

Din nou, companiile și organizațiile nu trebuie să se conformeze întotdeauna solicitării dumneavoastră. Dacă ele consideră că datele dumneavoastră personale sunt exacte, trebuie să vă spună acest lucru și să vă explice decizia lor. Un alt motiv pentru a nu da curs (în totalitate) cererii dvs. de rectificare ar putea fi atunci când cererea dvs. este în mod vădit nefondată sau excesivă (a se vedea punctul 3.2).

3.5. Dreptul la restricționarea prelucrării

Acest drept este o alternativă la solicitarea de ștergere a datelor cu caracter personal și vă permite să solicitați companiei sau organizației să înceteze prelucrarea (unora dintre) datele dumneavoastră cu caracter personal, de obicei doar pentru o perioadă de timp, în timp ce alte probleme sunt în curs de rezolvare. Acest drept implică faptul că societatea sau organizația poate doar să stocheze datele dumneavoastră cu caracter personal, fără a le utiliza în continuare.

Companiile și organizațiile au, de asemenea, posibilitatea de a refuza cererea de restricționare a prelucrării, cu obligația de a oferi o explicație în acest sens. Unul dintre motivele de refuz poate fi din nou faptul că cererea este în mod vădit nefondată sau excesivă (a se vedea 3.2).

3.6. Dreptul la portabilitatea datelor

Acest drept vă oferă posibilitatea de a obține și de a transfera datele dumneavoastră cu caracter personal - pe care le-ați furnizat companiei sau organizației - în altă parte. În practică, acest lucru înseamnă că vă puteți muta, copia sau transfera cu ușurință propriile date cu caracter personal

dintr-un mediu IT în altul, într-un mod sigur și securizat și utilizat în mod obișnuit, sau puteți cere companiei sau organizației să facă acest lucru.

Acest drept se aplică numai în cazul în care societatea sau organizația se bazează pe „consimțământ” sau pe „necesitatea contractuală” ca bază legală pentru prelucrarea acestor date cu caracter personal sau în cazul în care acestea sunt prelucrate prin mijloace automatizate (adică prin intermediul unor programe și instrumente IT specializate și, de exemplu, nu pe hârtie).

Companiile și organizațiile au, de asemenea, posibilitatea de a refuza cererea de restricționare a prelucrării, cu obligația de a oferi o explicație în acest sens. Unul dintre motivele de refuz poate fi din nou faptul că cererea este în mod vădit nefondată sau excesivă (a se vedea 3.2).

3.7. Dreptul de opoziție

Dreptul la opoziție nu este un drept general. Vă puteți invoca dreptul de a vă opune prelucrării datelor cu caracter personal în funcție de situația dvs. particulară și a datelor prelucrate în scopul de a vă oferi servicii de marketing direct. Acest drept vă permite să opriți sau să împiedicați companiile și organizațiile să prelucreze (o parte din) datele dvs. personale.

Dreptul de a vă opune prelucrării în scopuri de marketing direct este un drept absolut, ceea ce înseamnă că societățile și organizațiile trebuie întotdeauna să dea curs acestei solicitări. Atunci când dreptul de a obiecta este exercitat din alt motiv, companiile și organizațiile pot decide să continue să vă prelucreze datele cu caracter personal dacă pot dovedi că există un motiv imperios necesar pentru a face acest lucru. Companiile și organizațiile au, de asemenea, posibilitatea de a refuza cererea de restricționare a prelucrării, cu obligația de a oferi o explicație în acest sens. Unul dintre motivele de refuz poate fi din nou faptul că cererea este în mod vădit nefondată sau excesivă (a se vedea 3.2).

3.8. Drepturile legate de luarea automată a deciziilor, inclusiv crearea de profiluri

Profilarea se referă la evaluarea aspectelor dumneavoastră personale pentru a face predicții despre dumneavoastră.

Exemplu: Un site de socializare evaluează anumite informații despre dumneavoastră (cum ar fi vârsta, sexul, înălțimea) și, pe baza acestora, vă clasifică într-un anumit grup din motive de recomandare de conținut sau de publicitate.

Luarea deciziilor bazate exclusiv pe mijloace automatizate se referă la situația în care tehnologia însăși ia decizii despre dvs. prin mijloace tehnologice, fără nicio implicare umană. Acest lucru se poate face fără crearea de profiluri.

În baza GDPR, aveți dreptul de a nu face obiectul unei decizii bazate exclusiv pe mijloace automatizate, dacă decizia are ca rezultat efecte juridice (adică sunt afectate drepturile dvs. legale) care vă privesc sau vă afectează în mod semnificativ într-un mod similar (adică vă influențează circumstanțele, comportamentul sau alegerile). Deoarece astfel de decizii au probabil un impact semnificativ asupra vieții dumneavoastră (acestea se pot referi, de exemplu, la solvabilitate, la recrutarea electronică, la performanța la locul de muncă), este necesară o protecție specială.

Exemplu: Companiile de asigurări care analizează postările de pe rețelele de socializare ale clienților (potențiali) folosind un algoritm care caută anumite cuvinte și fraze care indică un comportament prudent sau faptul că sunteți sănătos pentru a vă atribui un nivel de risc în vederea stabilirii primei de asigurare.

3.8. Practic

Atunci când vă exercitați drepturile, companiile și organizațiile au la dispoziție o lună pentru a vă răspunde la solicitările dumneavoastră și pentru a vă furniza informații în sprijinul deciziei lor. Cererile trebuie depuse la companie sau organizație, verbal sau în scris (de obicei, printr-un e-mail sau printr-o secțiune specifică a site-ului web). Ar trebui să fie la fel de ușor să vă exercitați aceste drepturi precum a fost să furnizați datele dvs. personale în primul rând.

Publicitatea direcționată/comportamentală

În trecut, companiile investeau în principal în publicitate la radio și televiziune. Un dezavantaj al acestei metode este că tuturor le este prezentată aceeași reclamă, indiferent dacă este sau nu de interes pentru oameni, ceea ce nu este foarte eficient. În zilele noastre, social media și progresele tehnologice permit companiilor să aleagă să își promoveze produsele și serviciile în fața consumatorilor într-un mod țintit: de exemplu, o reclamă pentru pantofi de alergare este prezentată doar utilizatorilor de social media care merg în mod regulat la alergare și în zilele în care nu plouă. Astfel de reclame direcționate pot fi găsite pe fluxul de știri din social media sau pe partea laterală a acestuia și pot fi recunoscute prin cuvinte precum „sponsorizat”.

Care dintre datele dumneavoastră sunt utilizate pentru publicitate?

1. Datele cu caracter personal pe care le introduceți atunci când vă creați contul de social media (de exemplu, vârsta, locul în care locuiți, data nașterii).
2. Tot ceea ce postați pe contul dvs. de social media, cum ar fi fotografii, videoclipuri și comentarii. De exemplu, dacă postați ceva de genul "Mi-e foaaaaarte foame acum", este posibil să primiți o reclamă de la un lanț de fast-food.
3. Lucrurile pe care le faceți și le căutați în afara platformei de socializare. De exemplu, dacă vizitați site-ul web al unui anumit eveniment, este posibil să primiți reclame despre acest eveniment sau despre un eveniment similar pe contul dvs. de social media. Acest din urmă lucru este posibil datorită „cookie-urilor”.

Cookie-urile sunt fișiere de mici dimensiuni stocate pe computerul, laptopul, smartphone-ul sau tableta dvs. pentru a ține evidența site-urilor web pe care le vizitați. Rețineți că societățile trebuie să vă ceară permisiunea înainte de a utiliza cookie-uri publicitare (există și alte tipuri de cookie-uri). Dacă nu doriți să fiți urmărit pe diferite site-uri web online, nu uitați să refuzați cookie-urile. Utilizarea modulelor cookie și a altor tehnologii de urmărire este reglementată de normele ePrivacy, nu de GDPR.

Este important de adăugat aici faptul că unele companii de social media dețin mai multe platforme și, prin urmare, pot folosi informațiile obținute despre dvs. pe ambele platforme (Facebook și Instagram, de exemplu).

4. Locația dumneavoastră (în timp real). Platformele de social media pot vedea chiar și unde vă aflați, pe baza wifi-ului și a gps-tracker-ului de pe telefonul dvs. Acest lucru ar putea avea ca rezultat faptul că ați putea primi reclame pentru o anumită sală de sport, dacă vă aflați în apropierea acesteia.

Toate informațiile menționate mai sus sunt reținute și interpretate de algoritmi și, bineînțeles, nu de ființe umane reale. Pe baza acestor date, companiile care aleg să facă publicitate pe rețelele de socializare pot alege un „grup țintă” (de exemplu, băieții de 16 ani din zona Amsterdam cărora le place fotbalul). Reclama potrivită, la momentul potrivit și în locul potrivit, poate influența serios comportamentul dumneavoastră, ceea ce este în beneficiul companiilor. Deși publicitatea personalizată nu ar trebui să fie întotdeauna percepută ca un lucru rău, ar trebui să fiți cu adevărat precaut cu privire la aceasta. Mai ales atunci când sunt implicate date sensibile (de exemplu, rasa, preferințele politice etc.), acest tip de publicitate ar putea fi înșelător, iar datele dvs. personale ar putea fi chiar folosite în mod abuziv (de exemplu, direcționarea către dvs. cu conținut fals, în scopul de a vă schimba sau radicaliza preferințele politice).

Ce trebuie făcut în caz de încălcări?

V-a fost partajat ilegal un fișier personal? A creat un profil fals al dvs. pe rețelele de socializare? Sau, poate ați încercat să vă exercitați unul dintre drepturile GDPR, dar nu sunteți mulțumit de răspunsul companiei sau al organizației? În primul rând, puteți solicita întotdeauna persoanei care vă încalcă drepturile de protecție a datelor, să șteargă sau să corecteze datele cu caracter personal în cauză (de exemplu, o fotografie, un profil fals, datele de contact). Dacă nu se întâmplă nimic, vă puteți adresa platformei de socializare pentru a șterge sau corecta datele cu caracter personal. Dacă acești pași nu sunt satisfăcători, puteți depune o plângere la autoritatea națională de protecție a datelor. (O altă opțiune este să vă impuneți drepturile prin intermediul unei căi de atac judiciare).

Fiecare țară din UE are propria autoritate de protecție a datelor. Puteți găsi o listă aici: https://edpb.europa.eu/about-edpb/board/members_en

Autoritățile de protecție a datelor sunt autorități publice independente care monitorizează și supraveghează dacă societățile și organizațiile de pe teritoriul lor aplică în mod corect normele de protecție a datelor. De asemenea, acestea oferă consultanță de specialitate cu privire la aspecte legate de protecția datelor și tratează plângerile primite de la persoane ca dumneavoastră. Autoritățile pot emite avertismente, muștrări, o interdicție temporară sau definitivă de prelucrare și amenzi (foarte mari).

Pe site-urile web ale acestor autorități de protecție a datelor puteți găsi modul în care puteți depune o plângere, aceasta putând fi făcută prin telefon, e-mail sau prin intermediul unui formular de contact disponibil pe site-ul lor.

Resurse

- https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (General handbook on data protection)
- <https://www.youtube.com/watch?v=XVBHishpew8> (YouTube video: what is the GDPR?)
- https://www.youtube.com/watch?v=3fuirT_PwDI (YouTube video: GDPR explained)
- <https://www.youtube.com/watch?v=PVaVIOJniSQ&t=6s> (YouTube video: my data, my choice)
- https://cris.vub.be/files/27962258/arcades_teaching_handbook_final_EN.pdf (Free university of Brussels (VUB): The European Handbook for Teaching Privacy and Data Protection at schools)
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747620/Data_Protection_Toolkit_for_Schools_OpenBeta.pdf (UK GOV: Data protection: a toolkit for schools)
- <https://www.gdpr.school/free-resources/> (useful GDPR sources for schools)
- https://edpb.europa.eu/about-edpb/board/members_en (List of national data protection authorities)
- <https://ico.org.uk/> (Website UK data protection authority → a lot of information!)

- <https://en.mediawijs.be/poster-step-by-step-how-should-i-protect-my-privacy-on-social-media> (Mediawijs website „How do I protect my privacy on social media?”)
- https://www.youtube.com/results?search_query=internet+safety+tips+for+teens (YouTube video with internet safety tips for teens)
- <https://www.youtube.com/watch?v=yrln8nyVBLU> (YouTube: Safe Web Surfing: Top Tips for Kids and Teens Online)
- <https://mediawijs.be/nieuws/slag-gdpr-jouw-klas> (Mediawijs website about using the GDPR as part of your classes → in Dutch)

Resurse suplimentare

- <https://d1afx9quaogywf.cloudfront.net/sites/default/files/Resources/School%20College%20Personal%20Data%20Advice%20and%20Guidance.pdf> (Information for schools to be GDPR compliant)
- <https://www.youtube.com/watch?v=xtLR0Ey5-vo&t=76s> (YouTube video with information for schools to be GDPR compliant)
- <https://www.youtube.com/watch?v=SpjpxspJNew&t=7s> (YouTube video with information for schools to be GDPR compliant)

Learning Snacks

Creșterea gradului de conștientizare a GDPR este crucială

Este esențial ca, în era digitală de astăzi, elevii și profesorii, precum și toți ceilalți membri ai personalului din unitățile de învățământ să cunoască GDPR și legislația privind protecția datelor în general. Cantitatea de date cu caracter personal care circulă online este enormă și va continua să crească, prin urmare, toată lumea trebuie să învețe cum să gestioneze în mod responsabil datele personale proprii și ale altora.

De ce este important GDPR? Valoarea datelor cu caracter personal!

În zilele noastre, producem cu toții zilnic cantități uriașe de date personale, în special online (de exemplu, postând fotografii, videoclipuri sau actualizări de stare pe rețelele de socializare, dar și făcând cumpărături online, citind un ziar online sau jucând jocuri online - toate acestea generează date care pot fi legate de dumneavoastră). Unele companii - pe lângă colectarea și prelucrarea datelor cu caracter personal pentru a furniza un anumit serviciu - urmăresc să colecteze cât mai multe date pentru a vă direcționa eficient cu ajutorul publicității. Astfel, datele cu caracter personal au o valoare economică importantă pentru companii și organizații. În plus, autoritățile publice sunt interesate de datele cu caracter personal, deoarece acestea le pot oferi noi informații. Dar și persoanele cu intenții rău intenționate, cum ar fi hackerii și hoții de identitate, sunt în căutare de datele dumneavoastră. O utilizare necontrolată a datelor cu caracter personal ar putea, în consecință, să pună companiile private, hackerii și autoritățile publice într-o poziție de putere și să vă pună într-o situație nedorită.

Gândiți-vă înainte de a distribui!

Întotdeauna gândiți-vă bine ce date personale distribuiți, cui și cum doriți să vă prezentați în postările din social media (text, imagini, videoclipuri). Este important să vă gândiți pe termen lung în acest caz, deoarece informațiile ar putea să plutească pe internet pentru totdeauna, deoarece nu este ușor să ștergeți informațiile de pe internet. Aveți grijă de setările de confidențialitate, astfel

încât persoanele pe care nu le cunoașteți să nu vă poată vedea (mare parte din) datele personale. Chiar și prin exercitarea dreptului la ștergere, cel mai probabil nu veți putea șterge toate urmele digitale.

Pot să-mi dau singur consimțământul pentru prelucrarea datelor mele personale?

Există o vârstă legală la care copiii pot consimți (sau nu) la prelucrarea datelor cu caracter personal de către furnizorii de servicii online. Această limită de vârstă poate varia între 13 și 16 ani în fiecare stat membru al UE.

Transparența/informarea este esențială!

Unul dintre principiile principale care stau la baza GDPR este principiul transparenței: companiile și organizațiile trebuie să fie clare cu privire la faptul că prelucrează datele dumneavoastră cu caracter personal, ce date cu caracter personal prelucrează, din ce motive și cum o fac, pentru cât timp etc. Acest principiu se traduce prin dreptul persoanelor de a fi informate, ceea ce ar trebui să vă permită să faceți alegeri în cunoștință de cauză cu privire la datele dvs. personale. În acest fel, GDPR dorește să pună indivizii în situația de a fi responsabili de ceea ce se întâmplă cu datele lor personale.

Cum pot ști ce face o companie sau o organizație cu datele mele personale?

Primul lucru pe care ar trebui să îl faceți atunci când doriți să aflați ce fac companiile sau organizațiile cu datele dumneavoastră personale este să verificați politica de confidențialitate. Această politică trebuie să implice o serie de elemente obligatorii. Dacă se pare că lipsește ceva sau ceva nu este clar, puteți încerca să contactați compania sau organizațiile pentru clarificări suplimentare.

Ce trebuie să fac atunci când cineva îmi folosește în mod abuziv datele pe rețelele de socializare?

Opțiunea 1: Contactați persoana/compania/organizația care utilizează datele dumneavoastră cu caracter personal în mod ilegal și solicitați-le să șteargă sau să corecteze datele dumneavoastră cu caracter personal.

Opțiunea 2: Contactați platforma de socializare pentru a solicita ștergerea sau corectarea datelor dvs. cu caracter personal.

Opțiunea 3: Depuneți o plângere la autoritatea națională pentru protecția datelor (consultați site-ul acesteia).

(Opțiunea 4: Mergeți în instanță.)

Infografice

Vedeți întregul material didactic + infograficul de mai jos.

Ce trebuie să faceți atunci când cineva vă folosește în mod ilegal datele personale pe rețelele de socializare?

1. Contactați persoana/compania/organizație care utilizează datele dvs. cu caracter personal într-un mod ilegal și solicitați-le să vă șteargă sau să corecteze datele dvs. cu caracter personal.

2. Contactați platforma de socializare pentru a solicita ștergerea sau corectarea datelor dvs. personale.

3. Depuneți o plângere la **autoritatea națională** pentru protecția datelor (consultați site-ul acesteia).

Planuri de activități cu elevii

- Începeți ora întrebând dacă elevii știu ce sunt datele personale și de ce cred că este important să protejeze datele personale.
- Permiteți elevilor să verifice setările de confidențialitate de pe Facebook (sau de pe un alt site de socializare): cine poate vedea ce fel de informații despre dumneavoastră? După aceea, poate avea loc o discuție între colegii de clasă care împărtășesc de ce doresc ca setările lor să fie într-un anumit fel sau dacă ar dori să își schimbe setările.
- Rugați elevii să caute care este pragul de vârstă pentru a-și da în mod valabil consimțământul în conformitate cu GDPR în țara dumneavoastră. Acest lucru poate fi făcut prin intermediul site-ului web al autorității naționale de protecție a datelor. Consultați: https://edpb.europa.eu/about-edpb/board/members_en.
- După ce au primit informații despre principiul transparenței, unul dintre principiile centrale ale GDPR, și despre rolul politicilor de confidențialitate în această privință, elevii au putut inspecta politica de confidențialitate a unui site web de socializare la alegere pentru a vedea dacă toate informațiile obligatorii se regăsesc acolo. Ulterior, ei pot discuta între ei despre acest lucru.
- După ce li se explică elevilor că au anumite drepturi în ceea ce privește prelucrarea datelor lor personale, aceștia ar putea depune o „cerere de acces” la Facebook (sau la un alt site de socializare), pentru a vedea ce date personale deține Facebook despre ei. A se vedea: <https://www.facebook.com/help/contact/2032834846972583>.

Evaluarea activității

Puteți evalua cu ușurință dacă elevii au înțeles informațiile despre GDPR prin aplicarea unor chestionare cu întrebări scurte al căror răspuns este adevărat sau fals, ca în exemplele de mai jos:

1. O fotografie care prezintă o persoană din spate, complet nerecunoscută, nu este niciodată o dată cu caracter personal în sensul GDPR? (**Fals:** Imaginea ca atare, fără alte informații, nu este o dată cu caracter personal, dar din momentul în care cineva adaugă la imagine numele, adresa sau numărul de telefon al acestei persoane, imaginea devine o dată cu caracter personal, deoarece din acel moment este legată de o anumită persoană).

2. Majoritatea site-urilor și aplicațiilor pe care le folosesc îmi prelucrează datele personale. (**Adevărat:** Scopul prelucrării datelor cu caracter personal poate fi diferit. De exemplu, de obicei, prelucrarea unui nume și a unei parole este necesară în scopul autentificării. Adesea, datele cu caracter personal, cum ar fi sexul, vârsta, interesele, sunt prelucrate în scopuri de marketing).

3. GDPR nu tratează toate datele cu caracter personal în același mod. (**Adevărat:** Principala împărțire făcută în GDPR este între datele cu caracter personal „obișnuite” și categoriile speciale de date cu caracter personal (de exemplu, sănătate, orientare sexuală, religie). Acestea din urmă trebuie tratate cu mai multă atenție datorită naturii lor sensibile (partajarea unor astfel de date implică un risc mai mare, deoarece este mai probabil ca acestea să ducă la consecințe nedorite, cum ar fi discriminarea, excluderea etc.) și de aceea, în principiu, prelucrarea acestor date este interzisă. (Datele privind infracțiunile penale și datele privind copiii fac, de asemenea, obiectul unui regim special).

4. O școală publică online buletinele de note ale fiecărui elev pentru a permite părinților să compare rezultatele copilului lor cu cele ale colegilor de clasă. Acest lucru este permis deoarece este în interesul superior al copilului. (**Fals:** Nu așa se procedează. Pentru fiecare prelucrare care are loc, o companie sau altă organizație - inclusiv o școală -, trebuie să se bazeze pe un temei legal valabil determinat în GDPR. Deoarece acest lucru ar putea afecta potențial negativ copiii, singurul mod în care o școală ar putea face acest lucru este atunci când obține consimțământul fiecărui copil și/sau părinte.

5. Atunci când se prelucrează date cu caracter personal, este întotdeauna necesar consimțământul persoanei ale cărei date sunt vizate. (**Fals:** Consimțământul este doar unul dintr-o

listă limitată de temeiuri legale pe care companiile și alte organizații se pot baza pentru a-și justifica activitățile de prelucrare (a se vedea articolele 6 și 9 din RGPD). Prin urmare, consimțământul nu este întotdeauna necesar. Pentru fiecare activitate de prelucrare, trebuie să alegeți întotdeauna un temei juridic pentru prelucrare, în funcție de temeiul cel mai potrivit pentru situație.

6. În trecut, v-ați dat consimțământul pentru ca fotografia dvs. să fie postată pe pagina de socializare a unei companii și chiar nu vă mai place această fotografie. Din păcate, deoarece v-ați dat consimțământul pentru publicarea fotografiei în trecut, nu puteți face nimic în acest sens. **(Fals:** Puteți oricând să vă retrageți consimțământul, ceea ce înseamnă că societatea va trebui să șteargă fotografia).

7. Unii elevi au fost fotografiați în clasă și și-au dat consimțământul pentru ca fotografia respectivă să fie folosită în raportul școlii. Ulterior, școala a decis să distribuie acest raport pe paginile lor de socializare. Acest lucru este permis în conformitate cu GDPR. **(Fals:** Consimțământul trebuie să fie dat într-o manieră specifică și nu poate fi grupat în mai multe scopuri. Aceasta înseamnă că școala ar fi trebuit să obțină un consimțământ separat și explicit pentru utilizarea raportului pe canalele sale de socializare.

8. Obiectivul principal al GDPR este de a restricționa publicitatea online. **(Fals:** în societatea digitalizată de astăzi, în care datele personale sunt super valoroase, GDPR urmărește să redea cetățenilor controlul asupra datelor lor personale, oferindu-le o protecție și drepturi mai mari + întrucât se aplică direct în întreaga UE, armonizează cele 27 de legi diferite privind protecția datelor).

9. Atunci când salvați pe telefon o fotografie a unei alte persoane pe care ați găsit-o pe Instagram, doar pentru a-i arăta coafezei dvs. tunsoarea pe care v-ar plăcea să o faceți, GDPR nu se aplică. **(Adevărat:** GDPR nu se aplică activităților personale și casnice).

10. Publicitatea personalizată/comportamentală pe rețelele de socializare este permisă numai dacă v-ați dat consimțământul pentru aceasta? **(Adevărat:** Pentru publicitatea bazată pe comportamentul dvs. de navigare, este necesară utilizarea de cookie-uri. Pentru ca site-urile web să stocheze aceste module cookie pe dispozitivul dvs. este necesar consimțământul dvs. prealabil, pe baza normelor ePrivacy, nu a GDPR. În plus, companiile ar trebui să vă ofere întotdeauna posibilitatea de a vă retrage acest consimțământ).