Declarație privind prelucrarea datelor cu caracter personal în contextul epidemiei de COVID-19

Adoptată la 19 martie 2020

Comitetul European pentru Protecția Datelor a adoptat următoarea declarație:

Peste tot în Europa, guvernele și organizațiile publice și private iau măsuri pentru a ține sub control epidemia de COVID-19 și pentru a atenua impactul acesteia. Aceste măsuri pot include prelucrarea diferitelor tipuri de date cu caracter personal.

Normele în materie de protecție a datelor (cum ar fi Regulamentul General privind Protecția Datelor - RGPD) nu îngrădesc măsurile luate în lupta împotriva pandemiei de COVID-19. Combaterea bolilor transmisibile este un obiectiv important împărtășit de toate națiunile, drept pentru care ar trebui să beneficieze de cel mai larg sprijin posibil. Stoparea propagării bolilor și utilizarea tehnicilor moderne în lupta împotriva flagelurilor care fac ravagii în numeroase zone ale planetei constituie obiective de interes pentru întreaga omenire. Cu toate acestea, CEPD ține să sublinieze că, inclusiv în aceste momente excepționale, operatorul de date și persoana împuternicită de operator trebuie să asigure protecția datelor cu caracter personal ale persoanelor vizate. Prin urmare, ar trebui să se țină seama de o serie de considerații pentru a se garanta legalitatea prelucrării datelor cu caracter personal și, în toate cazurile, ar trebui reamintit faptul că orice măsură luată în acest context trebuie să respecte principiile generale de drept și nu trebuie să fie ireversibilă. Situația de urgență este o condiție legală ce poate legitima îngrădiri ale libertăților, cu condiția ca acestea să fie proporționale și limitate la perioada de urgență.

1. Legalitatea prelucrării

RGPD este un act legislativ cu o sferă amplă de aplicare și prevede norme care se aplică, de asemenea, prelucrării datelor cu caracter personal într-un context precum cel legat de COVID-19. **RGPD autorizează autoritățile competente din sectorul sănătății publice și angajatorii să prelucreze datele cu caracter personal în contextul unei epidemii, în conformitate cu dreptul intern și cu condițiile stabilite de acesta**. De exemplu, această prelucrare este permisă în situațiile în care este necesară din motive de interes public major în domeniul sănătății publice. În aceste circumstanțe, nu este necesar să se obțină consimțământul persoanelor fizice.

1.1 În ceea ce privește prelucrarea datelor cu caracter personal, inclusiv a categoriilor speciale de date de către autoritățile publice competente (de exemplu, autoritățile din domeniul sănătății publice), CEPD consideră că articolele 6 și 9 din RGPD fac posibilă prelucrarea datelor cu caracter personal, în special atunci când aceasta intră sub incidența mandatului legal al autorității publice prevăzut de legislația națională și de condițiile stabilite în RGPD.

1.2 În contextul ocupării forței de muncă, prelucrarea datelor cu caracter personal poate fi necesară pentru respectarea unei obligații legale care îi revine angajatorului, precum obligațiile în materie de sănătate și de securitate la locul de muncă, sau din motive de interes public, precum controlul bolilor și al altor amenințări la adresa sănătății. De asemenea, RGPD prevede derogări de la interdicția de prelucrare a anumitor categorii speciale de date cu caracter personal, cum ar fi cele privind sănătatea, în cazul în care prelucrarea este necesară din motive de interes public major în domeniul sănătății publice [(articolul 9 alineatul (2) litera (i)], în baza dreptului Uniunii sau a dreptului intern, sau în cazul în care este necesar să se protejeze interesele vitale ale persoanei vizate [(articolul 9 alineatul (2) litera (c)], dat fiind că Considerentul 46 se referă în mod explicit la controlul unei epidemii.

1.3 În ceea ce privește prelucrarea datelor de telecomunicații, cum ar fi datele de localizare, trebuie să se respecte în egală măsură și legile naționale de punere în aplicare a Directivei privind viața privată și comunicațiile electronice. În principiu, datele de localizare pot fi utilizate de către operator numai în cazurile în care acestea sunt anonimizate sau în care persoanele fizice și-au exprimat consimțământul în acest sens. Cu toate acestea, articolul 15 din **Directiva privind viața privată și comunicațiile electronice autorizează statele membre să introducă măsuri legislative pentru a proteja siguranța publică.** Un astfel de act legislativ excepțional este posibil **numai în cazul în care constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice**. Aceste măsuri trebuie să fie conforme cu Carta drepturilor fundamentale și cu Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale. În plus, măsurile de acest tip **sunt supuse controlului jurisdicțional al Curții de Justiție a Uniunii Europene și al Curții Europene a Drepturilor Omului.** În cazul unei situații de urgență, ar trebui, de asemenea, ca legislația respectivă să fie strict limitată la durata situației de urgență în cauză.

2. Principii de bază referitoare la prelucrarea datelor cu caracter personal

Datele cu caracter personal care sunt necesare pentru atingerea obiectivelor urmărite ar trebui să fie prelucrate în scopuri determinate și explicite.

În plus, persoanele vizate ar trebui să primească informații transparente cu privire la activitățile de prelucrare care sunt desfășurate și la principalele lor caracteristici, inclusiv cu privire la perioada de păstrare a datelor colectate și la scopurile prelucrării. Informațiile ar trebui să fie ușor accesibile și furnizate într-un limbaj clar și simplu.

Este important să se adopte măsuri de securitate adecvate și politici de confidențialitate care să ofere asigurarea că nu se divulgă date cu caracter personal unor părți neautorizate. Măsurile puse în aplicare pentru gestionarea situației de urgență actuale și procesul decizional prin care se iau astfel de măsuri ar trebui să fie documentate în mod corespunzător.

3. Utilizarea datelor de localizare mobile

- **Guvernele statelor membre pot să utilizeze datele cu caracter personal legate de telefoanele mobile ale persoanelor fizice în eforturile lor de a monitoriza și a ține sub control răspândirea COVID-19 sau de a atenua impactul acesteia?**

În unele state membre, guvernele au în vedere utilizarea datelor de localizare mobilă ca o posibilă modalitate de a monitoriza și a ține sub control răspândirea COVID-19 sau de a atenua impactul acesteia. Această utilizare ar presupune, de exemplu, posibilitatea de a geolocaliza persoanele fizice sau de a trimite mesaje de sănătate publică unor persoane dintr-o zonă dată, prin telefon sau SMS. **Autoritățile publice ar trebui să încerce mai întâi să prelucreze datele de localizare într-un mod anonim (mai precis, prelucrând datele agregate într-un mod care să nu permită reidentificarea persoanelor), ceea ce ar permite generarea de rapoarte privind concentrația de dispozitive mobile existentă într-un anumit loc („cartografie").**

Normele privind protecția datelor cu caracter personal nu se aplică datelor care au fost anonimizate în mod corespunzător.

Atunci când nu este posibil să se prelucreze numai date anonime, Directiva privind viața privată și comunicațiile electronice **autorizează statele membre să introducă măsuri legislative pentru a proteja siguranța publică** (articolul 15).

În cazul în care se introduc măsuri de autorizare a prelucrării datelor de localizare neanonimizate, statele membre sunt obligate să instituie **garanții adecvate**, de exemplu, oferindu-le persoanelor fizice care utilizează servicii de comunicații electronice **dreptul la o cale de atac**.

Se aplică, de asemenea, principiul proporționalității. Ar trebui să se prefere în mod constant soluțiile cel mai puțin intruzive, ținându-se seama de scopul specific care trebuie atins. Măsurile invazive, cum ar fi „urmărirea" persoanelor fizice (și anume prelucrarea datelor neanonimizate privind istoricul localizării) ar putea fi considerate proporționale în circumstanțe excepționale și în funcție de modalitățile concrete de prelucrare. Aceste date ar trebui totuși să facă obiectul unui control consolidat și al unor garanții sporite care să asigure respectarea principiilor de protecție a datelor (proporționalitatea măsurii în ceea ce privește durata și domeniul de aplicare, păstrarea limitată a datelor și limitarea scopului).

4. Ocuparea forței de muncă

- **Un angajator poate să le ceară vizitatorilor sau angajaților să furnizeze informații specifice privind sănătatea în contextul COVID-19?**

Aplicarea principiului proporționalității și a minimizării datelor este deosebit de relevantă în acest caz. Angajatorii ar trebui să solicite informații privind sănătatea numai în măsura în care dreptul intern permite acest lucru.

- **Este permis unui angajator să supună angajații la controale medicale?**

Răspunsul depinde de legislația națională în materie de ocupare a forței de muncă sau de sănătate și siguranță. Angajatorii ar trebui să acceseze și să prelucreze date privind sănătatea numai dacă propriile lor obligații care le revin prin lege impun acest lucru.

- **Un angajator poate să divulge colegilor sau altor persoane decât angajații faptul că un angajat este infectat cu COVID-19?**

Angajatorii ar trebui să informeze personalul cu privire la cazurile de COVID-19 și să ia măsuri de protecție, dar nu ar trebui să comunice mai multe informații decât ceea ce este necesar. În cazurile în care este necesar să se dezvăluie numele angajatului (angajaților) care a (au) contractat virusul (de

exemplu, în contextul unor măsuri de prevenție), iar dreptul intern permite acest lucru, angajații în cauză sunt informați în prealabil, fiindu-le apărate demnitatea și integritatea.

- **Ce informații prelucrate în contextul COVID-19 pot fi obținute de către angajatori?**

Angajatorii pot obține informații cu caracter personal pentru a-și îndeplini sarcinile și pentru a organiza activitatea în conformitate cu legislația națională.

Pentru Comitetul European pentru Protecția Datelor,

Președintele

(Andrea Jelinek)