privacyONE
in alliance with BIRIȘ·GORAN

LEGAL ALERT

NORMELE DE APLICARE ÎN ROMÂNIA A REGULAMENTULUI GENERAL PRIVIND PROTECȚIA DATELOR

Data: 27 iulie 2018

Contact

Bd. Aviatorilor nr. 47, etaj 2, sector 1,
Bucureşti, România

www.privacyone.ro

contact@privacyone.ro

Context

În data de 25 mai 2018, cadrul legislativ general al protecției datelor s-a modificat substanțial odată cu aplicarea Regulamentului UE nr. 2016/679 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 („**GDPR**").

Deşi GDPR este de directă aplicare în toare țările UE, regulamentul permite fiecărui stat să adopte derogări sau garanții în anumite situații specifice – câteva exemple sunt jurnalismul, prelucrarea CNP sau contextul relațiilor de muncă.

Pentru a stabili astfel de derogări, Parlamentul României a adoptat în data de 27 iunie 2018 Legea nr. 190/2018 privind măsuri de punere în aplicare a GDPR (în continuare „**Legea de Aplicare GDPR**"), publicată în Monitorul Oficial nr. 651 din 26 iulie 2018.

Legea de Aplicare GDPR intră în vigoare pe 31 iulie 2018 şi conține reguli speciale pentru prelucrarea unor categorii de date personale, derogări de la GDPR, indicații despre responsabilul cu protecția datelor (DPO), despre organisme de certificare şi prevederi despre aplicarea sancțiunilor.

În plus, prin acte normative distincte au fost modificate normele de organizare şi funcționare a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) – legea 129/2018 în vigoare din 24 iunie 2018, a fost adoptat un formular de notificare a incidentelor de securitate legate de prelucrarea datelor personale - decizia nr. 128/2018 disponibilă aici, şi a fost aprobată procedura de primire şi soluționare a plângerilor - decizia nr. 133/2018 disponibilă aici.

Relevanță

Legea de aplicare GDPR impune reguli speciale sau restricți pentru anumite prelucrări de date personale, ceea ce înseamnă că cei care prelucrează CNP-ul sau aplică măsuri de supraveghere a angajaților vor trebui să își analizeze prelucrările deja existente raportat la noile reguli. Pentru activitățile jurnalistice, legea permite derogări de la majoritatea categoriilor de obligații din GDPR.

Dacă au loc incidente de securitate raportabile, se va folosi modelul de notificare doptat de ANSPDCP. În cazul unor investigații la fața locului, ANSPDCP va trebui să respecte garanțiile impuse prin legea sa de organizare şi funcționare.

Date genetice, biometrice şi de sănătate

Procesele decizionale automate sau profilarea care folosesc date genetice, biometrice sau de sănătate pot să fie realizate doar cu consimțământul persoanelor vizate sau dacă există o dispoziție legală expresă. Prelucrarea acestor date pentru alte scopuri nu este restricționată, fiind aplicabile toate temeiurile prevăzute la art. 9.2 GDPR.

Codul numeric personal

Regimul de prelucrare a identificatorului unic național se relaxează, nemaifiind aplicabilă limitarea prelucrării doar în temeiul obligației legale, consimțământului persoanei sau autorizației ANSPDCP. Devine deci posibilă prelucrarea CNPului în temeiul interesului legitim (urmărit de operator sau de un terț), însă pentru această situație *(nu şi pentru celelalte)* se impun condiții suplimentare:

a) aplicarea unor măsuri tehnice pentru respectarea principiului minimizării datelor şi asigurarea securității;

b) numirea unui responsabil cu protecția datelor (DPO);

c) stabilirea unor termene de stocare a datelor;

d) instruirea periodică a personalului care are realizează prelucrarea datelor sub autoritatea operatorului sau a împuternicitului acestuia.

Monitorizarea la locul de muncă

Cei care utilizează sisteme de monitorizare a angajaților prin [sic] mijloace de comunicații electronice sau supraveghere video vor trebui să respecte următoarele reguli:

e) să justifice temeinic interesele legitime pe care le urmăresc şi să se asigure că acestea prevalează asupra drepturilor şi libertăților persoanelor vizate (*Notă: este necesară realizarea unui test de echilibru, dar şi documentarea acestui test pentru a demonstra conformarea*);

f) să facă informarea prealabilă, completă şi explicită a angajaților (*Notă: informarea nu presupune colectarea consimțământului, lucru care oricum este neindicat în relațiile de muncă; angajatorii vor trebui însă să demonstreze că au realizat această informare*);

g) să consulte în prealabil sindicatul sau reprezentantul angajaților;

h) să aplice alte forme mai puțin intruzive pentru a atinge scopul pentru care este necesară monitorizarea şi să realizeze monitorizarea doar dacă aceste măsuri mai blânde nu au fost eficiente;

i) durata de stocare a datelor personale rezultate din monitorizare nu poate fi mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate (*Notă: cazuri temeinic justificate pot fi apărarea drepturilor în justiție acolo unde înregistrarea surprinde un incident, dar şi alte situații care însă trebuie argumentate în scris*).

Merită menționat şi că, deşi titlul marginal este „Prelucrarea datelor cu caracter personal în contextul relațiilor de muncă", articolul nu reglementează decât aceste două situații particulare, lăsând descoperite situații întâlnite foarte des, cum ar fi prelucrarea datelor sensibile sau a celor referitoare la condamnări penale fără să existe o obligație legală pentru angajator (de exemplu situația testării alcoolemiei sau a solicitării certificatelor de cazier judiciar la angajare). De asemenea, nu este acoperită situația monitorizării (nici video nici de altă natură) în alte spații.

Îndeplinirea unei sarcini care serveşte unui interes public

Legea de aplicare GDPR defineşte „îndeplinirea unei sarcini care serveşte unui interes public" ca incluzând acele activități ale partidelor politice sau ale organizațiilor cetățenilor aparținând minorităților naționale, ale organizațiilor neguvernamentale, care servesc realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public ori funcționării sistemului democratic, incluzând încurajarea participării cetățenilor în procesul de luare a deciziilor şi a pregătirii politicilor publice, respectiv promovarea principiilor şi valorilor democrației". Această definiție este cel puțin discutabilă prin aria foarte îngustă de aplicare şi totodată caracterul vag, având în vedere prevederile preambulului 45 GDPR:

În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. (...) De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplinește o sarcină care servește unui interes public sau care face parte din exercitarea autorității publice ar trebui să fie o autoritate publică sau o

altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică și protecția socială, precum și gestionarea serviciilor de asistență medicală, de dreptul privat, cum ar fi o asociație profesională.

Este cel puțin surprinzător că pentru legiuitorul român interesul public se exercită exclusiv în scop politico-democratic, iar nu şi în domeniul medical, al protecției sociale sau altele.

Derogări pentru partidele politice

Datele personale speciale vor putea fi prelucrate de partide politice, organizații ale cetățenilor aparținând minorităților naționale şi organizații neguvernamentale fără a avea nevoie de consimțământul persoanelor vizate dacă: (a) se aplică anumite garanții (informare, transparență, garantarea drepturilor la rectificare şi ştergere) şi (b) prelucrarea are loc în vederea realizării obiectivelor acestor organizații.

Chiar dacă legea nu menționează acest lucru, GDPR prevede clar în art. 9.2.d) că datele speciale pot fi prelucrate de partide politice şi alte entități non-profit fără consimțământ doar dacă se referă la membri sau la foști membri sau la persoane cu care există contacte permanente în legătură cu scopurile sale și că aceste date nu pot fi comunicate terților fără consimțământul persoanelor vizate. De aici rezultă că pot fi prelucrate fără consimțământ doar datele speciale relevante față de scopul acelei organizații (e.g. date despre apartenența la partid în cazul partidului respectiv).

De altfel, şi preambulul 56 GDPR prevede că „În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiția să se prevadă garanțiile corespunzătoare."

Mai mult, derogarea permisă partidelor politice şi ONG-urilor nu este generală, ci acestea trebuie să respecte în continuare toate celelalte reguli în materia prelucrării de date personale prevăzute la art. 5 GDPR (informarea, limitarea la scop, minimizarea, exactitatea, securitatea, limitarea duratei de stocare, responsabilitate).

Derogări pentru jurnalism şi cercetare

Sunt exceptate de la aplicarea unor prevederi GDPR acele prelucrări de date care se fac în scopuri jurnalistice, de exprimare academică, artistică sau literară,

precum şi cele în scop de cercetare ştiinţifică sau istorică, în scopuri statistice ori în scopuri de arhivare în interes public.

În cazul jurnalismului, Legea de Aplicare GDPR a scos prelucrările de date de sub incidența majorității prevederilor GDPR (mai puțin sancțiunile), dacă prelucrările (1) se referă la date personale care au fost făcute publice în mod manifest de către persoana vizată sau (2) datele sunt strâns legate de i) calitatea de persoană publică a persoanei vizate sau ii) caracterul public al faptelor în care este implicată persoana vizată. Practic, derogarea înseamnă că cei care fac prelucrări de date în cadrul activităților de jurnalism (dacă îndeplinesc şi condițiile din lege) nu sunt ținuți să respecte obligațiile privind protecția datelor, nici măcar confidențialitatea sau securitatea.

Această reglementare, deşi reprezintă o derogare permisă în principiu de art. 85 GDPR, este discutabilă deoarece motivul pentru care regulamentul permite derogarea în scopuri jurnalistice este asigurarea unui echilibru între dreptul la protecția datelor şi dreptul la libera exprimare şi informație. Cu alte cuvinte, derogările ar trebui să se aplice doar acolo unde cele două drepturi fundamentale nu pot fi conciliate – ceea ce presupune aplicarea unui test de echilibru şi respectarea acelor obligații care rămân compatibile (ca, de exemplu, măsuri de securitate a datelor sau integritatea şi confidențialitatea datelor).

Organisme de certificare

Acreditarea organismelor de certificare prevăzute la art. 43 din Regulamentul general privind protecția datelor se realizează de Asociația de Acreditare din România - RENAR, în calitate de organism național de acreditare. Organismele de certificare vor fi acreditate potrivit reglementărilor legale aplicabile, în conformitate cu standardul EN-ISO/IEC 17065 şi cu cerințele suplimentare stabilite de ANSPDCP, precum şi cu respectarea prevederilor art. 43 GDPR.

Sancționarea autorităților şi organismelor publice

Legea de Aplicare GDPR instituie un regim sancționator diferențiat între autoritățile şi organismele publice, şi restul entităților. Mai exact, în vreme ce regula generală prevăzută de GDPR în art. 58.2 este că autoritatea de supraveghere poate dispune oricare dintr-o serie de măsuri, inclusiv amendă care poate ajunge la un maxim de 10 milioane EUR sau 2% din cifra de afaceri, sau 20 milioane EUR sau 4% din cifra de afaceri, în funcție de prevederile încălcate, Legea

de Aplicare GDPR prevede un regim foarte diferit pentru autoritățile publice din România.

Mai exact, indiferent de gravitatea încălcării în discuție, întotdeauna autoritatea de supraveghere va aplica sancțiunea avertismentului şi va anexa un plan de remediere conform anexei incluse în Legea de Aplicare GDPR.

Legea nu prevede vreun termen maxim pentru remediere, lăsând la latitudinea autorității acest aspect, precum şi „posibilitatea", nu obligația, de a relua controlul când acest termen expiră. Abia dacă se reia controlul şi se constată că entitatea controlată nu a adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere, autoritatea de supraveghere poate aplica amendă, cu două paliere:

amendă de la 10.000 lei până la 100.000 lei	**amendă de la 10.000 lei până la 200.000 lei**
• art. 8, art. 11, art. 25-39, art. 42 şi 43 GDPR; • art. 42 şi 43 GDPR; • art. 41 alin. (4) GDPR; • art. 3-9 din Legea de Aplicare GDPR.	• art. 5-7 şi art. 9 GDPR; • art. 12-22 GDPR; • art. 44-49 GDPR; • capitolul IX GDPR; • art. 58 alin. (1) şi (2) GDPR.

Cu alte cuvinte, deşi a avut la dispoziție un termen de remediere şi totuşi nu a remediat încălcarea, o autoritate publică poate primi un maxim de amendă de 200.000 lei, în vreme ce pentru aceeaşi faptă un operator privat riscă un maxim de amendă de 20 milioane EURO sau 4% din cifra de afaceri globală din anul anterior, fără termen de remediere.

Trebuie totuşi spus că acest tratament diferențiat îşi are originea chiar în dispozițiile GDPR, mai exact art. 83 alin. (7), care prevede că *„fiecare stat membru poate prevedea norme prin care să se stabilească dacă şi în ce măsură pot fi impuse amenzi administrative autorităților publice şi organismelor publice stabilite în statul membru respectiv"*.

Câteva chestiuni care nu se regăsesc în Legea de Aplicare GDPR

În primul rând, Legea de Aplicare GDPR nu conține nicio prevedere în legătură cu vârsta copiilor sub care trebuie obținut acordul părinților/tutorilor pentru prelucrarea datelor în legătură cu serviciile societății informaționale oferite copiilor, prevăzut la art. 8 GDPR. Acest lucru înseamnă că în România se va aplica regula prevăzută de art. 8(1) GDPR, anume că **dacă serviciul societății informaționale este oferit unui copil şi acesta are sub 16 ani, este necesar acordul titularul răspunderii părintești asupra copilului**.

O altă chestiune nereglementată este exercitarea acțiunilor colective potrivit art. 80(2) GDPR, ceea ce înseamnă că **în România nu vor fi posibile acțiuni colective**.

În ce privește reprezentarea persoanelor vizate potrivit art. 80(1) GDPR, singura prevedere relevantă se găsește în Legea 129/2018, care în cadrul modificării art. 14^7 din legea de organizare a ANSPDCP prevede condițiile dovedirii mandatului de către organizația ce asigură reprezentarea.

Modificarea legii de organizare ANSPDCP

În cadrul pachetului de modificări legislative a fost a fost adoptată pe 15 iunie 2018 legea pentru modificarea şi completarea legii de organizare şi funcționare a ANSPDCP (Legea 129/2018 care modifică Legea 102/2005 privind înființarea, organizarea şi funcționarea ANSPDCP, publicată în Monitorul Oficial nr. 503 din 19 iunie 2018).

Legea 129/2018 introduce un capitol nou despre controlul ANSPDCP şi soluționarea plângerilor. ANSPDCP are competența de a realiza investigații inopinate la fața locului, iar cei investigați trebuie să pună la dispoziție informațiile şi documentele necesare. Dacă personalul de investigație este împiedicat să își exercite atribuțiile, ANSPDCP poate obține o cerere de autorizare de la Curtea de Apel București. Investigația ANSPDCP nu poate începe înainte de ora 8,00 şi nu poate continua după ora 18,00 (fără acordul scris al celui investigat) şi trebuie efectuată în prezența celui investigat sau a reprezentantului său.

Modelul de raportare a incidentelor de securitate

GDPR impune obligația de a înregistra în toate cazurile acele incidente care presupun o încălcare a securității datelor cu caracter personal şi de a notifica aceste incidente în termen de 72 de ore către autoritatea de supraveghere dacă sunt susceptibile să genereze un risc pentru drepturile și libertățile persoanelor fizice. ANSPDCP a adoptat modelul de *Notificare de încălcare a securității datelor cu caracter personal pentru operatorii de date cu caracter personal* care ar trebui transmis ANSPSCP în cazul unor incidente de securitate, în cazurile prevăzute de GDPR (Decizia ANSPDCP nr. 128/2018, publicată în Monitorul Oficial nr. 557 din 3 iulie 2018).

Formularul este disponibil pe website-ul ANSPDCP (download direct): http://dataprotection.ro/servlet/ViewDocument?id=1488

Pentru mai multe detalii legate de subiectele tratate în acest material, persoanele de contact sunt:

Andreea Lisievici, Partner (andreea@privacyone.ro)
Dana Ududec, Associate (dana.ududec@privacyone.ro)

privacyONE
in alliance with BIRIȘ·GORAN

Br. Aviatorilor nr. 47, etaj 2,
sector 1, Bucureşti

contact@privacyone.ro

www.privacyone.ro