KPMG Legal
TONCESCU & ASOCIATII

Protecția datelor cu caracter personal în timpul reîntoarcerii la normalitate

kpmg.ro

Perioada de la începutul acestui an a fost una nemaiîntâlnită, cel puțin în istoria recentă, și ne-a obligat să ne adaptăm din mers unei noi realități despre care cu un an în urma nu am fi putut să ne imaginăm că va exista în decursul vieților noastre. Adaptarea la noua stare de fapt s-a făcut atât la nivel individual, cât și la nivelul relațiilor de afaceri.

Ca urmare a acestei încercări de adaptare, ne-am lovit de diverse întrebări sau situații cu care s-au confruntat clienții noștri, în general în legătură cu implicații privind protecția datelor cu caracter personal în contextul schimbărilor fundamentale în fluxul afacerii generate de pandemia de COVID-19 și, în special, în ce privește așa-zisa întoarcere la normalitate și încercarea de reluare a activităților de birou.

În aceste condiții, am pregătit în continuare un sumar al celor mai întâlnite întrebări și dileme care s-au născut în această perioadă, având intenția de a oferi claritate cu privire la acest subiect, în contextul unei abundențe de păreri și idei, nu de puține ori contradictorii, lansate în spațiul public în această perioadă.

Sperăm că acest document vă va fi util în rezolvarea unor probleme cu care toate companiile s-au confruntat în această perioadă și vă invităm să regăsiți în această publicație cele mai arzătoare subiecte pe care le-am identificat noi în acest context.

Nu ezitați să ne contactați în cazul în care vreți să aflați mai multe despre oricare dintre aceste chestiuni.

Lectură plăcută!

Cristiana Fernbach

Partner, KPMG Legal - Toncescu și Asociații
Head of Technology, IP & Data Privacy
cfernbach@kpmg.com

Cuprins

1 Verificarea temperaturii angajaților și vizitatorilor

Având în vedere reglementările emise de autoritățile române, companiile care își desfășoară activitatea pe teritoriul României trebuie să desemneze un responsabil pentru a verifica temperatura angajaților (zilnic) și a vizitatorilor. De asemenea, pe viitor, chiar dacă această obligație nu va mai exista, ar putea exista situații în care companiile să își dorească să implementeze în mod voluntar triajul epidemiologic.

În aceste condiții, se pune în special problema dacă triajul epidemiologic prin măsurarea temperaturii corporale a angajaților și vizitatorilor implică o prelucrare de date cu caracter personal.

Într-o primă opinie, o serie de autorități de protecție a datelor din unele state membre au arătat că, atâta timp cât datele privind temperatura nu sunt înregistrate în nicio modalitate, operațiunea de măsurare a temperaturii corporale nu reprezintă o operațiune de prelucrare de date cu caracter personal.

Pe de altă parte, alte autorități de protecție a datelor au arătat că simplul acces la datele privind temperatura corporală, chiar și fără reținerea lor ulterioară, reprezintă o operațiune de prelucrare a datelor cu caracter personal, care trebuie desfășurată în condițiile prevăzute de Regulamentul General de Protecție a Datelor 2016/679 (,,**GDPR**'').

Din moment ce opiniile autorităților europene de protecție a datelor au fost împărțite în ceea ce privește acest aspect, menționăm că Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (,,**ANSPDCP**'') nu a emis o îndrumare oficială care să clarifice în ce măsură verificarea temperaturii reprezintă o prelucrare de date cu caracter personal.

Cu toate acestea, au fost vehiculate o serie de poziții publice ale ANSPDC conform cărora aceasta s-ar ralia opiniei că dispozițiile GDPR devin aplicabile numai în măsura în care informațiile privind temperatura corporală a unei persoane fizice se înregistrează într-un sistem de evidență. Totuși, așa cum am precizat și anterior, această poziție nu a fost confirmată printr-un document oficial.

Pe de altă parte, menționăm că Ordinul comun nr. 874/2020 al Ministerului Sănătății și Ministerului Afacerilor Interne (,,**Ordinul MS-MAI**'') privind instituirea obligativității purtării măștii de protecție, a triajului epidemiologic și dezinfectarea obligatorie a mâinilor pentru prevenirea contaminării cu virusul SARS-CoV-2 pe durata stării de alertă precizează în mod explicit faptul că triajul epidemiologic nu implică înregistrarea datelor cu caracter personal.

Astfel, deși Ordinul MS-MAI nu precizează în mod clar dacă verificarea temperaturii reprezintă o prelucrare de date cu caracter personal, totuși acesta specifică faptul ca datele privind temperatura corporală nu pot fi stocate de către operatorii economici.

În condițiile în care nu există o poziție clară cu privire la această chestiune, pentru evitarea oricărui risc legat de o potențială prelucrare nelegală a datelor cu caracter personal, considerăm că este recomandat ca operatorii economici să își actualizeze informările cu privire la prelucrarea datelor cu caracter personal astfel încât să includă și informațiile cu privire la triajul epidemiologic, atât în informările pentru angajați, cât și în informările pentru vizitatori. Această informare ar trebui să precizeze în mod explicit că datele cu caracter personal cu privire la temperatura corporală nu sunt stocate ulterior măsurării.

Mergând mai departe, conform Ordinului MS-MAI, unui vizitator a cărui temperatura nu depășește 37,3°C și nu prezintă simptome respiratorii, i se permite accesul în incintă cu înregistrarea biroului, camerei sau departamentului unde va merge. Chiar dacă triajul epidemiologic nu presupune o prelucrare a datelor, înregistrarea datelor cu privire la biroul, camera sau departamentul unde vizitatorul va merge reprezintă o prelucrare a datelor cu caracter personal. În acest caz, această prelucrare este efectuată pentru ca autoritățile să identifice acea persoană și pentru a simplifica procedurile în cazul unei anchete epidemiologice. Informațiile cu privire la acest tip de prelucrare a datelor cu caracter personal vor trebui comunicate de asemenea persoanelor vizate.

În acest timp, nu trebuie să uităm că, în conformitate cu prevederile GDPR, operatorii de date cu caracter personal au obligația de a implementa măsuri tehnice și organizatorice adecvate pentru a garanta securitatea prelucrării datelor. În acest sens, recomandăm ca operatorii economici să se asigure că persoana desemnată pentru verificarea temperaturii își asumă obligații de confidențialitate explicite cu privire la acest aspect și că această persoană este instruită corespunzător pentru a păstra confidențialitatea datelor, respectiv a temperaturii măsurate.

Dacă pentru triajul epidemiologic efectuat în baza prevederilor legale am concluzionat că operatorii economici nu vor întâmpina dificultăți de implementare semnificative, în măsura în care respectă recomandările privind informarea persoanelor vizate și instruirea persoanei desemnate pentru verificarea temperaturii, nu același lucru se poate spune despre măsurile de triaj epidemiologic implementate în mod voluntar de către angajator, de la momentul când măsurile legale nu vor mai fi aplicabile.
Având în vedere că în această ipoteză nu ne mai putem baza pe existența unei obligații legale pentru efectuarea triajului epidemiologic, operatorii economici vor trebui să identifice un alt temei pentru prelucrarea datelor cu caracter personal în scopul efectuării triajului epidemiologic.

Chiar dacă am admite că dispozițiile GDPR devin aplicabile numai în măsura în care informațiile privind temperatura corporală a unei persoane fizice se înregistrează într-un sistem de evidență, menționăm totuși că, în ceea ce îi privește pe angajați, angajatorii vor avea cel mai probabil nevoie să documenteze cel puțin cazurile în care temperatura corporală a unui angajat depășește 37,3°C, întrucât, în acest caz, angajatorii vor fi nevoiți să refuze accesul persoanei respective în incintă și să o îndrume către autoritățile sanitare.

În această ipoteză sunt relevante și îndrumările incluse în Declarația privind prelucrarea datelor cu caracter personal în contextul epidemiei de COVID-19 adoptată la 19 martie 2020 de Comitetul European pentru Protecția Datelor („**Declarația**”). Potrivit Declarației, 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.

În ceea ce privește temeiul juridic al prelucrării, în Declarație se arată că GDPR 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.

Recomandări

Luarea măsurilor tehnice și organizatorice necesare pentru a nu se înregistra date privind temperatura corporală

Identificarea corectă și completă a datelor cu caracter personal prelucrate, precum și a temeiurilor juridice de prelucrare

Numirea și instruirea unui responsabil pentru verificarea temperaturii angajaților și vizitatorilor

Respectarea dispozițiilor emise de autorități

Informarea exactă a persoanelor vizate

2 Utilizarea camerelor inteligente de către operatorii economici

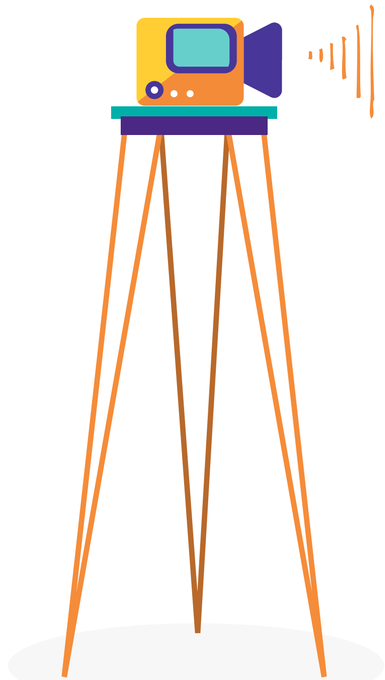
O temă recurentă în dezbaterea publică în această perioadă a fost și chestiunea instalării de camere inteligente în mediul public, dar și posibilitatea instalării acestora în mediul privat. Astfel, operatorii economici ar putea avea în vedere instalarea de camere care să detecteze temperatura automat (camere termografice), purtarea măștii de către indivizi sau respectarea măsurilor de distanțare socială. Aceste dispozitive pot fi de folos în evaluarea riscului de contaminare sau a respectării măsurilor impuse. În cazul în care operatorii economici decid instalarea acestor camere inteligente, este de precizat că instalarea acestora pentru supravegherea angajaților sau vizitatorilor are consecințe importante în ceea ce privește viața privată a acestor persoane. Dezvoltarea unor sisteme numeroase de acest tip prezintă riscul generalizării sentimentului de supraveghere a acestor persoane și a banalizării tehnologiilor intruzive. Din moment ce acest tip de dispozitive captează date și imagini care permit identificarea unei persoane, utilizarea acestora trebuie să respecte principiile stabilite de GDPR, iar operatorii economici care implementează aceste tehnologii trebuie să stabilească un scop bine definit și să identifice baza legală potrivită pentru prelucrarea acestor date. Aceste dispozitive pot fi implementate doar dacă există consimțământul persoanei vizate și dacă sunt necesare în raport cu obiectivele urmărite (adică să nu aducă o atingere disproporționată vieții private). Caracterul necesar și proporțional al recurgerii la asemenea dispozitive trebuie să fie evaluat în raport cu:

- absența altor mijloace mai puțin intruzive pentru realizarea obiectivului;
- importanța datelor prelucrate;
- perimetrul implementării acestor dispozitive (numărul de camere, aria vizuală a acestora, durata utilizării acestora etc.).

În cazul în care dispozitivele inteligente prelucrează categorii speciale de date cu caracter personal, prelucrarea trebuie să se încadreze în excepțiile articolului 9, alineatul (2) din GDPR.

În acest caz, reamintim situația consimțământului în relația angajator-angajat, unde consimțământul exprimat de către angajat ar putea fi un consimțământ invalid deoarece există un dezechilibru de putere între aceste părți și există riscul ca un consimțământ exprimat în acest context să nu fie liber exprimat.

Astfel, operatorii care prelucrează categorii speciale de date cu caracter personal vor fi nevoiți să identifice o altă excepție dintre cele prevăzute de articolul 9, alineatul (2) din GDPR, precum situația 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 situația în care este necesar să se protejeze interesele vitale ale persoanei vizate - articolul 9 alineatul (2) litera (c).
În ceea ce privește termo-scanarea ne putem imagina două scenarii: instalarea de camere termografice la intrarea în sediul operatorului economic pentru a se realiza triajul epidemiologic și instalarea de camere termografice în mai multe birouri din sediul operatorului economic pentru a realiza monitorizarea temperaturii angajaților.



În primul caz, operatorul economic poate realiza triajul epidemiologic prin camera termografică cu soft integrat care este programat să afișeze temperatura și decizia de a intra sau nu în sediu este luată de această cameră, în momentul afișării temperaturii. Astfel, ne putem afla în prezența unui proces individual decizional automatizat deoarece decizia este bazată exclusiv pe prelucrare automată și produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. În aceste condiții, operatorii economici ar trebui să facă o evaluare serioasă a consecințelor legate de prelucrarea datelor cu caracter personal și să realizeze inclusiv o evaluare a impactului asupra protecției datelor.

Cu privire la această situație, poate apărea întrebarea dacă atâta timp cât aceste informații nu sunt stocate, o astfel de activitate ar putea fi tratată ca nereprezentând o prelucrarea de date cu caracter personal. Din punctul nostru de vedere, răspunsul este negativ, întrucât această operațiune desfășurată prin mijloace automate, care presupune o decizie ce produce efecte juridice asupra persoanei vizate, reprezintă fără urmă de îndoială o prelucrare realizată printr-un sistem de evidență a datelor, indiferent de perioada minimă de stocare a datelor.

Având în vedere aceste aspecte, operatorii economici vor fi nevoiți să identifice un temei adecvat de prelucrare a datelor cu caracter personal, să realizeze informarea corectă și completă a persoanelor vizate și să realizeze inclusiv o evaluare a impactului asupra protecției datelor.

În al doilea scenariu, operatorul economic ar putea decide să instaleze camere termografice în mai multe birouri pentru a monitoriza temperatura angajaților. În acest caz, operatorii economici vor fi nevoiți, suplimentar față de recomandările din primul scenariu de mai sus, care rămân aplicabile, să îndeplinească și condițiile care derivă din Legea nr. 190/2018 în legătură cu operațiunea de monitorizare a angajaților prin mijloace electronice, respectiv:

interesele legitime urmărite de angajator să fie temeinic justificate și să prevaleze asupra intereselor sau drepturilor și libertăților persoanelor vizate;

angajatorul să realizeze informarea prealabilă obligatorie, completă și în mod explicit a angajaților;

angajatorul să fi consultat sindicatul sau, după caz, reprezentanții angajaților înainte de introducerea sistemelor de monitorizare;

alte forme și modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator să nu își fi dovedit anterior eficiența; și

durata de stocare a datelor cu caracter personal să fie proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate.

Recomandări

Luarea măsurilor tehnice și organizatorice necesare pentru reducerea la minim a datelor personale prelucrate

Realizarea evaluării impactului asupra protecției datelor

Implementare de reguli specifice pentru protecția datelor și pentru asigurarea securității datelor

Identificarea unui temei adecvat pentru prelucrarea datelor

3 Monitorizarea stării de sănătate a angajaților și observarea simptomelor vizitatorilor

Operatorii economici și-au pus întrebarea cum ar putea să monitorizeze starea de sănătate a angajaților pentru a preveni răspândirea virusului COVID-19 fără să existe riscuri în legătură cu drepturile fundamentale ale omului și protecția datelor cu caracter personal.

În ceea ce privește angajații, monitorizarea stării de sănătate a acestora se realizează prin comunicarea permanentă cu medicul/serviciul de medicina muncii conform Ordinului nr. 3577/2020 al Ministerului Muncii si Protecției Sociale („Ordinul nr. 3577/2020''). Cu ocazia întoarcerii la birou este posibil ca unii angajatori să recurgă la completarea unui chestionar privind simptome COVID-19 pentru a constata starea de sănătate a angajaților, dar completarea sistematică a unui chestionar de către angajați ar trebui evitată conform opiniilor unor autorități europene de supraveghere a protecției datelor.

Pentru a proteja categoriile vulnerabile de angajați, autoritățile competente au recomandat identificarea acestor categorii în cadrul companiilor și amenajarea de spații speciale unde să își desfășoare activitatea. Pentru a identifica aceste categorii, angajatorii o pot face tot prin solicitarea completării unui chestionar. Acest chestionar nu ar trebui să fie excesiv de intruziv. Prin chestionar nu ar trebui să fie solicitate informații despre ce condiții preexistente concrete de sănătate prezintă angajatul, ci doar să se răspundă la întrebarea dacă prezintă sau nu anumite condiții de sănătate care l-ar include în categoria de persoane vulnerabile. Acest tip de chestionare relevă date despre starea de sănătate actuală a angajatului și aceste date sunt sensibile, de aceea companiile cu mulți angajați vor fi nevoite să efectueze o evaluare a impactului asupra protecției datelor pentru a asigura conformitatea cu GDPR în temeiul articolului 35, alineatul (3), litera b).

În ceea ce privește vizitatorii, nu se poate realiza monitorizarea stării de sănătate a acestora, întrucât o astfel de prelucrare ar fi excesivă și ar exceda scopului urmărit, ci doar se pot cere informații (de exemplu: cu privire la istoricul de călătorie) și se pot observa simptome atunci când doresc să intre în sediul operatorului economic.

În ceea ce privește întrebările adresate prin chestionar vizitatorilor care nu includ obținerea unor informații privind sănătatea acelor persoane, prelucrarea acestor date se poate realiza în condițiile articolului 6 din GDPR. Considerăm că temeiurile potrivite pentru prelucrarea datelor personale care nu includ date privind sănătatea ar putea fi: fie consimțământul persoanei vizate, fie realizarea interesului legitim urmărit de operator, fie protejarea interesele vitale ale persoanei vizate sau ale altei persoane fizice.

În situația în care operatorii aleg să își întemeieze prelucrarea acestor date cu caracter personal pe temeiul realizării intereselor legitime ale operatorului, menționăm că va fi necesară realizarea unei evaluări privind interesul legitim.

Indiferent dacă chestionarul este adresat angajaților sau vizitatorilor, operatorii de date ar trebui să îi informeze în prealabil de completarea chestionarului, să solicite minimul necesar de informații pentru atingerea obiectivului urmărit, să implementeze măsurile tehnice și organizatorice pentru asigurarea securității datelor și să stabilească o perioadă scurtă de stocare a acestor date.

Recomandări

- Evaluarea interesului legitim
- Asigurarea securității datelor
- Informarea persoanei vizate
- Evitarea chestionarului sistematic adresat angajaților
- Evitarea chestionarului intruziv în momentul identificării categoriilor vulnerabile
- Evitarea prelucrărilor excesive

4 Politica de revenire la birou din perspectiva GDPR

Având în vedere că măsurile de distanțare socială au generat o schimbare a regimului normal de muncă în cadrul majorității angajatorilor, în acest moment se pune problema revenirii salariaților la activitățile de birou în condiții normale, însă în același timp cu asigurarea unui mediu de lucru sigur pentru angajați. În aceste condiții, este recomandat ca angajatorii să își pregătească o politică de revenire la birou, care să includă cel puțin următoarele aspecte:

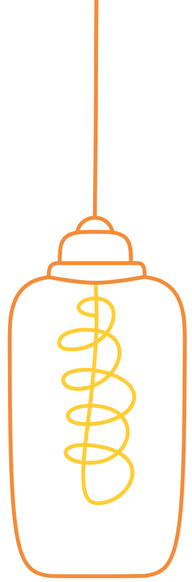
- planul de răspuns împotriva COVID-19 dacă o persoană prezintă simptome;
- chestionarul care trebuie completat de către angajați înaintea revenirii la birou;
- instruirea pentru revenirea la birou pentru angajați;
- numirea și instruirea responsabilului cu verificarea temperaturii;
- măsurile de distanțare socială;
- măsurile pentru păstrarea unei evidențe a persoanelor care intră în sediul operatorului economic;
- planul pentru a proteja categoriile vulnerabile și chestionarul de completat de către aceste persoane.

Cu privire la noua politică de implementat, aceasta trebuie aliniată cu principiile GDPR pentru a se asigura protecția datelor cu caracter personal.

Angajatorii trebuie să aibă pregătit un plan pe care să îl poată aplica în cazul în care apar cazuri de COVID-19 pe premisele acestora. Planul trebuie să prevadă izolarea persoanei suspecte și limitarea numărului de oameni care intră în contact cu acea persoană. De asemenea, angajații trebuie să fie informați cu privire la regulile cuprinse în acest plan pentru a ști cum să reacționeze în situații de risc.

În ceea ce privește verificarea temperaturii, operatorii economici trebuie să stabilească măsurile de respectat de către angajați, cine verifică temperatura și prin ce procedee se poate verifica temperatura. Este de precizat că cea mai utilizată metodă de verificare a temperaturii este cea prin termometru digital non contact care nu înregistrează date.

În legătură cu numirea responsabilului cu verificarea temperaturii, recomandăm ca desemnarea să fie documentată, de exemplu: să se realizeze prin decizie a managementului sau prin procedura aprobată de management. De asemenea, este necesar ca persoana desemnată să fie instruită în mod special cu privirea la utilizarea termometrului non contact – pentru respectarea procedurii instituite prin



Ordinul MS-MAI, dar și cu privire la respectarea obligațiilor de confidențialitate.

Dacă se decide instalarea unei camere termografice pentru verificarea temperaturii în birouri, este de precizat că, în măsura în care aceasta stochează datele și compania are mulți angajați, consimțământul acestora este necesar și efectuarea unei evaluări a impactului asupra protecției datelor ar putea fi necesară pentru a se asigura conformitatea cu GDPR deoarece aceasta reprezintă o prelucrare de date sensibile pe scară largă.

În orice caz, dacă metodele implementate pentru verificarea temperaturii sau orice altă procedură pentru verificarea stării de sănătate a angajaților presupune o stocare de date, operatorul economic trebuie să identifice temeiul juridic în baza căruia efectuează această prelucrare și să implementeze o politică de păstrare a datelor cu caracter personal.

Unii operatori economici și-au pus întrebarea dacă pot solicita angajaților lor să utilizeze o aplicație pentru combaterea virusului COVID-19 și este important de precizat că acest tip de aplicație necesită consimțământul persoanei vizate pentru a fi instalată pe dispozitivul acesteia. O astfel de prelucrare a datelor cu caracter personal ar putea fi realizată în baza consimțământului persoanelor vizate, însă angajatorii vor trebui să se asigure ca acest consimțământ este valabil, fără să fie viciat de dezechilibrul de forțe din relația angajat-angajator. Astfel, angajatorul trebuie să se asigure că angajații nu vor suferi consecințe negative în urma refuzului de a își da consimțământul pentru prelucrarea datelor în această modalitate.

În final, este important de precizat că politica de revenire la birou va presupune și o ajustare a politicilor de protecție a datelor și securității adaptate la contextul actual.

Recomandări

- Implementarea unei politici de revenire la birou conforme GDPR și a unui plan de răspuns împotriva COVID-19
- Respectarea principiului minimizării datelor
- Adaptarea politicilor de protecție a datelor
- Stabilirea perioadei de retenție a datelor

5 Pseudo-ancheta epidemiologică efectuată de angajator

În cazul în care, în cadrul unei companii, un angajat este confirmat pozitiv la testarea pentru COVID-19, angajatorul ar trebui să asigure confidențialitatea acestei informații și să o dezvăluie către ceilalți angajați doar în măsura în care o astfel de dezvăluire este necesară pentru asigurarea sănătății și securității celorlalți salariați.

În aceste condiții, este recomandată evitarea dezvăluirii identității persoanei testate pozitiv. Cu toate acestea, angajatorul are obligația de a informa autoritățile competente (Direcția de Sănătate Publică) din raza căreia își desfășoară activitatea în cazul în care este identificat un angajat diagnosticat cu COVID-19.

Având în vedere Ordinul nr. 3577/2020, în cazul în care un angajat este suspect sau confirmat cu infectare de COVID-19, angajatorul trebuie să informeze persoanele cu care angajatul a venit în contact prelungit și aceste persoane trebuie să se izoleze la domiciliu pentru o perioadă de 14 zile. Așa cum am menționat anterior, dezvăluirea identității persoanei vizate ar trebui evitată, cu excepția cazului când dezvăluirea identității persoanei respective este absolut esențială pentru îndeplinirea obligației de informare și pentru protejarea sănătății persoanelor cu care angajatul diagnosticat pozitiv a venit în contact prelungit.

În acest context, operatorii economici își pun întrebarea în ce situație ar putea efectua chiar ei, în calitate de angajatori, o pseudo-anchetă epidemiologică pentru a informa persoanele cu care a intrat în contact respectivul angajat și ce implicații de protecția datelor presupune această procedură. Companiile au posibilitatea de a solicita o serie de informații salariaților diagnosticați pozitiv, însă trebuie să se asigure că o astfel de solicitare este justificată și proporțională – în niciun caz compania nu se poate substitui Direcțiilor de Sănătate Publică în efectuarea anchetelor epidemiologice.

Stocarea datelor personale (ex: numele persoanelor cu care a intrat în contact angajatul) este o prelucrare de date cu caracter personal și pentru a fi realizată trebuie să se încadreze în unul dintre cazurile prevăzute de articolul 6 GDPR. Astfel, prelucrarea este legală dacă este efectuată în vederea îndeplinirii unei obligații legale (litera c) care îi revine operatorului (conform Ordinului nr. 3577/2020) sau este necesară pentru a proteja interesele vitale (litera d) ale persoanei vizate sau ale altei persoane fizice. În aceste cazuri, numele persoanei vizate poate fi stocat fără consimțământul acesteia.

Alte preocupări în acest caz ar fi cât timp poate păstra angajatorul datele personale colectate de la angajatul suspect/confirmat cu COVID-19, în ce condiții poate divulga numele persoanelor cu care a intrat în contact (fără acordul acestora) autorităților competente, colegilor sau publicului și măsurile de securitate de avut în vedere care să protejeze datele colectate.

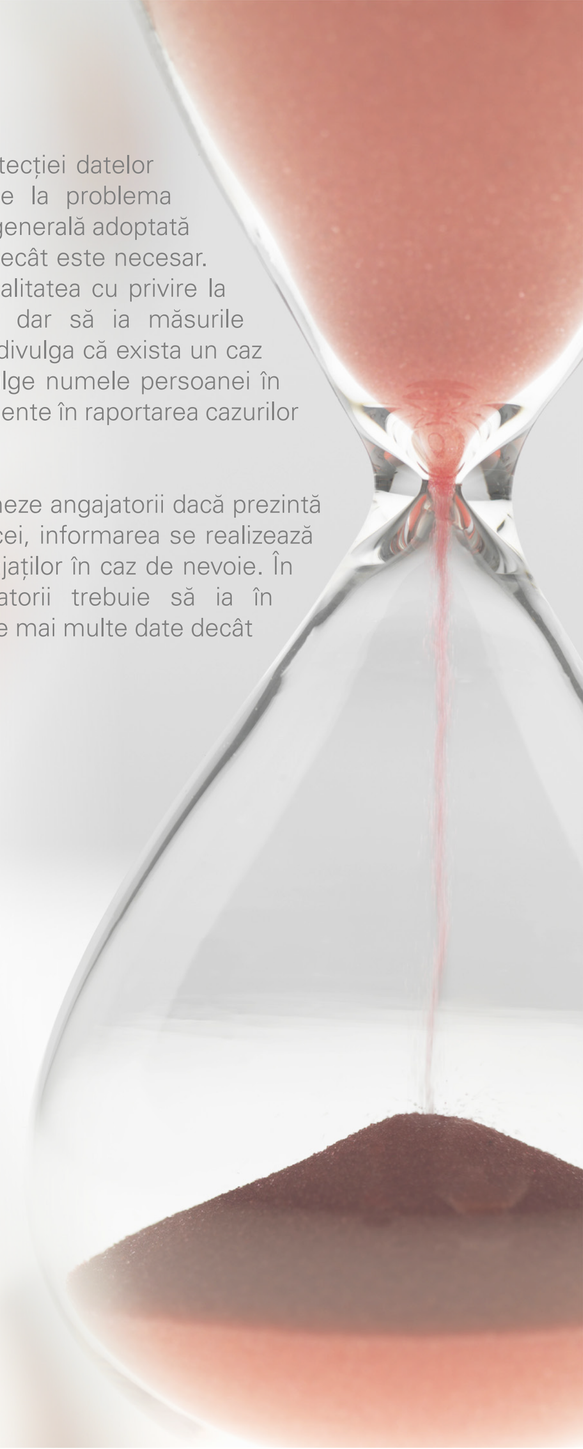
În ceea ce privește divulgarea numelui și a stării de sănătate a unui individ publicului, este de menționat poziția ANSPDCP care a publicat într-un comunicat de presă că aceste informații pot fi divulgate în sfera publică numai dacă persoana vizată își dă consimțământul pentru aceasta. Cu toate acestea, această poziție nu ar trebui să prejudicieze activitățile jurnalistice prevăzute de Legea nr. 190/2018 de punere în aplicare a GDPR. În orice caz, divulgarea în sfera publică ar trebui să se efectueze cu informarea persoanei vizate, respectând demnitatea și integritatea acesteia. Este de menționat că a coopera cu autoritățile competente în efectuarea anchetei epidemiologice în cazul unui angajat confirmat cu COVID-19 nu este o divulgare publică și reprezintă o prelucrare necesară pentru îndeplinirea unei obligații legale a angajatorului și pentru protejarea intereselor vitale ale altor persoane fizice.

Mai multe autorități de supraveghere în domeniul protecției datelor din Uniunea Europeană au publicat opinii cu privire la problema divulgării numelui persoanei infectate colegilor. Poziția generală adoptată a fost că angajatorul ar trebui să nu divulge mai mult decât este necesar. Este recomandat ca angajatorii să păstreze confidențialitatea cu privire la identitatea persoanelor diagnosticate cu COVID-19, dar să ia măsurile necesare pentru protejarea celorlalți salariați (ar putea divulga că exista un caz confirmat în companie, dar nu este indicat să se divulge numele persoanei în cauză). În schimb, autoritățile nu au menționat impedimente în raportarea cazurilor autorităților competente în domeniul sănătății publice.

Este de menționat că angajații au obligația să își informeze angajatorii dacă prezintă simptome ale infectării cu virusul SARS-CoV2. De obicei, informarea se realizează prin chestionare pe care angajatorul le furnizează angajaților în caz de nevoie. În ceea ce privește formularea chestionarelor, angajatorii trebuie să ia în considerare principiul minimizării datelor și să nu solicite mai multe date decât este necesar pentru atingerea obiectivului urmărit.

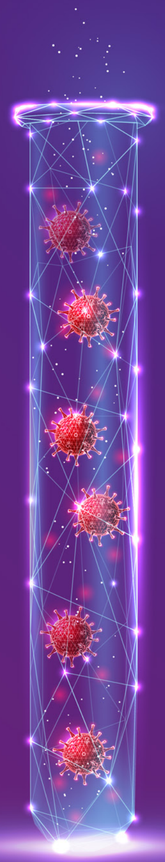
Recomandări

- Respectarea confidențialității identității persoanelor confirmate cu COVID-19
- Cooperarea cu autoritățile competente în domeniul sănătății publice
- Respectarea principiului minimizării datelor
- Luarea măsurilor tehnice și organizatorice pentru securitatea datelor
- Stabilirea perioadei de retenție a datelor



6 Testarea angajaților

În contextul actual, angajatorii și-au pus problema verificării stării de sănătate a angajaților în momentul întoarcerii la birou și au încercat să identifice modalități de reducere a riscului de contaminare în interiorul sediului lor. Cea mai sigură metodă de a identifica existența vreunui risc în legătură cu întoarcerea la birou a angajaților este testarea acestora pentru a stabili dacă starea lor de sănătate le permite întoarcerea la birou.



Menționăm că autoritățile române nu au dat indicații în ceea ce privește testarea obligatorie sau opțională organizată de angajator. Cu toate acestea, autoritatea de supraveghere din Marea Britanie („**ICO**") a publicat un ghid privind testarea angajaților în care arată că legislația privind protecția datelor nu împiedică angajatorii să ia măsurile necesare pentru a menține personalul și publicul în siguranță pe timpul pandemiei, însă trebuie respectate principiile de prelucrare a datelor cu caracter personal.

Temeiul juridic indicat de ICO în cazul testării angajaților este interesul legitim coroborat cu articolul 9, alineatul (2), litera b) „*prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern*". Cu toate acestea, angajatorii care doresc să recurgă la aceste teste trebuie să efectueze propria evaluare a interesului legitim.

Atunci când vorbim de date privind sănătatea și de prelucrare pe scară largă a datelor cu caracter personal, în special în situația în care angajatorul se adresează unui număr mare de angajați, efectuarea unei evaluări a impactului asupra protecției datelor este obligatorie.

Având în vedere prevederile GDPR, dar și pozițiile autorităților de protecție a datelor de la nivel european, în special ale celor din Marea Britanie, Franța și Belgia, considerăm că măsura testării angajaților ar trebui implementată în momentul în care este dovedită necesitatea specifică a acesteia.

O astfel de necesitate ar putea fi justificată atunci când există indicii că unii angajați au simptome sau au fost confirmați cu COVID-19. Într-o astfel de ipoteză, considerăm că angajatorii ar putea implementa măsura privind testarea obligatorie a angajaților pentru a le permite întoarcerea la locul de muncă.

Pe de altă parte, o măsură de testare obligatorie a angajaților, fără a exista suspiciuni întemeiate privind existența unui focar de COVID-19 la nivelul angajatorului, ar putea fi considerată excesivă din punct de vedere al prelucrării datelor cu caracter personal.

Recomandări

- Informarea completă a persoanelor vizate
- Prelucrarea datelor în mod adecvat, relevant, exact și limitat la ceea ce este necesar
- Identificarea unui temei adecvat pentru prelucrarea datelor
- Efectuarea evaluării interesului legitim și a evaluării impactului asupra protecției datelor

Echipa KPMG Legal

Practica de Tehnologie, Proprietate intelectuală și Protecția datelor

Cristiana Fernbach

Partener, KPMG Legal - Toncescu și Asociații

cfernbach@kpmg.com

Membră în Baroul București

Membră a International Association of Privacy Professionals (IAPP)

2010

Universitatea de Management din Singapore, Singapore Asian Business Studies

2009

SDA Școala de Management din Bocconi, Italia

Master în Drept

Freie Universitäts Berlin

Licență în Drept

Universitatea Nicolae Titulescu

Data privacy, IP, Technology

Limbi străine

Nivel avansat în română, engleză și germană

Experiență profesională

Cristiana are o experiență de peste 16 ani în avocatura de business. Ea a fost implicată în numeroase proiecte complexe privind protecția datelor și dreptul noilor tehnologii pentru companii multinaționale. Este specializată în dreptul noilor tehnologii, digital media și protecția datelor.

Descrierea experienței

Experiența ei se întinde pe toate sectoarele, dar cel mai recent se poate observa un accent pe servicii financiare, TMT, publicitate, farmaceutică și servicii educaționale.

Ea a fost recunoscută de The Legal 500 în sectorul TMT pentru că a furnizat consultanță clienților de nivel superior cu privire la probleme de confidențialitate.

Cristiana a fost implicată în asistarea uneia dintre instituțiile financiare de top din România în procesul de urmărire a fluxurilor de date și implementarea GDPR.

Ea a fost implicată în auditul unui distribuitor de top și al vânzătorilor de medicamente din România și a oferit sprijin legal în evaluarea stadiului actual al procesului de conformitate GDPR, precum și în procesul de identificare a măsurilor de atenuare a riscurilor de neconformitate.

A fost implicată în proiectul de conformitate GDPR pentru una dintre cele mai mari agenții de comunicare din România și din regiune, precum și în furnizarea de consultanță și asistență juridică DPO-ului organizației în implementarea măsurilor de conformitate.

Experiența ei cuprinde de la aspecte comerciale și de reglementare, în special pentru sectorul bancar și TMT, până la structurarea complexă a contractelor de licențiere software, gestionarea portofoliului de IP și tehnologia blockchain.

Flavius Florea

Senior Managing Associate, KPMG Legal - Toncescu și Asociații

fflorea@kpmg.com

Membru în Baroul București

Membru a International Association of Privacy Professionals (IAPP)

Master în Drept

Universitatea din București, Facultatea de Drept

Licență în Drept

Universitatea din București, Facultatea de Drept

Data privacy, IP, Technology

Limbi străine

Nivel avansat în română, engleză și franceză

Experiență profesională

Flavius este un avocat entuziast, cu un Master în Drept privat, experimentat atât în domenii precum Telecom, Media și dreptul noilor tehnologii, cât și în probleme de protecția datelor. Flavius are experiență în furnizarea de consultanță legală unui spectru larg de clienți, de la companii internaționale de înaltă importanță până la start-up-uri vibrante pe probleme de protecție a datelor, chestiuni societare și comerciale, de insolvență și privind legislația piețelor de capital. El este interesat în special de domeniul IT&C și a coordonat proiecte majore pentru un portofoliu de clienți diversificat, cu scopul de a asigura conformitatea cu GDPR.

Descrierea experienței

Flavius a fost implicat în furnizarea de consultanță unora dintre cele mai mari nume din industria tehnologică, în litigii de referință pe piața din România, care privesc inclusiv protecția datelor cu caracter personal (dreptul de a fi uitat) și litigii privind drepturile de proprietate intelectuală.

Are experiență în consilierea unui spectru larg de clienți de la companii internaționale de înaltă importanță până la start-up-uri vibrante pe probleme de confidențialitate a datelor, chestiuni comerciale și dreptul comerțului electronic.

Cătălina Fînaru

Senior Associate, KPMG Legal - Toncescu și Asociații

catalinafinaru@kpmg.com

Membră în Baroul București

Licență în Drept

Universitatea din București

Data privacy, IP, Technology

Limbi străine

Nivel avansat în română și engleză

Experiență profesională

Cătălina are experiență extinsă în consultanța privind protecția datelor, dreptul noilor tehnologii și comerț electronic. Ea a fost implicată într-un număr semnificativ de proiecte de conformitate GDPR și a oferit asistență juridică privind măsurile de atenuare a riscurilor și privind cadre complexe contractuale de confidențialitate a datelor.

Descrierea experienței

- Cătălina a fost implicată în proiecte complexe care implică consultanță juridică cu privire la toate aspectele proceselor de conformitate GDPR.
- Cătălina a oferit asistență juridică în procesul de transferuri internaționale de date cu caracter personal atât în UE, cât și în afara UE, precum și în răspunsul la incidentele de încălcare a datelor.
- Cătălina a fost implicată în asistarea uneia dintre instituțiile financiare de top din România în procesul de urmărire a flow-urilor datelor și implementarea GDPR.
- La primul Global Legal Hackathon din România, Cătălina a câștigat alături de echipa sa premiul special pentru cel mai bun produs pentru dezvoltarea unei aplicații GDPR care este utilă pentru gestionarea programului de conformitate în organizații.

Contact:

Laura Toncescu

Partner,
Head of KPMG Legal - Toncescu și Asociații

ltoncescu@kpmg.com

Cristiana Fernbach

Partner, KPMG Legal - Toncescu și Asociații
Head of Technology, IP & Data Privacy

cfernbach@kpmg.com

KPMG Legal
TONCESCU & ASOCIATII

KPMG Legal

TONCESCU & ASOCIATII