

România este pe cale sa aprobe Directiva privind avertizorii de integritate. Cât de pregatite sunt companiile pentru noile reglementari?



Circa 42% dintre fraudele din companii au fost depistate în urma sesizărilor primite de la avertizorii de integritate (i.e. persoane care raportează, într-un context profesional, fapte neetice, încălcări de legi, reguli sau proceduri), conform unui studiu al Asociației Internaționale a Examinatorilor de Frauda.

Astfel de raportări ar trebui încurajate având în vedere că fraudele/criminalitatea economică produc atât pierderi financiare semnificative, cât și reputaționale, respectiv conduc la erodarea încrederii pe care publicul o are într-o instituție/companie.

România, dar și alte state europene, nu au încă o legislație clară în acest domeniu și există o teamă de consecințe negative pe care le pot suporta avertizorii de integritate ca urmare a raportărilor. În acest context, la data de 16 decembrie 2019 Uniunea Europeană a adoptat Directiva 2019/1937 privind protecția persoanelor care raportează încălcări ale dreptului european, aceasta urmând a fi implementată în legislația tuturor statelor membre, inclusiv prin extinderea domeniului sau de aplicare, la aspecte legate de încălcarea dreptului național.

Pe scurt, persoanele care raportează încălcări legislative (ex. acte frauduloase, dar nu numai), vor fi protejate de lege și nu vor trebui să se teamă de consecințe, iar companiile vor trebui să implementeze proceduri interne de tratare a acestor raportări.

În România, deși termenul limită pentru transpunerea la nivel național a directivei a expirat deja (i.e. decembrie 2021), legea ce ar urma să fie adoptată în acest sens se află încă în procedura legislativă în Parlament. În stadiul actual, se preia destul de fidel textul Directivei, fiind incluse prevederi legale referitoare la răspunderea civilă, disciplinara, contravențională sau penală, după caz, a celor ce încalca reglementarea, dar și sancțiuni corespunzătoare.

Anticipând nevoile care vor fi generate de noua legislație a avertizorilor de integritate, PwC a dezvoltat o platformă online care facilitează raportarea și investigarea sesizărilor avertizorilor de integritate, identificând totodată prin implicarea unei echipe multidisciplinare PwC și D&B printr-o analiză de tip forensic și, respectiv, juridic (dreptul muncii și protecția datelor personale) și aspectele cele mai importante pe care reprezentanții companiilor ar trebui să le ia în considerare încă de acum, spre a nu fi ulterior luați prin surprindere la momentul când se vor aplica aceste norme ce conțin exigențe extrem de ridicate și sancțiuni aferente dure.

Ce prevede directiva?

Directiva stabilește, printre altele, cadrul de protecție a avertizorilor de integritate, aria de aplicabilitate, tipurile de canale de raportare, respectiv cine ar trebui să le implementeze (ex. instituții publice și entități private cu mai mult de 50 de angajați) și responsabilități (ex. atribuții de primire și investigare a sesizărilor primite).

Protecția se aplică atât angajaților actuali care raportează fapte sau suspiciuni de încălcare a legii, cât și foștilor angajați, celor în proces de recrutare sau celor care doresc să își pastreze anonimatul. Legat de ultimul aspect, conform Directivei, raportarea poate fi făcută și anonim, însă rămâne de văzut ce prevederi va avea legea din România cu privire la raportările anonime.

Canalele de raportare pot fi online, cutii poștale, linii telefonice dedicate, întâlniri la solicitarea persoanei care efectuează raportarea. Indiferent de formă, canalele trebuie să permită protecția identității avertizorului, iar datele cu caracter personal trebuie prelucrate conform prevederilor legale aplicabile.

Directiva mai prevede următoarele termene de informare: 1) avertizorul trebuie să fie informat de primirea raportării în termen de cel mult șapte zile calendaristice de la primirea acesteia; 2) avertizorul trebuie să fie informat asupra stadiului acțiunilor subsecvente raportării, în termen de trei luni de la data confirmării primirii sesizării.

Principalul canal de raportare este cel intern implementat de o companie, urmat de canalele externe de raportare implementate de autorități competente, și de divulgarea în spațiul public. Avertizorul poate decide să folosească direct canalul extern de raportare, dacă canalele interne nu există sau dacă considera că aspectele sesizate nu pot fi remediate prin intermediul canalelor interne de raportare. În cazul în care raportarea pe canalele interne sau externe nu a dat rezultate sau dacă avertizorul nu a fost notificat cu privire la acțiunile subsecvente în termen de trei luni (sau șase luni în cazurile temeinic justificate), acesta poate alege ca o ultimă soluție divulgarea în spațiul public. Divulgarea publică poate fi utilizată și în caz de pericol iminent sau evident pentru interesul public (ex. risc de prejudiciu ireversibil) sau dacă prin utilizarea raportării externe există un risc de represalii / ca încălcarea să nu fie remediată.

Ce pot și trebuie să facă încă de acum societățile pentru a se conforma cerințelor legislative aplicabile după transpunerea Directivei în lege și intrarea acesteia din urmă în vigoare?

Modalitatea de implementare a prevederilor viitoarei legi pentru companii este foarte importantă, mai ales în contextul impactului pe care un asemenea act normativ l-ar putea avea asupra afacerii. Să nu uităm că, de exemplu, nerespectarea reglementărilor în materia protecției datelor cu caracter personal poate conduce la aplicarea unor sancțiuni pecuniare semnificative (ex. de până la 4% din cifra de afaceri globală) sau că anumite companii pot fi atrase în scandaluri media cu efecte financiare și reputaționale de nedorit.

În aceste condiții, ținând cont și de complexitatea și tehnicitatea problemelor în discuție, ar trebui ca entitățile private să aibă în vedere încă de dinaintea intrării în vigoare a viitoarei legi ce transpune Directiva, respectiv:

- Revizuirea și actualizarea politicilor de conformitate pentru a răspunde cerințelor viitoarei legi care va transpune Directiva.
- Aspectele relevante privind protecția datelor cu caracter personal, cum ar fi adaptarea politicilor de protecția datelor, redactarea sau revizuirea notelor de informare aferente acestor noi activități de prelucrare.
- În măsura în care nu există deja, implementarea unor canale interne specifice de raportare. Dacă astfel de canale de raportare sunt deja implementate, analizarea necesității unor actualizări, precum și evaluarea accesibilității și a gradului de ușurință cu care acestea pot fi folosite.
- (Re)informarea și încurajarea angajaților cu privire la posibilitățile de raportare, dar și modificarea

corespunzatoare a reglementarilor interne aplicabile (i.e. regulament intern, politici specifice aplicabile în diferite situații în detalierea acestuia etc.).

- Desemnarea și instruirea unei / unor persoane imparțiale cu atribuții de primire și investigare a sesizărilor primite. De avut în vedere ca persoana care primește sesizarea nu trebuie să fie și cea care efectuează investigația. De altfel, formarea unei echipe de investigație și selectarea procedurilor de investigație sunt aspecte foarte importante și poate afecta rezultatul investigației. Echipa de investigație trebuie să fie formată din oameni care au experiența, cunoștințele și abilitățile necesare pentru a efectua investigația, iar metodele selectate (interviuri, analiza de documente, computer forensic, etc) trebuie să asigure identificarea faptelor relevante. De exemplu investigația unei raportări financiare frauduloase presupune ca în echipă să fie o persoană cu cunoștințe economice. Surse importante de informații în investigații sunt interviurile și echipamentele IT. Prin urmare, în echipă trebuie să fie un investigator experimentat care știe ce să întrebe și când să întrebe, respectiv o persoană experimentată în computer forensic. Cadrul legal este de asemenea vital de observat în orice investigație.
- Evaluarea resurselor necesare implementării și gestionării canalelor interne de raportare și, în funcție de nevoie, luarea în considerare a posibilității de a contracta serviciile unor furnizori existenți în piața de servicii de tip forensic, care pot oferi suport și consultanță integrată 1) cu implementarea și evaluarea canalelor de raportare; 2) cu investigarea sesizărilor primite, mai ales atunci când cazurile sunt complexe și riscante pentru o companie (ex. investigații de sesizări de acte de corupție, spalare de bani, harțuire, scheme complexe de fraudă, cazuri de harțuire, etc).

Chiar dacă momentul în care se va aplica noua lege este încă incert, este de așteptat ca acest proces să fie accelerat de riscul inerent al unei proceduri de infringement inițiate de către Comisia Europeană, așa cum s-a mai întâmplat în alte cazuri când România a ratat termenele de transpunere a actelor europene. Ar fi deci doar o iluzie pentru cei vizați de normele mai sus-descrie să creadă că ar mai fi ceva timp pentru a se pregăti în vederea unei aplicări corespunderilor acestora când, în realitate este deja destul de târziu.

Astfel, companiile ar trebui să înceapă încă de acum să acționeze în sensul pregătirii implementării prevederilor, pentru a nu avea ulterior dificultăți și surprize neplăcute.