alcool, nu faptul de a fi consumat alcool anterior programuluide lucru. Putem, de asemenea, sancționa disciplinar consumul de băuturi alcoolice întimpul orelor de program.

Dacă există suspiciuni privind consumul de alcool, angajatorul va putea să se adreseze poliției. De altfel, pentru anumite activități, consumul de alcool constituie chiar infracțiune: de exempu, părăsirea postului şi prezenţa la serviciu sub influenţa alcooluluisau a altor substanţe pentru cei ce lucrează în domeniul siguranţei circulaţiei pe căile ferate (art. 331 din Codul penal).

Regulamentul intern va cuprinde, de asemenea, și noi abateri disciplinare, cum ar fi,spre exemplu, neglijența în păstrarea datelor personale ale altor salariați.

7. Responsabilul cu protecția datelor

Desemnarea unui astfel de operator este obligatorie numai în anumite cazuri, specialdeterminate în Regulament, respectiv dacă:

– prelucrarea este efectuată de o autoritate sau un organism public;

– operațiunile de prelucrare sunt periodice și sistematice;

– privesc prelucrarea pe scară largă a unor date speciale;

– constituie activitatea principală a firmei.

Atunci când există, responsabilul cu protecția datelor poate fi (în funcție de obiectulde activitate și de dimensiunile companiei):

a) un salariat special angajat cu acest scop.

Profesia de responsabil cu protecția datelor cu caracter personal a fost introdusă în ClasificareaOcupațiilor din România, prin Ordinul nr. 5.384/2017 al ministrului muncii și justiției sociale privindmodificarea şi completarea Clasificării ocupaţiilor din România – nivel de ocupaţie (şase caractere) – cod COR: 242231, nivelul de studii – 4 (studii superioare).

Trebuie observat că responsabilul cu protecția datelor are o anumită autonomie încadrul companiei, chiar și când are calitatea de salariat, cât privește activitatea de protecțiea datelor, neputând fi sancționat sau concediat pentru îndeplinirea sarcinilor sale.

El poate fi contactat direct de către orice salariat, în vederea exercitării drepturilor lorpotrivit Regulamentului european.

În cazul instituțiilor publice vor trebui respectate toate celelalte condiții ale managementuluiresurselor umane aplicabile aici: de la prezența postului în organigrama aprobatăprin at normativ până la desfășurarea unui concurs în vederea angajării;

b) un salariat pre-existent, căruia i s-au adăugat în fișa postului responsabilități însfera protecției datelor.

Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții, dar niciunadintre aceste sarcini și atribuții nu trebuie să genereze un conflict de interese (spre exemplu,funcții din conducerea organizației, care să atragă capacitatea de a lua decizii chiarîn domeniul colectării de date – director, director executiv, director resurse umane etc.).

În cazul în care atribuțiile responsabilului cu protecția datelor sunt preluate de cătreun angajat pre-existent, se va încheia cu acesta un act adițional. Este necesar acordulsalariatului în discuție;

c) un prestator de servicii, cu care s-a încheiat contract civil.

Astfel, potrivit art. 37 alin. (6) din Regulament, responsabilul cu protecția datelor poate fi un membru alpersonalului operatorului sau persoanei împuternicite de operator sau poate să îșiîndeplinească sarcinile în baza unui contract de servicii;

d) un salariat sau un colaborator „partajat" de mai multe companii.

Astfel, Regulamentul prevede că un grup de întreprinderi poate numi un responsabil cu protecțiadatelor unic, cu condiția ca responsabilul cu protecția datelor să fie ușor accesibildin fiecare întreprindere.

În cazul în care operatorul sau persoana împuternicită de operator este o autoritatepublică sau un organism public, poate fi desemnat un responsabil cu protecția datelorunic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structuraorganizatorică și dimensiunea acestora.

Din punct de vedere juridic, acest tip de contract se numește „job sharing"; el nu estereglementat la noi. Ca urmare, modul concret prin care responsabilul cu protecțiadatelor va fi partajat între mai multe firme sau instituții publice va putea fi desfășurareaunui contract cu fracțiune de normă pentru fiecare dintre ele.

Operatorul sau persoana împuternicită de operator publică datele de contact aleresponsabilului cu protecția datelor și le comunică autorității de supraveghere.

Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

(a) informarea și consilierea angajatorului și a angajaților care se ocupă de prelucrarecu privire la obligațiile care le revin în temeiul regulamentului și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

(b) monitorizarea respectării reglementărilor referitoare la protecția datelor și a politicilorangajatorului în ceea ce privește protecția datelor cu caracter personal, inclusivalocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupraprotecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul35. Într-adevăr, în art. 35 din Regulament se prevede că în cazul în care untip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibilsă genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice,operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilorde prelucrare prevăzute asupra protecției datelor cu caracter personal. Larealizarea unei evaluări a impactului asupra protecției datelor, operatorul solicităavizul responsabilului cu protecția datelor, dacă acesta a fost desemnat;

(d) cooperarea cu autoritatea de supraveghere;

(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privindaspectele legate de prelucrare, inclusiv consultarea prealabilă cu autoritatea desupraveghere pentru a obține autorizarea din partea acesteia în legătură cu prelucrareaspecială de date, precum și, dacă este cazul, consultarea cu privire la oricealtă chestiune.

Ca urmare, fișa postului responsabilului cu protecția datelor se va întocmi pornindu-sede la aceste atribuții. Operatorul sprijină responsabilul cu protecția datelor înîndeplinirea acestor sarcini, asigurându-i resursele necesare pentru executarea acestorsarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare,și pentru menținerea cunoștințelor sale de specialitate.

Este necesară, așadar, urmarea de cursuri de formare profesională. Chiar dacă nu există în prezentcursuri acreditate, totuși o evaluare atentă a cursurilor de pe piață va putea conduce angajatorul (operator) la identificarea celor mai potrivite cursuri, astfel încât responsabilul cu protecția datelor să îșipoată îndeplini aceste atribuții.

Ca profil, Regulamentul prevede că responsabilul cu protecția datelor ar trebui să fie desemnat pebaza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile dindomeniul protecției datelor, precum și pe baza capacității de a-și îndeplini sarcinile (art. 37 alin. (5)).Adăugăm la acestea și cunoștințele de IT, utile mai ales în ipoteza stocării de date în format electronic.

Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitateaîn ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptulUniunii sau cu dreptul intern.

În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în modcorespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura,domeniul de aplicare, contextul și scopurile prelucrării. El este cel care va notifica, lanevoie, la Autoritatea națională de supraveghere, orice incident de securitate.

Notificarea va cuprinde cel puțin:

(a) caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo undeeste posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precumși categoriile și numărul aproximativ al înregistrărilor de date cu caracter personalîn cauză;

(b) numele și datele de contact ale responsabilului cu protecția datelor sau un altpunct de contact de unde se pot obține mai multe informații;

(c) consecințele probabile ale încălcării securității datelor cu caracter personal;

(d) măsurile luate sau propuse spre a fi luate de operator pentru a remedia problemaîncălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentruatenuarea eventualelor sale efecte negative.

8. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

Reglementarea inițială a acestui organism și a atribuțiilor sale era cuprinsă în Legeanr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale deSupraveghere a Prelucrării Datelor cu Caracter Personal, publicată în Monitorul Oficialnr. 391 din 9 mai 2005, cu modificările și completările ulterioare. Ca urmare a intrării învigoare a Regulamentului de protecție a datelor, acest act normativ a fost modificat prinLegea nr. 129/2018 pentru modificarea şi completarea Legii nr. 102/2005, precum şipentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrareadatelor cu caracter personal şi libera circulaţie a acestor date, publicată