Regulamentul intern privind prelucrarea datelor personale

Actualizat la data 31.07.2018

Preambul

În 25 mai 2018 a intrat în vigoare Regulamentul European nr. 2016/679 privind protectia persoanelor fizice referitor la prelucrarea datelor personale si libera circulatie a acestor date, care instituie dreptul comun în această materie.

Scopurile pentru care a fost adoptat regulamentul european sunt: unificarea legislației și practicii statelor europene, cresterea gradului de protecție a datelor personale, crearea unui climat de încredere în contextul dezvoltării mediului IT și al stocării datelor în cloud, domenii care au luat amploare în ultimul timp și care se vor dezvolta în continuare, precum și celelalte scopuri menționate în preambulul regulamentului european.

În acest context, subscrisa, numita mai jos „operator", ne aliniem cerințelor europene impuse, adoptând o serie de reguli cu privire la prelucrarea datelor personale.

CAPITOLUL I

Reguli particulare privind prelucrarea datelor personale

Art.1 Activitatea operatorului

Operatorul dezvoltă un sistem informatic de tip gestiune baze de date. Programul presupune mai multe conturi de utilizator, care permit clienților-utilizatori să gestioneze date din activitatea proprie. Datele se pot stoca local, într-un spațiu de stocare al clientului, sau central, într-un spațiu de stocare oferit de operator. În situația în care se va alege prima soluție, atragem atenția că va deveni și clientul operator de date personale cel puțin sub forma stocării lor și va avea responsabilitatea respectării legii speciale în prelucrarea lor.

Prin intermediul programului se pot prelucra date introduse de beneficiar și date obținute informatizat din bazele de date publice obținute în numele și pentru beneficiar. Toate acestea nu sunt furnizate de furnizor, ci de beneficiar și de administratorii bazelor de date publice, iar răspunderea asupra lor aparține acestora, după cum urmează, conform legii:

-datele introduse de beneficiar:

-categorii de date: beneficiarului i se solicită doar informațiile minime necesare funcționării programului, majoritatea fiind informații publice: număr dosar, denumire debitor, sediu

debitor, ș.a., printre ele putându-se afla și date cu caracter personal: numele pesoanelor fizice monitorizate, ș.a.

-furnizorul nu are niciun control asupra datelor, doar le stochează astfel cum au fost transmise.

-răspunderea pentru date: aceste informații introduse de beneficiar sunt personale, numai beneficiarul are acces la ele, iar răspunderea pentru ele aparține beneficiarului, inclusiv în ceea ce privește prelucrarea datelor cu caracter personal și informarea persoanelor vizate ale căror date se prelucrează.

-datele obținute din bazele de date publice pe cale informatizată:

-categorii de date: acestea sunt informații publice, putând avea acces la ele orice persoană: stări ale persoanelor și bunurilor care apar în baze de date, situații financiare, ș.a., iar printre ele se pot afla și date personale ale persoanelor fizice care apar în acele evidențe: nume, prenume, ș.a.

-rolul furnizorul: toate datele din bazele de date publice sunt obținute în numele și în interesul clientului, operatorul acționând ca mandatar pentru beneficiar, care intermediază obținerea informatizată, stocarea și punerea la dispoziția beneficiarului prin intermediul programului informatic, conform regulilor din contractul încheiat cu clienții. Datele sunt prezentate beneficiarilor fără ca furnizorul să intervină asupra conținutului lor. Acestea pot fi însă aranjate grafic, explicate, sau combinate și pot fi prezentate în rapoarte detaliate despre o anumită entitate (firmă, dosar).

-răspunderea pentru date: aparține administratorilor acelor baze de date, inclusiv în ceea ce privește prelucrarea datelor cu caracter personal și informarea persoanelor vizate ale căror date se prelucrează. Persoane vizate de prelucrarea datelor personale se vor adresa administratorilor bazelor de date. Atragem atenția că unii administratori ai acestor baze de date impun restricții de redistribuire în scopul de a nu transmite mai departe informația respectivă, restricții care se aplică beneficiarului informației, respectiv clientului pentru care operatorul acționează ca mandatar.

Art.2 Persoanele vizate la nivelul operatorului, sursele de informare, categoriile de date prelucrate de operator

Operatorul prelucrează următoarele categorii de date personale pentru următoarele categorii de persoane fizice.

PERSOANA VIZATA ȘI SURSE DE INFORMAȚII	CATEGORII DE DATE PERSONALE
I. Persoanele aflate în raporturi juridice cu operatorul sau care doresc sa intre în raporturi juridice cu operatorul: clienți, reprezentanții lor	-datele de identificare: nume, prenume, adresa de domiciliu, adresa de corespondență, e-mail, telefon, cont bancar, CNP, seria și numărul actelor de identitate și alte informatii rezultate din acestea (data și locul nașterii, cetațenia, ș.a.)

legali, parteneri contractuali, furnizori, finanțatori, angajați, voluntari, colaboratorii, potențiali clienți, angajați care urmează un proces de recrutare, ș.a. Avem în vedere pe cei care sunt persoane fizice, precum și pe reprezentanții legali sau convenționali ai acestora Surse de informații: datele personale pot fi puse la dispoziție de persoana vizată, reprezentantul ei, pot fi furnizate online pe e-mail, telefonic, sau prin completarea formularelor web, pot fi obținute din bazele de date publice, disponibile pentru consultare online sau la cerere, pot fi obținute de la autorități sau diverse insitituții publice.	-semnătura -informații privind seriozitatea, bonitatea persoanei vizate -pentru angajați, colaboratori, voluntari: date socio-demografice, ocupația, studii, locuri de muncă, funcții, sancțiuni, premii, venituri salariale, rețineri salariale, preferințe, date privind starea de sănătate specifică postului, fotografii -date de localizare: IP-ul echipamentului de calcul de pe care se accesează site-ul operatorului, date GPS -informații rezultate în urma înregistrării video la sediu sau la punctele de lucru, respectiv audio sau în mediile de comunicare online (e-mail, chat, ș.a.) -orice alte informații care derivă din acestea în urma prelucrărilor efectuate de operator, cum ar fi: istoric contractual, clasificarea persoanelor vizate după diverse criterii, informații specifice despre produsele și serviciile oferite de operator și despre felul în care persoana vizată le-a utilizat;
II. Date despre persoane vizate pe care le dețin clienții și le introduc aceștia în programul pus la dispoziție în interesul propriu al acestora și Datele obținute de operator din baze de date externe publice (portalul instanțelor, registrul comerțului, arhiva de garanții, ș.a.) în calitate de mandatari ai clienților și pe care le pune la dispoziție acestora	datele de identificare ale debitorilor, creditorilor, terților, situații economice, datelele de identificare ale utilizatorilor (nume prenume, coduri de acces), ș.a. situațiile juridice, economice, ș.a. privind persoanele și bunurile care apar în bazele de date monitorizate.

Art.3 Scopurile în care sunt prelucrate datele personale la nivelul operatorului. Mijloacele de prelucrare

-evaluarea și verificarea persoanei, minimizarea riscului pe care îl implică raportul juridic cu acesta,

-negocierea, începerea, executarea, menținerea, încetarea și arhivarea relației contractuale;

-oferirea de asistență, înștiințarea despre produsele și serviciile oferite, personalizarea acestora, îmbunătățirea și dezvoltarea produselor și serviciilor oferite, fidelizarea clientelei;

-înregistrarea audio a convorbirilor telefonice pentru a furniza dovada consimțământului cu privire la anumite servicii și pentru a îmbunătății calitatea serviciilor oferite;

-securizarea video a locației operatorului, prevenirea și combaterea faptelor sancționate de lege;

-identificarea online a persoanelor vizate, accesul la produse și servicii;

-monitorizarea activității;

-prevenirea și combatarea faptelor sancționate de lege;

-activități de registratură, corespondență, curierat, arhivare;

-analiza activității operatorului (analiza portofoliului de clienți, angajați, colaboratori, altor resurse, crearea unei baze de date interne, utilizată centralizat, de către departamentele și aplicațiile interne ale operatorului), raportări financiare și către autorități;

-solutionare litigii/ proceduri, efectuare expertize;

Operatorul folosește mijloacele de prelucrare clasice și cele puse la dispoziție de tehnologia actuală: mijloace materiale (dosare, registre, formulare de hârtie ș.a.), mijloace electronice (fișiere, tabele foi de calcul, ș.a). Operatorul va asigura securitatea lor conform prevederilor Regulamentului European: asigurarea cu parole, desemnarea unor persoane care prezintă garanții adecvate, ș.a.

Art. 4 Destinatarii potențiali ai datelor personale deținute de operator

În general, regimul accesului la datele personale este asemănător cu cel practicat de orice altă persoană juridică care activează în domeniul de servicii în care activează și operatorul.

În vederea îndeplinirii scopului respectiv, este posibil să aibă acces la datele personale următoarele persoane, în condițiile în care accesul la datele personale este limitat doar la cele necesare realizării scopului:

-angajații, voluntarii interni ai operatorului, sau colaboratorii externi;

-persoanele care asigură dezvoltarea, mentenanța și securitatea IT;

-contabilii, auditorii, experții, furnizori de servicii în vederea efectuării plăților on-line, instituții financiar-bancare și de asigurare (ex: când se efectuează plăți, se utilizează numele și contul bancar);

-societăți de curierat (ex: când se expediază comunicări, se utilizează numele și domiciliul);

-medicul de medicina muncii (ex: când se efectuează anual evaluarea sănătății angajaților, se utilizează numele și starea de sănătate);

-autorități publice, birouri notariale, cabinete de avocatură (ex: când se dau declarații sau se recuperează debite neplătite, se utilizează datele de identificare);

-societăți de arhivare (ex: când se arhivează documentele, se predau unui furnizor de servicii de arhivare sau Arhivelor Naționale);

-finanțatori, sponsori (ex: pentru a analiza realitatea cheltuirii sumelor pe care le finanțează);

-persoane juridice către care operatorul a cesionat contractele, drepturile sau obligațiile legate de acestea sau a subcontractat serviciile oferite;

-furnizori de servicii IT. (Ex: fotografii ale persoanelor vizate pot fi publicate cu acordul lor pe site-ul operatorului/medii de socializare, în scopul promovării produselor și serviciilor oferite de operator);

-alte persoane, pentru realizarea scopului respectiv;

În cazul clienților care folosesc un program furnizat de operator sau site-ul operatorului accesând contul propriu, fiecare are acces la datele proprii și pe care le introduce în program, fără a putea avea acces la datele altui client sau introduse de alt client și fără ca datele lui să poată fi accesate de alt client. În acest caz, accesul la datele personale este mai restrâns, putând să le acceseze: angajații interni ai operatorului, colaboratorii externi care asigură dezvoltarea, mentenanța, securitatea IT.

CAPITOLUL II

Reguli generale privind prelucrarea datelor personale

Art. 5 Terminologie

În acest regulament termenii folosiți sunt cei definiți de Regulamentul european nr. 2016/679 privind protectia persoanelor fizice referitor la prelucrarea datelor personale si libera circulatie a acestor date (numit în continuare Regulamentul european), de Legea nr. 190/2018, sau sunt cei folosiți în vocabularul curent al limbii române, sau de specialitate, după caz:

Conform Regulamentului european:

"date personale" sau "date cu caracter personal" = orice informaţii privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

"date" = date personale, date fără acest caracter, sau ambele categorii de date, în funcție de context;

"date publice" = date cu sau fără caracter personal, disponibile publicului online sau la cerere;

"prelucrare" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor personale sau asupra seturilor de date personale, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

"restricţionarea prelucrării" înseamnă marcarea datelor personale stocate cu scopul de a limita prelucrarea viitoare a acestora;

"creare de profiluri" înseamnă orice formă de prelucrare automată a datelor personale care constă în utilizarea datelor personale pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

"pseudonimizare" înseamnă prelucrarea datelor personale într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date personale unei persoane fizice identificate sau identificabile;

"sistem de evidenţă a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

"operatorul" = subscrisa, persoană juridică de drept român

"persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

"destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele personale, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile publice cărora li se pot comunica date personale în cadrul unei anumite anchete în conformitate cu dreptul Uniunii Euripene sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor personale, în conformitate cu scopurile prelucrării;

"parte terţă" înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de opertaor şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date personale;

"consimţământ" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele personale care o privesc să fie prelucrate;

"încălcarea securităţii datelor personale" înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor personale transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

"date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

"date biometrice" înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

"date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

Conform Legii nr. 190/2018:

> "număr de identificare național" = numărul prin care se identifică o persoană fizică în anumite sisteme de evidență și care are aplicabilitate generală: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială de sănătate.
>
> "îndeplinirea unei sarcini care serveşte unui interes public" = include acele activităţi ale partidelor politice sau ale organizaţiilor cetăţenilor aparţinând minorităţilor naţionale, ale organizaţiilor neguvernamentale, care servesc realizării obiectivelor prevăzute de dreptul constituţional sau de dreptul internaţional public ori funcţionării sistemului democratic, incluzând încurajarea participării cetăţenilor în procesul de luare a deciziilor şi a pregătirii politicilor publice, respectiv promovarea principiilor şi valorilor democraţiei.

În sensul prezentului regulament, "clientul" = persoana care încheie un contract cu operatorul, în general persoanele care beneficiază de serviciile și produsele furnizate de operator. Este asimilat și potențialul client, respectiv persoana care testează serviciile și produsele oferite de operator sau se află în perioada precontractuală.

Art. 6 Caracteristicile datelor personale în cadrul prelucrării. Principii ale prelucrării

Datele personale sunt:

> a) prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată ("legalitate, echitate şi transparenţă");
>
> b) colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale în condițiile în care se efectuează cu respectarea garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.) ("limitări legate de scop");
>
> c) adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor personale");
>
> d) exacte şi, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele personale care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere ("exactitate");
>
> e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele personale; datele personale pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate

exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu respectarea garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.) ("limitări legate de stocare");

f) prelucrate într-un mod care asigură securitatea adecvată a datelor personale, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate şi confidenţialitate").

Operatorul are obligaţia să respecte prevederile alineatului precedent şi să asigure îndeplinirea acestor prevederi în condițiile prevăzute de regulament ("responsabilitate").

Art. 7 Temeiul și condițiile prelucrării. Începerea operațiunilor de prelucrare. Legalitatea prelucrării

Prelucrarea datelor personale este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele situații:

a) Regula: consimțământul persoanei vizate. Consimțământul pentru prelucrarea datelor sale personale trebuie dat pentru unul sau mai multe scopuri specifice, trebuie să fie clar și neechivoc. Pentru minorii sub 16 ani (ori la o vârstă mai mică, în condițiile legii) sau persoanele lipsite de discernământ, consimțământul este încuviințat/ suplinit de către reprezentantul legal. Persoana vizată are dreptul să își retragă consimţământul în orice moment și este informată cu privire de acest lucru înainte de acordarea consimțământului. Retragerea consimțământului se face la fel de simplu ca și acordarea acestuia și produce efecte doar pentru viitor, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Lipsa/retragerea consimțământului persoanei vizate cu privire la prelucrarea datelor personale, daca nu sunt aplicabile cazurile legale de prelucrare a datelor personale, atrage imposibilitatea începerii/continuării raportului juridic cu toate consecințele legale și contractuale.

b) Excepțiile: alte cazuri legale când nu este necesar consimțământului persoanei vizate pentru prelucrarea datelor personale :

a) prelucrarea este necesară pentru executarea unui contract sau antecontract la care persoana vizată este parte ori pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract. Exemple: ofertarea, negocierea, încheierea şi executarea contractelor cu operatorul: furnizarea de servicii, asigurarea suportului, furnizarea de informații despre serviciile și produsele deținute, ș.a.

b) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale (dreptul intern/legislația UE) care îi revine operatorului. Exemple: identificarea si cunoașterea clientelei, identificarea și prevenirea faptelor sancționate de lege, ținerea arhivei și a evidențelor contabile, raportarea parametrilor activității operatorului, ș.a.

c) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice.

d) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public (a se vedea definiția dată conform Legii nr. 190/2018); în acest caz, prelucrarea se efectuează cu instituirea de către operator sau de partea terță a următoarelor garanții: punerea în aplicare a măsurilor tehnice şi organizatorice adecvate pentru respectarea principiilor prelucrării, în special a reducerii la minimum a datelor, respectiv a principiului integrităţii şi confidenţialităţii, numirea unui responsabil pentru protecţia datelor, dacă aceasta este necesară conform legii, stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.

e) prelucrarea este necesară în scopul intereselor legitime (dreptul intern/legislația UE) urmărite de operator sau de o parte terță căreia îi sunt dezvăluite datele personale, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil. Exemple: cunoașterea pieței, analiza statistică a portofoliului de clienti, analizarea unor idei de eficientizare a organizării și funcționării operatorului, dezvoltarea operatorului, îmbunătățirea produselor și serviciilor oferite, agregarea operațiunilor, crearea și menținerea unei baze de date interne, analiza solvabilității partenerului contractual, minimizarea riscurilor de piață și de fraudă la care se expune operatorul în legatură cu organizarea și furnizarea serviciilor și produselor oferite, securizarea informatică (baza de date, programe, rețea, web, ș.a.), securizarea locației (sediul, puncte de lucru);

f) prelucrarea datelor cu caracter personal în scopuri jurnalistice sau în scopul exprimării academice, artistice, literare poate fi efectuată dacă aceasta privește date personale care au fost făcute publice în mod manifest de către persoana vizată sau care sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată, conform Legi nr. 190/2018;

g) prelucrarea este făcută exclusiv în scopuri de arhivare publică, statistice, de cercetare istorică sau ştiinţifică, cu respectarea garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.).

În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimţământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară şi proporţională într-o societate democratică pentru a proteja obiectivele menţionate la articolul 23 alineatul (1) din Regulamentul European, operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate iniţial, ia în considerare, printre altele:

a)orice legătură dintre scopurile în care datele cu caracter personal au fost colectate şi scopurile prelucrării ulterioare preconizate;

b)contextul în care datele cu caracter personal au fost colectate, în special în ceea ce priveşte relaţia dintre persoanele vizate şi operator;

c)natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu articolul 9 din Regulamentul European, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale şi infracţiuni, în conformitate cu articolul 10 din Regulamentul European;

d)posibilele consecinţe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

e)existenţa unor garanţii adecvate, care pot include criptarea sau pseudonimizarea.

Art. 8 Durata prelucrării datelor personale. Încheierea operaţiunilor de prelucrare. Destinația ulterioară a datelor personale

La operațiunile de prelucrare al căror temei este **consimțământul,** datele personale sunt prelucrate pe durata raportului juridic cu operatorul și până la retragerea consimțământului persoanei vizate.

La operațiunile de prelucrare al căror temei îl formează **celelalte cazuri legale,** datele personale sunt prelucrate pe durata necesară realizării scopurilor concrete urmărite..

Indiferent de temei, la finalul prelucrării de operator, datele personale sunt triate și vor primi următoarele destinații, dacă persoana vizată nu și-a dat în mod expres și neechivoc consimţământul pentru o altă destinaţie:

a) distruse;

b) depuse spre arhivare în condițiile legii, stocate exclusiv în scopuri statistice, de cercetare istorică sau ştiinţifică, cu respectarea garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.). Durata arhivării (50 ani, 3 ani, ș.a.) este cea prevăzută de legislația specială în vigoare pentru diferitele categorii de date: Legea Arhivelor Naționale, Legea contabilității, alte legi speciale;

c) alte destinații prevăzute de lege;

Datele personale obținute în urma monitorizării prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă pot fi stocate pe o durată de maxim 30 zile cu excepția situațiilor prevăzute de lege sau a cazurilor temeinic justificate, conform Legii nr. 190/2018.

CAPITOLUL III

Reguli speciale privind prelucrarea datelor personale

Art. 9 Prelucrarea unor categorii speciale de date personale

Regula: Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice.

Excepțiile: prevederile alineatului precedent nu se aplică în următoarele cazuri:

a) persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepţia cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicţia prevăzută la alineatul precedent să nu poată fi ridicată prin consimţământul persoanei vizate

b) prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanţii adecvate pentru drepturile fundamentale şi interesele persoanei vizate;

c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) prelucrarea este efectuată în cadrul activităţii legitime şi cu garanţii adecvate de către persoana juridică cu scop nelucrativ, cu condiţia ca prelucrarea să se refere numai la membrii sau la foştii membri sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale şi ca datele cu caracter personal să nu fie comunicate terţilor fără consimţământul persoanelor vizate;

e) prelucrarea se referă la date personale care sunt făcute publice în mod manifest de către persoana vizată;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare;

g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la

protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate;

h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării condiţiilor şi garanţiilor ca datele respective să fie prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.

i) prelucrarea este necesară din motive de interes public în domeniul sănătăţii publice, cum ar fi protecţia împotriva ameninţărilor transfrontaliere grave la adresa sănătăţii sau asigurarea de standarde ridicate de calitate şi siguranţă a asistenţei medicale şi a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, în special a secretului profesional

j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, cu respectarea garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.), în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate.

Art.10 Prelucrarea datelor personale referitoare condamnări penale și infracțiuni

Prelucrarea datelor personale referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe (măsuri de siguranță sau sancțiuni administrative ori contravenționale) aplicate persoanei vizate, se efectuează numai sub controlul autorităților publice competente sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ţine numai sub controlul autorităţii de stat competente.

Operatorul poate solicita la angajare prezentarea cazierului judiciar și alte înscrisuri din care să rezulte situația juridică a persoanei care se angajează.

Art.11 Prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea

Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimţământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziţii legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate, potrivit Legii nr. 190/2018.

Prelucrarea datelor privind sănătatea realizată în scopul asigurării sănătăţii publice, astfel cum este definită în Regulamentul (CE) nr. 1.338/2008 al Parlamentului European şi al Consiliului din 16 decembrie 2008 privind statisticile comunitare referitoare la sănătatea publică, precum şi la sănătatea şi siguranţa la locul de muncă, publicat în Jurnalul Oficial al Uniunii Europene, seria L, nr. 354/70 din 31 decembrie 2008, nu se poate efectua ulterior, în alte scopuri, de către terţe entităţi.

Art.12 Prelucrarea unui număr de identificare național

Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, se poate efectua numai în temeiul consimțământului persoanei vizate (situația regulă) sau în celelalte cazuri prevăzute de lege (excepțiile legale).

Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, în scopul prevăzut la art. 6 alin. (1) lit. f) din Regulamentul European, respectiv al realizării intereselor legitime urmărite de operator sau de o parte terţă, se efectuează cu instituirea de către operator a următoarelor garanţii, potrivit Legii nr. 190/2018:

a)punerea în aplicare de măsuri tehnice şi organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum şi pentru asigurarea securităţii şi confidenţialităţii prelucrărilor de date cu caracter personal, conform dispoziţiilor art. 32 din Regulamentul European;

b)numirea unui responsabil pentru protecţia datelor în condițiile legii;

c)stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii;

d)instruirea periodică cu privire la obligaţiile ce le revin a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

Art.13 Prelucrarea care nu necesită identificare

În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica persoana vizată în scopul unic al respectării Regulamentului European.

Dacă, în cazurile menţionate la alineatul precedent, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, prevederile referitoare la dreptul de acces, la rectificare, ștergere, restricționarea prelucrării, la portalbilitate și obligația de notificare, nu se aplică, cu excepţia cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informaţii suplimentare care permit identificarea sa.

CAPITOLUL IV

Persoana vizată.

Drepturile sale în contextul prelucrării datelor personale

Art.14 Reguli generale de procedură

Operatorul aduce la cunoștința publică regulile de prelucrare a datelor personale, scopurile prelucrării, drepturile persoanelor vizate și alte informații generale despre prelucrarea datelor personale. Persoana vizată poate să se informeze despre aceste informații actualizate de pe site-ul web al operatorului.

Persoana vizată poate să formuleze cereri privind prelucrarea datelor personale. Prin cerere poate solicita ca răspunsul să fie furnizat la o altă adresă de corespondență, prin e-mail sau livrată personal, prin curier.

Cererile se soluționează gratuit, iar în cazul celor vădit nefondate sau excesive, operatorul poate să perceapă o taxă pntru costurile administrative de furnizare a informațiilor, comunicare sau pentru luarea măsurilor solicitate, ori poate să refuze soluționarea cererii.

Operatorul poate să solicite informații suplimentare privind identitatea persoanei vizate care a formulat cererea, sau alte informații necesare soluționării, de la persoana vizată sau de la instituțiile statului care le dețin.

Operatorul va soluționa cererea în termen de cel mult 1 lună de la primirea cererii (sau 15 zile în cazul exercitării dreptului de acces la date personale sau de opoziție), termen care poate fi prelungit cu două luni, în funcție de necesitate și de numărul cererilor. Soluția negativă va fi motivată și se va menționa

calea de atac (plângerea la autoritatea de supraveghere și acțiunea în instanță). Soluția poate fi refuzată dacă operatorul nu este în măsură să identifice persoana vizată.

În comunicări se poate folosi formatul scriptic, verbal, telefonic, electronic (mail, online, sau alt mijloc de comunicare). Pentru probațiune se folosește formatul scriptic sau electronic, iar operatorul poate să impună respectarea unor formalități în cazul în care are suspiciuni privind identitatea sau calitatea persoanei care formulează cererea: forma scrisă, împuternicire autentică, ș.a.. În comunicări se utilizează o formă concisă, transparentă, inteligibilă, ușor accesibilă, clară, simplă.

Art.15 Informarea persoanei vizate

În cazul în care **datele personale referitoare la o persoană vizată sunt colectate de la aceasta,** operatorul, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate toate informaţiile următoare, dacă și în măsura în care persoana vizată nu deține deja informațiile respective:

a) identitatea și datele de contact ale operatorului şi, după caz ale reprezentantului acestuia,

b) datele de contact ale responsabilului cu protecția datelor personale, după caz caz;

c) scopurile în care sunt prelucrate datele personale, precum și temeiul juridic al prelucrării;

d) interesele legitime urmărite de operator sau de o parte terță, în situația în care prelucrarea se face în temeiul unui interes legitim;

e) destinatarii sau categoriile de destinatari ai datelor personale;

f) dacă este cazul, intenția operatorului de a transfera date personale către o țară terță sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei Europene privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf din Regulamentul European, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie;

g) perioada pentru care vor fi stocate datele personale sau, dacă acest lucru nu este posibil, criterile utilizate pentru a stabili această perioadă;

h) existenţa drepturilor de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor

i) existența dreptului de a depune o plângere în faţa autorităţii de supraveghere

j) dacă prelucrarea se bazează pe consimțământ: existența dreptului de a retrage consimțământul, în orice moment, cu efecte pentru viitor, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;

k) dacă furnizarea de date personale reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii (în speță: imposibilitatea încheierii/continuării raportului juridic);

l) existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată;

În cazul în care **datele personale nu au fost obţinute direct de la persoana vizată,** operatorul va furniza persoanei vizate informațiile indicate supra, precum și următoarele informații: categoriile de date personale vizate, sursa din care provin sau dacă provin din surse disponibile public. Furnizarea informațiilor se face la următoarele termene:

a) într-un termen rezonabil, dar nu mai mare de o lună, ţinându-se seama de circumstanţele specifice în care sunt prelucrate datele cu caracter personal;

b) cel târziu la prima comunicare cu persoana vizată (dacă datele urmează să fie utilizate pentru comunicarea cu persoana vizată);

c) cel târziu la data la care datele sunt divulgate pentru prima oară (dacă se intenționează divulgarea datelor către alt destinatar).

În toate situațiile, în cazul în care operatorul intenţionează să prelucreze ulterior datele personale într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante.

Prevederile alineatelor precedente nu se aplică dacă și în măsura în care:

-persoana vizată deține deja informațiile;

-furnizarea acestor informaţii se dovedeşte a fi imposibilă sau ar implica eforturi disproporţionate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, sub rezerva respectării garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.), sau în măsura în care obligaţia de informare din prezentul articol este susceptibilă să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. In astfel de cazuri,

operatorul ia măsuri adecvate pentru a proteja drepturile, libertăţile şi interesele legitime ale persoanei vizate, inclusiv punerea informaţiilor la dispoziţia publicului;

-obţinerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern sub incidenţa căruia intră operatorul şi care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate;

-în cazul în care datele cu caracter personal trebuie să rămână confidenţiale în temeiul unei obligaţii statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligaţii legale de a păstra secretul.

Persoana vizată poate verifica online, la sediul social, sau la punctele de lucru, regulamentul de protecție a datelor personale și celelalte documente și poate solicita în scris de la operator informatii privind prelucrarea datelor personale, cum ar fi: identitatea operatorului, scopul în care se face prelucrarea, destinatarii datelor personale, drepturile persoanei vizate, ș.a.

Persoana vizată are nu numai dreptul, ci și obligația să se informeze de noutățile și modificările legislative apărute în această materie.

Art.16 Dreptul de acces la datele personale

Persoana vizată are dreptul de a obţine din partea operatorului:

-o confirmare că se prelucrează sau nu date personale care o privesc;

-acces la datele respective;

-informațiile care sunt furnizate în temeiul dreptului privind informarea persoanei vizate: scopurile prelucrării, destinatarii, ș.a.;

-o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. Dreptul de a obţine o copie nu aduce atingere drepturilor şi libertăţilor altora.

Conform Legii nr. 190/2018, dreptul de acces nu se aplică în cazurile de prelucrare în scopuri statistice și de cercetare științifică sau istorică și în cazurile de prelucrare în scopuri de arhivare publică, în măsura în care dreptul este de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogarea este necesară pentru îndeplinirea acestor scopuri.

Art.17 Dreptul la rectificare

Persoana vizată are dreptul de a obţine de la operator, fără întârzieri nejustificate:

-rectificarea datelor cu caracter personal inexacte care o privesc;

-completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaraţii suplimentare;

Conform Legii nr. 190/2018, dreptul la rectificare nu se aplică în cazurile de prelucrare în scopuri statistice și de cercetare științifică sau istorică și în cazurile de prelucrare în scopuri de arhivare publică, în măsura în care dreptul este de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogarea este necesară pentru îndeplinirea acestor scopuri.

Art. 18 Dreptul la ștergerea datelor („dreptul de a fi uitat”)

Persoana vizată are dreptul de a obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

a)datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

b)persoana vizată îşi retrage consimţământul pe baza căruia are loc prelucrarea şi nu există niciun alt temei juridic pentru prelucrarea;

c)persoana vizată se opune prelucrării în temeiul dreptului la opoziţie şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării în scop de marketing direct;

d)datele cu caracter personal au fost prelucrate ilegal;

e)datele cu caracter personal trebuie şterse pentru respectarea unei obligaţii legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidenţa căruia se află operatorul;

f)datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societăţii informaţionale unui copil, conform Regulamentului European.

În cazul în care operatorul a făcut publice datele cu caracter personal şi este obligat să le şteargă, operatorul, ţinând seama de tehnologia disponibilă şi de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ştergerea de către aceşti operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

Dreptul la ștergere nu se aplică în măsura în care prelucrarea este necesară:

a)pentru exercitarea dreptului la liberă exprimare şi la informare;

b)pentru respectarea unei obligaţii legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este învestit operatorul;

c)din motive de interes public în domeniul sănătăţii publice, în conformitate cu articolul 9 alineatul (2) literele (h) şi (i) şi cu articolul 9 alineatul (3) din Regulamentul European;

d)în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, cu respectarea garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.), în măsura în care dreptul de ștergere este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;

e)pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

Art. 19 Dreptul la restricționarea prelucrării

Persoana vizată are dreptul de a obţine din partea operatorului restricţionarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

a)persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;

b)prelucrarea este ilegală, iar persoana vizată se opune ştergerii datelor cu caracter personal, solicitând în schimb restricţionarea utilizării lor;

c)operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanţă;

d)persoana vizată și-a exercitat dreptul de opoziție, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

În cazul în care prelucrarea a fost restricţionată, astfel de date cu caracter personal pot, cu excepţia stocării, să fie prelucrate numai în următoarele cazuri:

-cu consimţământul persoanei vizate:

-pentru constatarea, exercitarea sau apărarea unui drept în instanţă;

-pentru protecţia drepturilor unei alte persoane fizice sau juridice;

-din motive de interes public important al Uniunii sau al unui stat membru.

O persoană vizată care a obţinut restricţionarea prelucrării este informată de către operator înainte de ridicarea restricţiei de prelucrare.

Conform Legii nr. 190/2018, dreptul la restricționarea prelucrării nu se aplică în cazurile de prelucrare în scopuri statistice și de cercetare științifică sau istorică și în cazurile de prelucrare în scopuri de arhivare publică, în măsura în care dreptul este de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogarea este necesară pentru îndeplinirea acestor scopuri.

Art. 20 Obligația de notificare privind rectificarea sau ştergerea datelor cu caracter personal sau restricţionarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ştergere a datelor cu caracter personal sau restricţionare a prelucrării efectuate în conformitate cu legea, cu excepţia cazului în care acest lucru se dovedeşte imposibil sau presupune eforturi disproporţionate.

Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

Conform Legii nr. 190/2018, obligația de notificare nu se aplică în cazurile de prelucrare în scopuri de arhivare publică, în măsura în care obligația este de natură să facă imposibilă sau să afecteze în mod grav realizarea scopului specific, iar derogarea este necesară pentru îndeplinirea acestui scop.

Art.21 Dreptul la portabilitatea datelor personale

Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

a)prelucrarea se bazează pe consimţământ sau prelucrarea se întemeiează pe un contract sau antecontract;

b)prelucrarea este efectuată prin mijloace automate.

În exercitarea dreptului său la portabilitatea datelor, persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

Exercitarea dreptului la portabilitate nu aduce atingere dreptului la ștergere. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este învestit operatorul.

Dreptul la portabilitate nu aduce atingere drepturilor şi libertăţilor altora.

Conform Legii nr. 190/2018, dreptul la portabilitate nu se aplică în cazurile de prelucrare în scopuri statistice și de cercetare științifică sau istorică și în cazurile de prelucrare în scopuri de arhivare publică, în măsura în care dreptul este de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogarea este necesară pentru îndeplinirea acestor scopuri.

Art.22 Dreptul de opoziţie

În orice moment, persoana vizată are dreptul să se opună, din motive legate de situaţia particulară în care se află, prelucrării în temeiul articolului 6 alineatul (1) litera (e) sau (f) din Regulamentul European (îndeplinirea unei sarcini care serveşte unui interes public şi realizarea intereselor legitime urmărite de operator), a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziţii. Operatorul nu mai prelucrează datele cu caracter personal, cu excepţia cazului în care operatorul demonstrează că are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra intereselor, drepturilor şi libertăţilor persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţă.

Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv. În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

Cel târziu în momentul primei comunicări cu persoana vizată, dreptul la opoziție este adus în mod explicit în atenţia persoanei vizate şi este prezentat în mod clar şi separat de orice alte informaţii.

În contextual utilizării serviciilor societăţii informaţionale şi în pofida Directivei 2002/58/CE, persoana vizată îşi poate exercita dreptul de a se opune prin mijloace automate care utilizează specificaţii tehnice.

Conform Regulamentului European, în cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice cu respectarea garanțiilor legislației de protecție a datelor personale prevăzute de art. 89 din Regulamentul European (reducerea la minim a datelor, măsurile de securitate, ș.a.), persoana vizată, din motive legate de situaţia sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepţia cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Conform Legii nr. 190/2018, dreptul la opoziție nu se aplică în cazurile de prelucrare în scopuri statistice și de cercetare științifică sau istorică și în cazurile de prelucrare în scopuri de arhivare publică, în măsura în care dreptul este de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogarea este necesară pentru îndeplinirea acestor scopuri.

Art.23 Procesul decizional individual automatizat. Crearea de profiluri

A. Descriere

Pentru a îmbunătăți calitatea serviciilor și produselor oferite și relația contractuală, pentru a respecta cerințele legale, operatorul se aliniază tendințelor de piață și poate folosi procese decizionale individuale automatizate. În acest scop, pot fi implementate procese automatizate, pe baza cărora se pot lua decizii cu privire la client (date de ieșire) fără intervenție umană, pe baza unor împrejurări stabilite (date de intrare). Ele se aplică în măsura și în condițiile în care sunt permise de lege.

Exemple de cazuri în care se pot lua decizii automate:

-la accesarea contului de utilizator pe site-ul operatorului se poate verifica locația și ora accesării. Pe baza unui motor de risc se poate constata că se accesează la un interval scurt același cont din altă locație în care nu este posibilă deplasarea fizică a utilizatorului. În acest caz se poate lua decizia automată a interzicerii accesului la cont, până la eventuale lămuriri. Prin acest proces se încearcă protejarea clientului de o eventuală accesare frauduloasă, fiind imposibil ca un aceasta să fie prezentă fizic în două locuri în același timp.

-cu ocazia ofertării, negocierii contractului, organizării de activități sau participării la acestea, operatorul poate transmite automat informări despre produsele și serviciile oferite pe baza caracteristicilor persoanei vizate furnizate de aceasta, de client sau obținute în mod legal. Prin acest proces se încearcă identificarea clientelei țintă, a angajaților sau voluntarilor care pot beneficia de produsele și serviciile operatorului și personalizării ofertei și informațiilor destinate acestora. Se evită astfel trimiterea de oferte la persoane care nu au nimic de-a face cu produsele și serviciile operatorului și care pot fi calificate drept „spam”.

-cu ocazia executării sau încetării contractului, operatorul poate folosi procese automatizate, suspendând automat contul, temporar sau definitiv, în funcție de anumite condiți (îndeplinirea unor obligații, pontaj, plăți, ajungerea la termenul contractual stabilit de părți, sau îndeplinirea unei condiții agreate de părți sau impuse de lege). Prin acest proces se încearcă un management mai bun al relației contractuale.

-cu ocazia executării contractului, operatorul poate folosi procese automatizate, notificând clientul despre anumite evenimente care se produc în bazele de date monitorizate și solicitate de client, diverse evenimente de interes. Aceste notificări se trimit în forma agreată de părți. Prin acest proces se încearcă alertarea clientului despre evenimentele monitorizate.

Toate aceste procese automatizate conțin algoritmi (prelucrarea automată) care se execută în cazul îndeplinirii condiției stabilite (date de intrare) și returnează un anumit răspuns (date de ieșire): suspendarea temporară a contului în caz de acces neautorizat, informarea, alertarea clientului, ș.a. Acești algoritmi se execută fără intervenție umană, astfel că fidelitatea procesului este maximă și înlătură orice eroare umană care poate interveni în prelucrarea datelor personale. Implementarea lor are ca finalitate satisfacția clientului, oferirea de produse și servicii personalizate cât mai apropiate de interesele lui.

Pentru furnizarea de servicii și produse și pentru un management mai bun al relației contractuale, operatorul poate crea profiluri care permit identificarea preferințelor și comportamentului persoanei vizate. Astfel, se poate verifica persoana vizată în bazele de date publice, în actele furnizate de acesta, la persoanele indicate de acesta, în istoricul contractual, iar pe baza informațiilor obținute pot fi efectuate profiluri. Crearea profilurilor nu este urmată întotdeauna de luarea unei decizii automatizate, ci pot fi luate și decizii umane. Interesul în crearea profilurilor este și al operatorului, întrucât, în situația în care sunt identificate riscuri de insolvabilitate, fraudă, condamnări sau alte riscuri, operatorul poate refuza furnizarea produselor și serviciilor.

B. Regim juridic

Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care o privesc sau o afectează în mod similar într-o măsură semnificativă.

Excepții: acest drept nu se aplică în cazul în care decizia automată:

a)este necesară pentru încheierea sau executarea unui contract între persoana vizată şi operator

b)este autorizată prin dreptul Uniunii sau dreptul intern, care prevede măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate;

c)are la bază consimţământul explicit al persoanei vizate.

În cazul excepțiilor menţionate la literele (a) şi (c), operatorul pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate:

-dreptul acesteia de a obţine intervenţie umană din partea operatorului;

-dreptul de a-şi exprima punctul de vedere;

-dreptul de a contesta decizia;

-retragerea, reevaluarea sau anularea oricărei decizii automate care produce efecte juridice în privinţa persoanei vizate, adoptată exclusiv pe baza unei prelucrări de date personale, efectuată prin mijloace automate

-dacă aceste măsuri nu pot fi aplicate, sau provoacă costuri suplimentare, operatorul poate decide neînceperea sau încetarea relației contractuale.

Excepțiile menţionate nu au la bază categoriile speciale de date personale prevăzute de art. 9 alin. (1) din Regulamentul European (originea rasială, etnică, opinii politice, confesiunea religioasă, convingeri filosofice, apartenența la sindicate, date genetice, biometrice, date privind sănătatea, viața sexuală), cu excepţia cazului în care se aplică art. 9 alin. (2) lit. a) sau g) (persoana vizată și-a dat consimțământul sau prelucrarea este necesară din motive de interes public) şi în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

Art.24 Dreptul de a depune plângere

Persoanele lezate pot depune plângere la autoritatea de supraveghere și se pot adresa justiției, în condițiile legii pentru apărarea oricăror drepturi garantate de lege care le-au fost incalcate și pentru repararea prejudiciilor suferite.

Plângerile și acțiunile în instanță vor fi introduse și soluționate conform legii specifice.

CAPITOLUL V

Operatorul.

Secțiunea I. Măsuri luate de operator

Art.25 Măsuri luate de operator

Operatorul pune în aplicare măsuri organizatorice și funcționale adecvate ținând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, pentru:

-*legalitate:* a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu legea;

-*temeinicie:* a pune în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor (sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării), a integra garanţiile necesare în cadrul prelucrării, a proteja drepturile persoanelor vizate.

Operatorul poate revizui respectivele măsuri şi le poate actualiza dacă este necesar. Aderarea la coduri de conduită aprobate sau la un mecanism de certificare aprobat, poate fi utilizată ca element care să demonstreze respectarea obligaţiilor privind protecția datelor.

Măsurile organizatorice constau în:

-stabilirea modalităților de prelucrare a datelor personale. Operatorul poate prelucra datele în oricare din modalitățile prevăzute de lege, încheind în acest sens actele și acordurile necesare, conform dispozițiilor respective din prezentul regulament:

-prelucrarea de operator, fără a apela la alte persoane;

-prelucrarea în raporturi juridice cu poziție de subordonare, respectiv prin persoane împuternicite (angajați, voluntari, colaboratori subordonați) – art. 28 din Regulamentul European;

-prelucrarea în raporturi juridice cu poziție de egalitate, respectiv în asociere (colaboratori independenți, operatori asociați, ș.a.) - art. 26 din Regulamentul European;

-prelucrarea prin reprezentanți din afara Uniunii, conform legii, dacă activitatea operatorului impune acest lucru – art. 27 din Regulamentul European.

-stabilirea responsabilității privind sistemul de protecție a datelor. În oricare din modalitățile de prelucrare, responsabilitatea proiectării, executării și corectării sistemului de protecție a datelor la nivelul operatorului aparține, conform dispozițiilor respective din prezentul regulament:

-conducerii executive;

-responsabilului cu protecția datelor.

Măsurile funcționale constau în:

-măsuri de informare;

-adaptarea actelor normative interne;

-evidențe ale activităților de prelucrare;

-măsuri de securitate a datelor cu caracter personal;

-măsuri în caz de încălcare a securității datelor cu caracter personal;

-evaluarea de impact;

-raporturile cu autoritatea de supraveghere;

-coduri de conduită și certificare

Secțiunea a II-a. Măsuri organizatorice

Art. 26 Prelucrarea prin operatori asociați

Operatorul se poate asocia cu alt operator în vederea prelucrării datelor personale ale persoanelor vizate, stabilind în comun scopurile și mijloacele de prelucrare.

Printr-un acord, operatorii stabilesc într-un mod transparent responsabilităţile fiecăruia în ceea ce priveşte îndeplinirea obligaţiilor care le revin în temeiul legislației de protecție a datelor, în special în ceea ce priveşte exercitarea drepturilor persoanelor vizate şi îndatoririle fiecăruia de furnizare a informaţiilor care trebuie furnizate în temeiul dreptului la informare, cu excepţia cazului şi în măsura în care responsabilităţile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

Acordul reflectă în mod adecvat rolurile şi raporturile respective ale operatorilor asociaţi faţă de persoanele vizate. Esenţa acestui acord este făcută cunoscută persoanei vizate.

Indiferent de clauzele acordului, persoana vizată îşi poate exercita drepturile în temeiul prezentului regulament cu privire la şi în raport cu fiecare dintre operatori.

Art. 27 Prelucrarea prin persoane împuternicite de operator

Operatorul poate desemna persoane împuternicite ca să efectueze prelucrarea în numele său, care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în prezentul regulament şi să asigure protecţia drepturilor persoanei vizate.

Mandatul primit este *intuitu personae* și nu poate fi transmis sau împărțit cu altcineva. Altă persoană poate fi desemnată drept persoană împuternicită doar cu acordul scris, specific sau general al operatorului. Persoana împuternicită informează operatorul cu privire la orice adăugare sau înlocuire a altor persoane împuternicite, iar operatorul se poate opune. Persoana recrutată are aceleaşi obligaţii privind protecţia datelor prevăzute în contractul sau în alt act juridic încheiat între operator şi persoana împuternicită, prin intermediul unui contract sau al unui alt act juridic, în special furnizarea de garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerinţele prezentului regulament. În cazul în care această a doua persoană împuternicită nu îşi respectă obligaţiile privind protecţia datelor, persoana împuternicită iniţială rămâne pe deplin răspunzătoare faţă de operator în ceea ce priveşte îndeplinirea obligaţiilor acestei a doua persoane împuternicite.

Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:

a)prelucrează (copiază, divulgă, transmite, șterge, ș.a.) datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică (obligația de confidențialitate); în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

b)se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;

c)adoptă toate măsurile de securitate necesare;

d)respectă condiţiile privind recrutarea unei alte persoane împuternicite;

e)ţinând seama de natura prelucrării, oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor pe care le are cu privire la prelucrarea datelor personale;

f)ajută operatorul să asigure respectarea obligaţiilor prevăzute la articolele 32-36 din Regulamentul European (securitatea prelucrării, încălcarea securității, evaluarea impactului, consultarea prealabilă), ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;

g)la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

h)pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

i) informează imediat operatorul în cazul în care, în opinia sa, o instrucţiune încalcă prezentul regulament sau alte dispoziţii din dreptul intern sau din dreptul Uniunii referitoare la protecţia datelor.

Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, sau la un mecanism de certificare aprobat, poate fi utilizată ca element prin care să se demonstreze existenţa garanţiilor suficiente menţionate în prezentul articol.

În cazul în care o persoană împuternicită de operator încălcă prezentul regulament, prin stabilirea scopurilor şi mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce priveşte prelucrarea respectivă și poate fi sancționată conform legii.

Indiferent de existența sau nu a unui contract încheiat cu operatorul, conform art. 29 din Regulamentul European, persoana împuternicită de operator şi orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează (copiază, divulgă, transmite, șterge, ș.a.) decât la cererea operatorului, cu excepţia cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru (obligația de confidențialitate).

Art. 28 Prelucrarea prin reprezentanţi din afara Uniunii

Subscrisa, persoană juridică poate fi reprezentant al unui operator sau persoană împuternicită care nu își are sediul în Uniune și poate desemna reprezentanți care nu își au sediul în Uniune, cu respectarea legii și a prevederilor privind transferurile de date.

Reprezentantul primește din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autorităţile de supraveghere şi persoanele vizate, în special, se pot adresa reprezentantului, în plus faţă de operator sau persoana împuternicită de operator sau în locul acestora, cu privire la toate chestiunile legate de prelucrarea, în scopul asigurării respectării prezentului regulament.

Desemnarea operatorului ca reprezentant de către alt operator sau persoana împuternicită de operator cu sediul în afara Uniunii nu aduce atingere acţiunilor în justiţie care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator din afara Uniunii, înseşi.

Art. 29 Responsabilul cu protecția datelor

Conducerea executivă a operatorului reprezintă operatorul și are toate atribuțiile operatorului în domeniul protecției datelor personale. Aceasta răspunde direct în fața celui mai înalt nivel al conducerii operatorului. Ea este numită, evaluată, sancționată și demisă de acest organ și are acces la

toate datele, la toate operațiunile de prelucrare și la toate resursele operatorului, pentru îndeplinirea tuturor competențelor.

Conducerea executivă desemnează unul sau mai mulți responsabili cu protecția datelor din rândul angajaților, voluntarilor sau colaboratorilor externi, care oferă garanții suficiente pentru luarea, aplicarea și corectarea măsurilor tehnice și organizatorice adecvate, pe baza calităților profesionale, cunoștințelor de specialitate în materia protecției datelor și capacității de a îndeplini sarcinile specifice.

Responsabilul cu protecția datelor răspunde în fața conducerii executive. El este numit, evaluat, sancționat și demis de conducerea executivă și are acces la datele, la operațiunile de prelucrare și la resursele, care sunt comunicate în vederea îndeplinirii competențelor acordate. Mandatul primit este *intuitu personae* și nu poate fi transmis sau împărțit cu altcineva. Altă persoană poate fi recrutată pe această funcție doar cu acordul conducerii executive și stabilind în mod clar cu modul de distribuire a responsabilităților. Poate fi numit un responsabil cu protecția datelor comun, cu alt operator, conform legii.

Competențele, care se transmit către responsabilul cu protecția datelor (în decizia de desemnare sau de modificare a competențelor, fișa postului sau contractul încheiat), în ipoteza în care a fost desemnat un responsabil, sunt:

-informează şi consiliază operatorul, precum şi angajaţii, colaboratorii și voluntarii care se ocupă de prelucrare, cu privire la obligaţiile care le revin în temeiul legii referitoare la protecţia datelor personale;

-monitorizează respectarea legii şi a măsurilor operatorului în ceea ce priveşte protecţia datelor personale, inclusiv alocarea responsabilităţilor şi acţiunile de sensibilizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente și raportează operatorului orice încălcare;

-consiliază, realizează și monitorizează evaluarea de impact în cazul în care aceasta este necesară și efectuează consultarea prealabilă a autorității de supraveghere în cazurile prevăzute de lege;

-cooperează cu autoritatea de supraveghere, parcurge procedura de înregistrare în cazul în care este necesar și își asumă rolul de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă și consultarea cu privire la orice altă chestiune;

-monitorizează legislația, actualizează regulamentul intern de protecție a datelor, redactează actele adiționale la contractele existente care conțin clauze privind prelucrarea datelor personale sau apelează ori propune apelarea la servicii externalizate, ține evidențele activității de prelucrare, monitorizează piața sistemelor de securitate IT și propune îmbunătățiri, ține

evidențele încălcărilor securității datelor și este reprezentantul operatorului în relațiile cu persoanele care formulează cereri în materie de protecție de date personale.

-are și alte sarcini și atribuții stabilite de operator, cu condiția să nu se genereze conflict de interese (ex: evaluarea propriei activități);

În cazul în care prelucrează date personale în calitate de persoană împuternicită, are și obligațiile corespunzătoare, prevăzute la acel articol.

Persoanele vizate pot contacta conducerea executivă sau responsabilul cu protecția datelor în privința tuturor chestiunilor legate de prelucrarea datelor lor şi de exercitarea drepturilor lor în temeiul legii adresându-se cu cerere la sediul social sau la adresa de e-mail ale operatorului.

În deciziile luate, conducerea executivă și responsabilul cu protecția datelor ţin seama în mod corespunzător de riscul asociat operaţiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul şi scopurile prelucrării.

Secțiunea a III-a. Măsuri funcționale

Art.30 Măsuri de informare

Se vor informa persoanele care se află în raporturi juridice cu operatorul, sau care urmează să intre în astfel de raporturi juridice și se emit acte juridice, după cum urmează:

-persoanele vizate (ale căror date sunt prelucrate de operator, indiferent de calitatea lor: clienți-beneficiari, angajați, voluntari, responsabilul cu protecţia datelor):

●notificarea de informare, act juridic care sintetizează noțiunile generale despre protecția datelor personale în cadrul operatorului și care conține elementele prevăzute la articolul referitor la dreptul la informare. Aceasta se pune la dispoziția persoanelor vizate, inclusiv pe site-ul operatorului;

●formularul de consimțământ, act juridic care atestă atestă luarea la cunostinta notei de informare, și a regimului de prelucrare la nivelul operatorului cuprins în regulament și prin care persoanele vizate se declară de acord cu prelucrarea datelor lor personale. Se poate folosi un format standard pentru contractele în vigoare și pentru cele noi, sau se poate folosi un act adițional pentru contractele în vigoare, sau s epot introduce clauze în contractele noi;

-persoanele împuternicite (care prelucrează date de la operator, sub autoritatea lui: angajați, voluntari, responsabilul cu protecţia datelor)

●actul adițional care cuprinde clauzele prevăzute de articolul referitor la persoanele împuternicite (clauzele nou introduse în actul adițional vor fi și clauze pentru contractul standard pentru acest post)

●procesul verbal de instruire, împreună cu tabelul nominal;

-colaboratorii – operatori asociați (care prelucrează date personale alături de operator, pe poziție de egalitate):

●acord asociere care cuprinde clauzele prevăzute de articolul referitor la operatori asociați

-destinatarii (asupra cărora operatorul nu are drept de control intern și cărora le-au fost divulgate date cu caracter personal, fără a avea dreptul de a le prelucra):

●notificarea, care cuprinde următoarele obligații în privința datelor personale provenite de la operator: să nu le prelucreze (copiază, divulgă, transmite, șterge, ș.a.) decât la cererea operatorului, cu excepția cazului în care acționează în baza legii (desfășurarea activității de prelucrare sub autoritatea operatorului, obligația de confidențialitate) și să aplice măsurile de securitate prevăzute la articolul respectiv

-reprezentați stat terț (care reprezintă operatorul în stat terț):

●mandat care cuprinde clauzele prevăzute de articolul referitor la reprezentanți stat terț;

Se efectuează informarea generală, publicându-se pe site-ul operatorului: regulamentul, notificarea de informare, formularul de consimțământ, celelalte informații și documente de interes. Aceste informații sunt publice, iar orice persoană care intră în raporturi juridice de prelucrare a datelor personale cu operatorul are posibilitatea de a se informa din această sursă și nu poate invoca necunoașterea informațiilor publicate acolo. De asemenea, nu se poate invoca necunoașterea informațiilor cuprinse în legislație (nimeni nu poate invoca necunoașterea legii).

Art.31 Actele normative interne

Operatorul emite prezentul regulament intern privind prelucrarea datelor personale.

Operatorul aliniază actele normative interne la acest regulament, inserând norme de trimitere.

Art.32 Evidențele activitaților de prelucrare.

La nivelul operatorului se păstrează o evidență în scris, inclusiv în format electronic (foaie de calcul / bază de date) a activităților de prelucrare, care cuprinde următoarele informații:

-informații generale:

-numele şi datele de contact ale operatorului;

-scopurile prelucrării;

-o descriere a categoriilor de persoane vizate şi a categoriilor de date personale;

-categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele personale, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;

-acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date personale;

-acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate;

-dinamic: registrul de evidență a activităților de prelucrare, în care se menționează inclusiv, dacă este cazul, transferurile de date personale către o ţară terţă sau o organizaţie internaţională cu identificarea ţării terţe sau a organizaţiei internaţionale respective; de asemenea, se păstrează o evidență a tuturor categoriilor de activități de prelucrare prin menționarea filtrelor corespunzătoare în formatul electronic utilizat. Totodată, se păstrează și evidența încălcărilor securităţii datelor personale (cel puțin: descriere a situaţiei de fapt, a efectelor acesteia, a măsurilor de remediere întreprinse).

-static: tabel cu persoane vizate, cu indicarea situatiei actuale, a statusului voinței lor in dreptul fiecareia;

O asemenea evidență trebuie ținută și de persoanele împuternicite de operator.

Art.33 Securitatea prelucrării, măsuri tehnice

Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice (distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat), operatorul implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

a)pseudonimizarea şi criptarea datelor personale;

b)capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare:

-arhiva electronică: se limitează accesul la datele personale și se protejează cu parole (se alocă parolele către angajații, colaboratorii și voluntarii care prelucrează datele personale), se instalează sisteme antivirus, se actualizează periodic, ș.a. Se securizează și monitorizează atât sistemele locale, aflate în controlul direct (HD/server/calculator local, în firmă) cât și cele din afara controlului direct (servere externe/cloud).

-arhiva fizică: se asigură locația cu încuietori, eventual și sisteme de monitorizare video, alarme, ș.a. iar în cazuri excepționale se asigură paza.

c)capacitatea de a restabili disponibilitatea datelor personale şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică: se asigură back-up periodic, se verifică sincronizarea sistem local – server extern, ș.a.

d)un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării. La evaluarea nivelului adecvat de securitate, se ţine seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele personale transmise, stocate sau prelucrate într-un alt mod. În acest sens se monitorizează piața sistemelor IT și, în funcție de costuri, se implementează la nivelul operatorului și se verifică periodic măsurile luate.

Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerinţelor prevăzute mai sus.

Art.34 Măsuri în caz de încălcare a securității datelor personale

În cazul încălcării securității datelor personale, persoana împuternicită, operatorul asociat, reprezentantul, responsabilul cu protecția datelor, orice altă persoană care ia cunoștință de încălcare, înștiințează operatorul de îndată ce ia cunoștință de încălcare.

Operatorul notifică acest lucru autorității de supraveghere competente în termen de cel mult 72 ore (dacă se depășește termenul se vor da explicații motivate pentru întârziere) de la data la care a luat cunoștință de încălcare, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. În notificare se menționează cel puțin:

a) caracterul încălcării securităţii datelor personale, inclusiv, acolo unde este posibil, categoriile şi numărul aproximativ al persoanelor vizate în cauză, precum şi categoriile şi numărul aproximativ al înregistrărilor de date personale în cauză;

b) numele şi datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obţine mai multe informaţii;

c) consecinţele probabile ale încălcării securităţii datelor personale;

d) măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securităţii datelor personale, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Atunci când şi în măsura în care nu este posibil să se furnizeze informaţiile în acelaşi timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

Operatorul informează cu privire la această încălcare și persoana vizată, de îndată, în cazul în care încălcarea securităţii datelor personale este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, sau în situația în care autoritatea de supraveghere a decis astfel. În informarea transmisă persoanei vizate se include o descriere într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor personale, precum şi cel puţin informaţiile şi măsurile menţionate la literele (b), (c) şi (d).

Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiţii este îndeplinită:

a)operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor personale afectate de încălcarea securităţii datelor personale, în special măsuri prin care se asigură că datele personale devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

b)operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor vizate menţionat nu mai este susceptibil să se materializeze;

c)ar necesita un efort disproporţionat. În această situaţie, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

Operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor personale, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor personale, a efectelor acesteia şi a măsurilor de remediere întreprinse. Această documentaţie permite autorității de supraveghere și persoanei vizate să verifice conformitatea cu legea.

Art.35 Evaluarea de impact

Operatorul nu desfășoară activități de prelucrare de natura celor pentru care legea impune evaluarea de impact.

În consecință, aceasta va fi realizată numai la solicitarea autorității de supraveghere, conform legii.

Art.36 Raporturile cu autoritatea de supraveghere (înregistrare, consultare, cooperare)

Operatorul va urma procedura de înregistrare la autoritatea de supraveghere în situația în care se află în cazurile prevăzute de lege pentru care înregistrarea este obligatorie.

Operatorul şi persoana împuternicită de operator şi, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor acesteia

Operatorul consultă autoritatea de supraveghere înainte de prelucrare atunci când:

-evaluarea impactului asupra protecţiei datelor personale prevăzută anterior indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului;

-legea prevede în mod expres această obligație

Atunci când se consultă autoritatea de supraveghere, se furnizează acesteia:

a)dacă este cazul, responsabilităţile respective ale operatorului, ale operatorilor asociaţi şi ale persoanei împuternicite, implicați în activităţile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

b)scopurile şi mijloacele prelucrării preconizate;

c)măsurile şi garanţiile prevăzute pentru protecţia drepturilor şi libertăţilor persoanelor vizate, în conformitate cu prezentul regulament;

d)dacă este cazul, datele de contact ale responsabilului cu protecția datelor;

e)evaluarea impactului asupra protecţiei datelor personale, după caz; şi

f)orice alte informaţii solicitate de autoritatea de supraveghere.

Art.37 Coduri de conduită, certificare

Operatorul poate adera la codurile de conduită aprobate în materie în scopul de a oferi garanții adecvate în cadrul eventualelor transferuri de date personale către state terțe, precum și în cazurile când sunt obligatorii aceste garanții.

Operatorul poate să obțină certificarea de la instituții abilitate în scopul de a demonstra existenţa unor garanţii adecvate și faptul că operaţiunile de prelucrare efectuate respectă prezentul regulament, mai ales în cadrul transferurilor de date personale către ţări terţe .

Aderarea la coduri de conduită și certificarea se face în funcție de context și de resursele operatorului și nu înlătură obligația operatorului de a respecte prevederile legii în materie.

Capitolul VI

Transferul în străinătate al datelor personale

Art. 38 Condițiile transferului în străinătate al datelor personale

Operatorul desfășoară activitatea în România și de principiu nu transferă date personale către țări terțe. O situație de trasnfer poate fi, în cazul datelor electronice, stocarea lor pe un server extern, însă prelucrarea lor se va face tot de la un sistem de calcul situat în România.

Transferul către o țară terță de date personale care fac obiectul unei prelucrari sau sunt destinate să fie prelucrate după transfer poate avea loc numai în condițiile în care nu se încalcă legislația de protecție a datelor.

De asemenea, țara terță către care se intenționează transferul trebuie să asigure un nivel de protecție adecvat, condiție apreciată de Comisia Europeană printr-o decizie de punere în aplicare), sau, dacă lipsește acea decizie, operatorul trebuie să ofere garanții adecvate, în condițiile prevăzute de art. 46 din Regulamentul European;

În absența deciziei Comisiei Europene sau a unor garanții adecvate, poate avea loc un transfer către o țară terță în situațiile prevăzute de lege.

Capitolul VII

Autoritatea de supraveghere

Art.39 Competențe

Autoritatea de supraveghere are competențele stabilite de lege

Art.40 Procedura

Procedura în care este implicat operatorul sau persoana vizată cu autoritatea de supraveghere se desfășoară conform legii**.**

Capitolul VIII

Dispoziții finale

Art.41 Dispoziții finale

Prezentul regulament stabilește normele interne referitoare la protecția persoanelor vizate în ceea ce privește prelucrarea datelor personale efectuată de operator.

Temeiul legal în baza căruia a fost adoptat prezentul regulament este format de Regulamentul European de protecție a datelor personale și de legile naționale de punere în aplicare, cu modificările și completările ulterioare.

Prezentul regulament nu conține derogări de la legislația în domeniu, acesta preluând legislația de referință indicată, nu conferă drepturi noi și nici nu restrânge din drepturile existente. Ca atare:

-în situația modificării legislației din domeniu, prezentul regulament se actualizează de drept, conform noilor prevederi, conducerea operatorului având doar obligația de a actualiza înscrisul cu noile prevederi;

-în situația când apar neconcordanțe între prezentul regulament intern și legislația europeană sau națională în domeniul protecției datelor, se aplică prevederile legislative.

OPERATOR,

_____ L.S.