PROTECŢIA DATELOR CU CARACTER PERSONAL

Protectia datelor cu caracter personal

Acquis relevant

- Convenţia de punere în aplicare a Acordului Schengen din 14 iunie 1985 între guvernele statelor din Uniunea Economică Benelux, Republicii Federale Germania şi Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune, publicată în Jurnalul Oficial al Uniunii EuropeneL 239, 22.9.2000, p. 19.
- Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981, ratificată prin Legea nr.682/2001.
- Decizia cadru 977/2008/JAI privind protecţia datelor cu caracter personal prelucrate în cadrul cooperării poliţieneşti şi judiciare în materie penală.
- Decizia-cadru 2006/960/JAI a Consiliului privind simplificarea schimbului de informaţii şi date operative între autorităţile de aplicare a legii ale statelor membre ale Uniunii Europene.
- Directiva 95/46/CE, publicată în Jurnalul Oficial al Uniunii Europene L 281, 23.11.1995;
- Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal (ETS nr. 108), Consiliul Europei, 28.1.1981 (Convenţia 108 a Consiliului Europei).
- Protocolul adiţional la Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, cu privire la autorităţile de control şi fluxul transfrontalier al datelor, adoptat la Strasbourg la 18 noiembrie 2001, ratificat prin Legea nr. 55 /2005;

Legislaţia naţională care asigură cadrul juridic pentru aplicarea acquis-ului în domeniu

- Decizia ANSPDCP Nr. 60 din 6 iunie 2006 privind stabilirea unor formulare tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
- Decizia ANSPDCP Nr. 89 din 18 iulie 2006 privind stabilirea categoriilor de operaţiuni de prelucrare a datelor cu caracter personal, susceptibile de a prezenta riscuri speciale pentru drepturile şi libertăţile persoanelor;
- Decizia ANSPDCP Nr. 90 din 18 iulie 2006 privind cazurile în care nu este necesară notificarea prelucrării unor date cu caracter personal;
- Decizia ANSPDCP Nr. 91 din 18 iulie 2006 privind cazurile în care este permisă notificarea simplificată a prelucrării datelor cu caracter personal;
- Hotărârea Guvernului nr.781 din 25.07.2002 privind protecţia informaţiilor secrete de serviciu;
- HOTĂRÂREA nr. 16/2005 pentru aprobarea Regulamentului de organizare şi funcţionare a Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- Instrucţiunile ministrului administraţiei şi internelor nr. 27/2010 privind măsurile de natură organizatorica si tehnică pentru asigurarea securităţii prelucrărilor de date cu caracter personal efectuate de către structurile/unităţile Ministerului Administraţiei si Internelor;
- Legea 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice;
- Legea nr. 102 din 03.05.2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal - denumită în continuare A.N.S.P.D.C.P;
- Legea nr. 677 din 21.11.2001, privind protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
- Ordinul Avocatului Poporului nr. 75/2002 privind stabilirea unor măsuri şi proceduri specifice care să asigure un nivel satisfăcător de protecţie a drepturilor persoanelor ale căror date cu caracter personal fac obiectul prelucrărilor);
- Ordinul Avocatului Poporului nr.52/2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;

1. Imperativitatea protecţiei datelor cu caracter personal

1.1. Principiile care stau la baza protecţiei datelor cu caracter personal sunt:

a) prelucrate cu buna-credinţă şi în conformitate cu dispoziţiile legale în vigoare;

Prelucrarea datelor include colectarea, înregistrarea, organizarea, stocarea, consultarea, utilizarea, transferul, combinarea, blocarea, ştergerea sau distrugerea lor.

Datele obţinute se vor prelucra numai în scopurile permise de lege.

Legea impune condiţii suplimentare când este vorba de date sensibile, referitoare la originea rasială sau etnică, convingerile politice, religioase, apartenenţa sindicală, starea de sănătate sau viaţa sexuală.

b) colectate în scopuri determinate, explicite şi legitime;

Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau ştiinţifică nu va fi considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea dispoziţiilor legilor în vigoare, inclusiv a celor care privesc efectuarea notificării către autoritatea de supraveghere, precum şi cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele care reglementează activitatea statistica ori cercetarea istorică sau ştiinţifică;

c) adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate;

d) exacte şi, dacă este cazul, actualizate; în acest scop se vor lua măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate şi pentru care vor fi ulterior prelucrate, să fie şterse sau rectificate;

e) stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate şi în care vor fi ulterior prelucrate;

Stocarea datelor pe o durata mai mare decât cea menţionată, în scopuri statistice, de cercetare istorică sau ştiinţifică, se va face cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele care reglementează aceste domenii, şi numai pentru perioada necesară realizării acestor scopuri.

1.2. Legitimitatea prelucrărilor

Cu anumite excepţii [a se vedea categoriile speciale de date (ex. : datele legate de originea rasială), datele cu caracter personal având funcţie de identificare (ex: codul numeric personal) şi datele cu caracter personal referitoare la fapte penale sau contravenţii, care beneficiază de un regim special], orice prelucrare de date cu caracter personal poate fi efectuată numai dacă persoana vizată şi-a dat consimţământul în mod expres şi neechivoc pentru acea prelucrare.

Consimţământul persoanei vizate nu este necesar în următoarele cazuri:

a) când prelucrarea este necesară în vederea executării unui contract sau antecontract la care persoana vizată este parte ori în vederea luării unor măsuri, la cererea acesteia, înaintea încheierii unui contract sau antecontract;

b) când prelucrarea este necesară în vederea protejării vieţii, integrităţii fizice sau sănătăţii persoanei vizate ori a unei alte persoane ameninţate;

c) când prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale a operatorului;

d) când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terţul căruia îi sunt dezvăluite datele;

e) când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terţului căruia îi sunt dezvăluite datele, cu condiţia ca acest interes să nu prejudicieze interesul sau drepturile şi libertăţile fundamentale ale persoanei vizate.

f) când prelucrarea priveşte date obţinute din documente accesibile publicului, conform legii;

g) când prelucrarea este făcută exclusiv în scopuri statistice, de cercetare istorică sau ştiinţifică, iar datele rămân anonime pe toată durata prelucrării.

1.3. Categorii special de date cu caracter personal

- Prelucrarea datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice sau de natură similară, de apartenenţa sindicală, precum şi a datelor cu caracter personal privind starea de sănătate sau viaţa sexuală este interzisă.

Excepţii de la această regulă apar în următoarele cazuri:

a) când persoana vizată şi-a dat în mod expres consimţământul pentru o astfel de prelucrare;

b) când prelucrarea este necesară în scopul respectării obligaţiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanţiilor prevăzute de lege; o eventuală dezvăluire către un terţ a datelor prelucrate poate fi efectuată numai dacă există o obligaţie legală a operatorului în acest sens sau dacă persoana vizată a consimţit expres la această dezvăluire;

c) când prelucrarea este necesară pentru protecţia vieţii, integrităţii fizice sau a sănătăţii persoanei vizate ori a altei persoane, în cazul în care persoana vizată se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) când prelucrarea este efectuată în cadrul activităţilor sale legitime de către o fundaţie, asociaţie sau de către orice altă organizaţie cu scop nelucrativ şi cu specific politic, filozofic, religios ori sindical, cu condiţia ca persoana vizată să fie membră a acestei organizaţii sau să întreţină cu aceasta, în mod regulat, relaţii care privesc specificul activităţii organizaţiei şi ca datele să nu fie dezvăluite unor terţi fără consimţământul persoanei vizate;

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

f) când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiţie;

g) când prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente medicale pentru persoana vizată ori de gestionare a serviciilor de sănătate care acţionează în interesul persoanei vizate, cu condiţia ca prelucrarea datelor respective să fie efectuate de către ori sub supravegherea unui cadru medical supus secretului profesional sau de către ori sub supravegherea unei alte persoane supuse unei obligaţii echivalente în ceea ce priveşte secretul;

h) când legea prevede în mod expres aceasta în scopul protejării unui interes public important, cu condiţia ca prelucrarea să se efectueze cu respectarea drepturilor persoanei vizate şi a celorlalte garanţii prevăzute de prezenta lege.

- Prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală poate fi efectuată numai dacă:

a) persoana vizată şi-a dat în mod expres consimţământul; sau

b) prelucrarea este prevăzută în mod expres de o dispoziţie legală.

Autoritatea de supraveghere poate stabili şi alte cazuri în care se poate efectua prelucrarea acestor date, numai cu condiţia instituirii unor garanţii adecvate pentru respectarea drepturilor persoanelor vizate.

- Prelucrarea datelor cu caracter personal privind starea de sănătate pot fi prelucrate numai dacă:

a) dacă prelucrarea este necesară pentru protecţia sănătăţii publice;

b) dacă prelucrarea este necesară pentru prevenirea unui pericol iminent, pentru prevenirea săvârşirii unei fapte penale sau pentru împiedicarea producerii rezultatului unei asemenea fapte ori pentru înlăturarea urmărilor prejudiciabile ale unei asemenea fapte

Prelucrarea datelor privind starea de sănătate poate fi efectuată numai de către ori sub supravegherea unui cadru medical, cu condiţia respectării secretului profesional, cu excepţia situaţiei în care persoana vizata si-a dat în scris şi în mod neechivoc consimţământul atâta timp cât acest consimţământ nu a fost retras, precum şi cu excepţia situaţiei în care prelucrarea este necesară pentru prevenirea unui pericol iminent, pentru prevenirea săvârşirii unei fapte penale, pentru împiedicarea producerii rezultatului unei asemenea fapte sau pentru înlăturarea urmărilor sale prejudiciabile.

Cadrele medicale, instituţiile de sănătate şi personalul medical al acestora pot prelucra date cu caracter personal referitoare la starea de sănătate, fără autorizaţia autorităţii de supraveghere, numai dacă prelucrarea este necesară pentru protejarea vieţii, integrităţii fizice sau sănătăţii persoanei vizate. Când scopurile menţionate se referă la alte persoane sau la public în general şi persoana vizata nu si-a dat consimţământul în scris şi în mod neechivoc, trebuie cerută şi obţinută în prealabil autorizaţia autorităţii de supraveghere. Prelucrarea datelor cu caracter personal în afară limitelor prevăzute în autorizaţie este interzisă.

Cu excepţia motivelor de urgenta, autorizaţia prevăzută la paragraful anterior poate fi acordată numai după ce a fost consultat Colegiul Medicilor din România.

Datele cu caracter personal privind starea de sănătate pot fi colectate numai de la persoana vizată. Prin excepţie, aceste date pot fi colectate din alte surse numai în măsura în care este necesar pentru a nu compromite scopurile prelucrării, iar persoana vizată nu vrea ori nu le poate furniza.

- Prelucrarea datelor cu caracter personal referitoare la săvârşirea de infracţiuni de către persoana vizată ori la condamnări penale, măsuri de siguranţă sau sancţiuni administrative ori contravenţionale, aplicate persoanei vizate, poate fi efectuată numai de către sau sub controlul autorităţilor publice, în limitele puterilor ce le sunt conferite prin lege şi în condiţiile stabilite de legile speciale care reglementează aceste materii.

ANSPDCP poate stabili şi alte cazuri în care se poate efectua prelucrarea acestor date numai cu condiţia instituirii unor garanţii adecvate pentru respectarea drepturilor persoanelor vizate. În acelaşi timp, un registru complet al condamnărilor penale poate fi ţinut numai sub controlul unei autorităţi publice, în limitele puterilor ce îi sunt conferite prin lege.

Faţă de regulile speciale anume expuse ar mai fi de adăugat faptul că acestea nu se aplică în situaţia în care prelucrarea datelor se face exclusiv în scopuri jurnalistice, literare sau artistice, dacă prelucrarea priveşte date cu caracter personal 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.

2. Măsuri organizatorice şi tehnice pentru asigurarea protecţiei datelor cu caracter personal

Operatorul este obligat să aplice măsurile tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală.

Aceste măsuri trebuie să asigure, potrivit stadiului tehnicii utilizate în procesul de prelucrare şi de costuri, un nivel de securitate adecvat în ceea ce priveşte riscurile pe care le reprezintă prelucrarea, precum şi în ceea ce priveşte natura datelor care trebuie protejate.

Cerinţele minime de securitate a bazelor de date :

.2.1. Identificarea şi autentificarea utilizatorului

Prin utilizator se înţelege orice persoană care acţionează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea se poate face prin mai multe metode, cum ar fi: introducerea codului de identificare de la tastatură (un şir de caractere), folosirea unei cartele cu cod de bare, folosirea unei cartele inteligente (smart card) sau a unei cartele magnetice.

Fiecare utilizator are propriul său cod de identificare. Niciodată mai mulţi utilizatori nu trebuie să aibă acelaşi cod de identificare.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată trebuie dezactivate şi distruse după un control prealabil intern al operatorului. Perioada după care codurile trebuie dezactivate şi distruse se stabileşte de operator.

Orice cont de utilizator este însoţit de o modalitate de autentificare. Autentificarea poate fi făcută prin introducerea unei parole sau prin mijloace biometrice: amprenta dactiloscopică, amprenta vocală, etc.

Parolele sunt şiruri de caractere. Cu cât şirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afişate în clar pe monitor. Parolele trebuie schimbate periodic în funcţie de politicile de securitate ale entităţii (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face numai de către utilizatori autorizaţi de operator.

Operatorul trebuie să solicite realizarea unui sistem informaţional care să refuze automat accesul unui utilizator după 5 introduceri greşite ale parolei.

Orice utilizator care primeşte un cod de identificare şi un mijloc de autentificare trebuie să păstreze confidenţialitatea acestora şi să răspundă în acest sens în faţa operatorului.

Fiecare entitate va stabili o procedură proprie de administrare şi gestionare a conturilor de utilizator.

Operatorii autorizează anumiţi utilizatori pentru a revoca sau a suspenda un cod de identificare şi autentificare, dacă utilizatorul acestora şi-a dat demisia ori a fost concediat, şi-a încheiat contractul, a fost transferat la alt serviciu şi noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.

Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de conducerea entităţii.

2.2. Tipul de acces

Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu. Pentru aceasta operatorii trebuie să stabilească tipurile de acces după funcţionalitate (cum ar fi: administrare, introducere, prelucrare, salvare etc.) şi după acţiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, ştergere), precum şi procedurile privind aceste tipuri de acces.

Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri excepţionale.

Pentru activitatea de pregătire a utilizatorilor sau pentru realizarea de prezentări se vor folosi date anonime. Angajaţii care predau cursurile de pregătire vor folosi date cu caracter personal pe parcursul propriei lor pregătiri.

Operatorul va stabili modalităţile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câţiva utilizatori.

2.3. Colectarea datelor

Operatorul desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional.

Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizaţi desemnaţi de operator.

Operatorul va lua măsuri pentru ca sistemul informaţional să înregistreze cine a făcut modificarea, data şi ora modificării. Pentru o mai bună administrare operatorul va lua măsuri ca sistemul informaţional să menţină datele şterse sau modificate.

2.4. Execuţia copiilor de siguranţă

Operatorul stabileşte intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date cu caracter personal, precum şi ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranţă vor fi numiţi de operator, într-un număr restrâns. Copiile de siguranţă se vor stoca în alte camere, în fişete metalice cu sigiliu aplicat, şi, dacă este posibil, chiar în camere din altă clădire.

Operatorul trebuie să ia măsuri ca accesul la copiile de siguranţă să fie monitorizat.

2.5. Computerele şi terminalele de acces

Computerele şi alte terminale de acces pot fi instalate în încăperi cu acces restricţionat.

Dacă nu pot fi asigurate aceste condiţii, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei ori cartele magnetice.

Dacă pe ecran apar date cu caracter personal asupra cărora nu se acţionează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat. Mărimea acestei perioade se determină în funcţie de operaţiile care trebuie executate.

Terminalele de acces folosite în relaţia cu publicul, pe care apar date cu caracter personal, vor fi poziţionate astfel încât să nu poată fi văzute de public şi după o perioadă scurtă, stabilită de operator, în care nu se acţionează asupra lor, acestea trebuie ascunse.

2.6. Fişierele de acces

Operatorul este obligat să ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fişier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator.

Informaţiile înregistrate în fişierul de acces sau în registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fişierului accesat (fişei);
- numărul înregistrărilor efectuate;
- tipul de acces;
- codul operaţiei executate sau programul folosit;
- data accesului (an, lună, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrările automate aceste informaţii vor fi stocate într-un fişier de acces general sau în fişiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

Operatorul este obligat să păstreze fişierele de acces cel puţin 2 ani, pentru a fi folosite ca probe în cazul unor investigaţii. Dacă investigaţiile se prelungesc, aceste fişiere se vor păstra atât timp cât se va considera necesar.

Fişierele de acces trebuie să facă posibilă identificarea de către operator sau de către persoana împuternicită a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancţiuni sau a sesizării organelor competente.

2.7. Sistemele de telecomunicaţii

Operatorul este obligat să facă periodic controlul autentificărilor şi tipurilor de acces pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea sistemelor de telecomunicaţii.

Operatorii sunt obligaţi să conceapă sistemul de telecomunicaţii astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicaţii nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmisia datelor cu caracter personal.

Prin sistemele de telecomunicaţii se vor transmite numai datele cu caracter personal strict necesare.

2.8. Instruirea personalului

În cadrul cursurilor de pregătire a utilizatorilor operatorul este obligat să facă informarea acestora cu privire la prevederile Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, la cerinţele minime de securitate a prelucrărilor de date cu caracter personal, precum şi cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii utilizatorului.

Utilizatorii care au acces la date cu caracter personal vor fi instruiţi de către operator asupra confidenţialităţii acestora şi vor fi avertizaţi prin mesaje care vor apărea pe monitoare în timpul activităţii. Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.

2.9. Folosirea computerelor

Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva viruşilor informatici) operatorul va lua măsuri care vor consta în:

a) interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;

b) informarea utilizatorilor în privinţa pericolului privind viruşii informatici;

c) implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informatice;

d) dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afişate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.

2.10. Imprimarea datelor

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru această operaţiune de către operator. Operatorii sunt obligaţi să aprobe proceduri interne specifice privind folosirea şi distrugerea acestor materiale.

Fiecare entitate îşi va aproba propriul sistem de securitate, ţinând seama de aceste cerinţe minime de securitate a prelucrărilor de date cu caracter personal, iar în funcţie de importanţa datelor cu caracter personal prelucrate, îşi va impune măsuri de securitate suplimentare.

3. Supravegherea video

3.1. Cine ar trebui consultat când se introduce un sistem de supraveghere video?

Consultarea cu părţile interesate şi cu autorităţile competente este esenţială în identificarea tuturor problemelor protecţiei datelor personale relevante. Atunci când se hotărăşte folosirea unui sistem de supraveghere video şi se stabileşte cadrul şi politicile necesare protecţiei datelor personale, ar trebui consultate câteva sau toate organizaţiile următoare:

- Responsabilul cu protecţia datelor personale din instituţia respectivă
- Reprezentanţii angajaţilor
- Alte părţi interesate (incluzând, în unele cazuri, autorităţile locale)
- A.N.S.P.D.C.P.

3.2. Scopul supravegherii video

Înainte de a decide instalarea unui sistem de supraveghere, instituţia care doreşte acest lucru trebuie mai întâi să stabilească scopul pentru care se instalează sistemul de supraveghere şi trebuie să se asigure că acest scop este legal.

Scopul trebuie să fie clar, specific şi explicit. Vag, ambiguu sau simplu nu este de ajuns. Fiind specific scopului sistemului de supraveghere poate ajuta instituţia să fie în conformitate cu legislaţia în vigoare, să evalueze succesul sistemului lor şi să explice personalului şi publicului de ce este nevoie de el.

Scopul sistemului de supraveghere trebuie comunicat publicului într-un rezumat, la avizier şi detaliat pe site-ul web al instituţiei(în versiunea on-line a politicii de supraveghere video).

Limitarea privind folosirea datelor cu caracter personal trebuie să fie clar stabilită mai ales dacă acest lucru este cerut de reprezentanţii angajaţilor sau de alte părţi interesate. Mai mult, trebuie asigurat faptul că datele cu caracter personal nu vor fi folosite ulterior pentru alte scopuri sau introduse în dispozitive neprevăzute, astfel încât ele să fie folosite pentru scopuri care nu au fost luate în calcul.

Dacă o instituţie foloseşte sistemul de supraveghere video doar pentru scopuri de securitate şi acces, acest lucru poate fi considerat ca potenţial necesar pentru gestionarea şi funcţionarea instituţiei. Din această cauză, sistemul de supraveghere video se va baza pe un cadru legal.

În alt caz, reiese întrebarea dacă sunt incidente alte dispoziţii legale pentru supravegherea video. Exemple în acest sens pot fi următoarele situaţii:

- atunci când există o obligaţie legală pentru a avea un sistem de supraveghere video;
- atunci când persoanele vizate şi-au dat consimţământul.

Există alternative care au un impact mai redus în viaţa intimă şi privată?

Instituţia trebuie, de asemenea, să evalueze dacă există metode care au un impact mai redus pentru a obţine rezultatul dorit, fără a se folosi sistemul de supraveghere video. Supravegherea video nu ar trebui folosită dacă alte alternative adecvate sunt disponibile. O alternativă nu poate să fie considerată adecvată dacă nu este realizabilă, dacă este mai puţin eficientă decât supravegherea video sau dacă implică costuri disproporţionate.

Pe de altă parte, simpla disponibilitate a tehnologiei la un preţ relativ mic nu justifică folosirea sistemelor de supraveghere video.

Chiar dacă o instituţie concluzionează că există necesitatea folosirii unui sistem de supraveghere video şi că nu sunt alte metode disponibile ce au un impact mai redus asupra vieţii intime şi private, ar trebui să folosească această tehnologie în cazul în care efectele negative ale supravegherii video sunt compensate de beneficiile acesteia.

3.3. Monitorizarea angajaţilor

Măsuri de monitorizarea intruzive pot provoca angajaţilor un stres care nu este necesar şi în acelaşi timp pot provoca neîncrederea în organizaţie. De aceea, folosirea supravegherii video pentru a monitoriza cum îşi fac angajaţi treaba ar trebui evitată, neluând în considerare cazurile de excepţie în care instituţia demonstrează că are un interes imperativ în a-i monitoriza.

De aceea, o astfel de supraveghere trebuie să fie precedată de efectuarea unei evaluări de impact realizată de către instituţie.

Ţeluri ca gestionarea productivităţii la locul de muncă, asigurarea calităţii controlului, executarea politicilor instituţiei sau oferirea de dovezi privind rezolvarea disputelor, în principiu, în mod singular nu justifică supravegherea video a angajaţilor în cadrul instituţiei

3.4. Selectarea, poziţionarea şi configurarea sistemului de supraveghere video

Localizarea camerelor şi unghiuri de vizionare

Localizarea camerelor ar trebui să fie aleasă astfel încât să minimizeze vederea zonelor care nu sunt relevante scopului pentru care a fost amplasat sistemul de supraveghere.

Ca regulă, instalarea unui sistem de supraveghere video cu scopul de a proteja bunuri (de exemplu: proprietăţi sau informaţii) ale instituţiei sau pentru siguranţa personalului şi a vizitatorilor trebuie să se limiteze la monitorizarea:

- zonelor/spaţiilor în care sunt stocate informaţii sensibile , obiecte de mare valoare sau alte bunuri care necesită o protecţie sporită dintr-un motiv anume.
- Puncte de intrare şi ieşire ale clădirii (incluzând ieşiri de urgenţă sau ziduri şi garduri care împrejmuiesc clădirea).
- Puncte de intrare şi ieşire din clădire care fac legătura cu zone pentru care nu sunt instituite drepturi de acces şi sunt separate prin uşi închise sau alt mecanism de control al accesului.

Nu poate să fie exclus însă, faptul că cerinţele de securitate pot justifica o monitorizarea specială în cadrul unor clădiri. În acest caz, planurile de securitate ar trebui să cuprindă politici de supraveghere video şi instituţia ar trebui să justifice necesitatea şi proporţionalitate monitorizării suplimentare. Justificarea necesităţii şi proporţionalităţii unei astfel de monitorizări suplimentare se realizează printr-o evaluare de impact sau în alt mod.

Numărul de camere

Numărul de camere care trebuie instalate va depinde de mărimea clădirii şi de nevoile de securitate care, la rândul său, sunt condiţionate de o varietate de factori. Acelaşi număr şi tip de camere ar putea să fie potrivite pentru o instituţie dar, în acelaşi timp, să fie total disproporţionate pentru altă instituţie. În orice caz, numărul de camere este un bun indicator privind complexitatea şi mărimea sistemului de supraveghere şi ar putea sugera creşterea riscurilor ce privesc viaţa privată şi alte drepturi fundamentale. O dată cu creşterea numărului camerelor apare şi riscul ca ele să nu fie folosite eficient şi apare o suprasarcină de informaţii.

În acelaşi timp menţionăm că numărul de camere trebuie cuprins în politica de supraveghere.

4. Drepturile persoanei vizate

Drepturile persoanei sunt reglementate prin Legea nr.677/2001 fiind prevăzute în mod expres:

4.1. Dreptul la informare

Dreptul la informare, care se realizează în funcţie de două modalităţi de obţinere a datelor:

A. Când datele cu caracter personal sunt obţinute direct de la persoana vizată, cu excepţia cazului în care această persoană posedă deja informaţiile respective, operatorul **este obligat** să-i furnizeze cel puţin următoarele informaţii:

a) identitatea operatorului şi a reprezentantului acestuia, dacă este cazul;

b) scopul în care se face prelucrarea datelor;

c) informaţii suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie şi consecinţele refuzului de a le furniza; existenţa drepturilor legale, în special a dreptului de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care pot fi exercitate;

d) orice alte informaţii a căror furnizare este impusă prin dispoziţie a autorităţii de supraveghere, ţinând seama de specificul prelucrării.

B. când datele nu sunt obţinute direct de la persoana vizată:

Cu excepţia cazului în care persoana vizată posedă deja informaţiile respective, operatorul este obligat ca, în momentul colectării datelor sau, dacă se intenţionează dezvăluirea acestora către terţi, cel mai târziu până în momentul primei dezvăluiri, să furnizeze persoanei vizate cel puţin următoarele informaţii:

a) identitatea operatorului şi a reprezentantului acestuia, dacă este cazul;

b) scopul în care se face prelucrarea datelor;

c) informaţii suplimentare, precum: categoriile de date vizate, destinatarii sau categoriile de destinatari ai datelor, existenţa drepturilor legale, în special a dreptului de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care pot fi exercitate;

d) orice alte informaţii a căror furnizare este impusă prin dispoziţie a autorităţii de supraveghere, ţinând seama de specificul prelucrării.

De la regulile de realizare a acestui drept, menţionate anterior, **există şi anumite excepţii**:

- nu se aplică atunci când prelucrarea datelor se efectuează exclusiv în scopuri jurnalistice, literare sau artistice, dacă aplicarea acestora ar da indicii asupra surselor de informare.

- nu se aplică în cazul în care prelucrarea datelor se face în scopuri statistice, de cercetare istorică sau ştiinţifică, ori în orice alte situaţii în care furnizarea unor asemenea informaţii se dovedeşte imposibilă sau ar implica un efort disproporţionat faţă de interesul legitim care ar putea fi lezat, precum şi în situaţiile în care înregistrarea sau dezvăluirea datelor este expres prevăzută de le

4.2. Drepturile persoanei vizate în contextul prelucrări datelor cu caracter personal

Dreptul de acces la date

Orice persoana vizată are dreptul de a obţine de la operator, la cerere şi în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta. Operatorul este obligat, în situaţia în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puţin următoarele:

a) informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile cu privire la originea datelor;

c) informaţii asupra principiilor de funcţionare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă;

d) informaţii privind existenta dreptului de intervenţie asupra datelor şi a dreptului de opoziţie, precum şi condiţiile în care pot fi exercitate;

e) informaţii asupra posibilităţii de a consulta registrul de evidenţă a prelucrărilor de date cu caracter personal, de a înainta plângere către autoritatea de supraveghere, precum şi de a se adresa instanţei pentru atacarea deciziilor operatorului, în conformitate cu dispoziţiile prezentei legi.

Dreptul de opoziţie

Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, ca date care o vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care exista dispoziţii legale contrare. In caz de opoziţie justificată prelucrarea nu mai poate viza datele în cauză.

Persoana vizata are dreptul de a se opune în orice moment, în mod gratuit şi fără nici o justificare, ca datele care o vizează să fie prelucrate în scop de marketing direct, în numele operatorului sau al unui terţ, sau să fie dezvăluite unor terţi într-un asemenea scop.

Dreptul de a nu fi supus unei decizii individuale

A .Orice persoana are dreptul de a cere şi de a obţine:

- retragerea sau anularea oricărei decizii care produce efecte juridice în privinţa sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată sa evalueze unele aspecte ale personalităţii sale, precum competenta profesională, credibilitatea, comportamentul sau ori alte asemenea aspecte;
- reevaluarea oricărei alte decizii luate în privinţa sa, care o afectează în mod semnificativ, dacă decizia a fost adoptată exclusiv pe baza unei prelucrări de date care întruneşte condiţiile prevăzute la lit. a).

B. Respectându-se garanţiile prevăzute de legea 677/2001 , o persoana poate fi supusă unei decizii de natura celei vizate la litera A, numai în următoarele situaţii:

- decizia este luată în cadrul încheierii sau executării unui contract, cu condiţia ca cererea de încheiere sau de executare a contractului, introdusă de persoana vizată, să fi fost satisfăcută sau ca unele măsuri adecvate, precum posibilitatea de a-şi susţine punctul de vedere, să garanteze apărarea propriului interes legitim;
- decizia este autorizata de o lege care precizează măsurile ce garantează apărarea interesului legitim al persoanei vizate.

Dreptul de a se adresa justiţiei

Fără a se aduce atingere posibilităţii de a se adresa cu plângere autorităţii de supraveghere, persoanele vizate au dreptul de a se adresa justiţiei pentru apărarea oricăror drepturi garantate de prezenta lege, care le-au fost încălcate.

Orice persoana care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuată ilegal, se poate adresa instanţei competente pentru repararea acestuia.

Instanţa competentă este cea în a cărei rază teritorială domiciliază reclamantul. Cererea de chemare în judecata este scutită de taxa de timbru.

Dreptul de intervenţie asupra datelor

Orice persoana vizata are dreptul de a obţine de la operator, la cerere şi în mod gratuit:

a) după caz, rectificarea, actualizarea, blocarea sau ştergerea datelor a căror prelucrare nu este conformă prezentei legi, în special a datelor incomplete sau inexacte;

b) după caz, transformarea în date anonime a datelor a căror prelucrare nu este conformă prezentei legi;

c) notificarea către terţii cărora le-au fost dezvăluite datele a oricărei operaţiuni efectuate conform lit. a) sau b), dacă aceasta notificare nu se dovedeşte imposibilă sau nu presupune un efort disproporţionat faţă de interesul legitim care ar putea fi lezat.

4.3. Exercitarea drepturilor de către persoana vizată

Persoana vizata poate solicita de la operator informaţiile, printr-o cerere întocmită în formă scrisă, datată şi semnată. În cerere solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondentă care să asigure că predarea i se va face numai personal.

Operatorul este obligat să comunice informaţiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opţiuni a solicitantului exprimate.

In cazul datelor cu caracter personal legate de starea de sănătate, cererea poate fi introdusă de persoana vizată fie direct, fie prin intermediul unui cadru medical care va indica în cerere persoana în numele căreia este introdusă. La cererea operatorului sau a persoanei vizate comunicarea poate fi făcută prin intermediul unui cadru medical desemnat de persoana vizată.

In cazul în care datele cu caracter personal legate de starea de sănătate sunt prelucrate în scop de cercetare ştiinţifică, dacă nu exista, cel puţin aparent, riscul de a se aduce atingere drepturilor persoanei vizate şi dacă datele nu sunt utilizate pentru a lua decizii sau măsuri fata de o anumită persoana, comunicarea se poate face şi într-un termen mai mare decât cel de 15 zile, în măsura în care aceasta ar putea afecta bunul mers sau rezultatele cercetării, şi nu mai târziu de momentul în care cercetarea este încheiată. In acest caz persoana vizată trebuie sa îşi fi dat în mod expres şi neechivoc consimţământul ca datele să fie prelucrate în scop de cercetare ştiinţifică, precum şi asupra posibilei amânări a comunicării din acest motiv.

Persoana vizată nu poate solicita de la operator informaţii atunci când prelucrarea datelor se efectuează exclusiv în scopuri jurnalistice, literare sau artistice, dacă aplicarea acestora ar da indicii asupra surselor de informare.

4.4. Limitări ale exercitări drepturilor persoanei vizate

Sunt prevăzute de Legea nr.677/2001 care stabileşte faptul că în cadrul activităţilor de prevenire, cercetare şi reprimare a infracţiunilor şi de menţinere a ordinii publice, precum şi al altor activităţi desfăşurate în domeniul dreptului penal,
dispoziţiile privind dreptul la informare, dreptul de acces, dreptul de intervenţie şi dreptul de opoziţie nu se aplică dacă prin aplicarea acestora este prejudiciata eficienta acţiunii sau obiectivul urmărit în îndeplinirea atribuţiilor legale ale autorităţii publice.

Limitarea acestor drepturi este aplicabilă strict pentru perioada necesară atingerii obiectivului urmărit prin desfăşurarea activităţilor de prevenire, cercetare şi reprimare a infracţiunilor şi de menţinere a ordinii publice, precum şi al altor activităţi desfăşurate în domeniul dreptului penal.

Dispoziţiile Legii nr.238/2009 sunt mai specifice în acest sens şi stabilesc faptul că dispoziţiile referitoare la exercitarea drepturilor persoanei vizate, prevăzute de Legea nr. 677/2001 nu se aplică pe perioada în care o asemenea măsură este necesară pentru evitarea prejudicierii activităţilor specifice de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice, ca urmare a cunoaşterii de persoana vizată a faptului că datele sale cu caracter personal sunt prelucrate, sau este necesară pentru protejarea persoanei vizate ori a drepturilor şi libertăţilor altor persoane, în cazul în care există date ţi informaţii că aceste drepturi şi libertăţi sunt puse în pericol.

5. Autoritatea Naţională de Supraveghere a prelucrării Datelor cu Caracter Personal

În statele membre ale Uniunii Europene, activitatea de protecţie a datelor cu caracter personal revine unor autorităţi sau instituţii special constituite pentru îndeplinirea unor astfel de competenţe. În vederea alinierii legislaţiei României la acquis-ul comunitar, prin Legea nr. 102/2005, intrată în vigoare la data de 12 mai 2005, a fost înfiinţată Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Statutul de autoritate independentă este consacrat chiar la primul articol al acestui act normativ, unde se precizează că Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal este o autoritate publică autonomă şi independentă faţă de orice autoritate a administraţiei publice, ca şi faţă de orice persoană fizică sau juridică din domeniul privat. Potrivit legii, Autoritatea nu poate fi supusă nici unui mandat imperativ sau reprezentativ şi nu poate fi obligată să se supună instrucţiunilor sau dispoziţiilor altei autorităţi publice sau entităţi de drept privat.

Autoritatea are drept obiectiv apărarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţă intimă, familială şi privată, în legătură cu prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

5.1. Atribuţii

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal îşi desfăşoară activitatea în condiţii de completă independenţă şi imparţialitate. Autoritatea monitorizează şi controlează sub aspectul legalităţii prelucrările de date cu caracter personal care cad sub incidenţa Legii nr. 677/2001. În acest scop, autoritatea de supraveghere exercită următoarele atribuţii:

· primeşte şi analizează notificările privind prelucrarea datelor cu caracter personal;

· autorizează prelucrările de date în situaţiile prevăzute de lege;

· poate dispune, în cazul în care constată încălcarea dispoziţiilor prezentei legi, suspendarea provizorie sau încetarea prelucrării datelor, ştergerea parţială ori integrală a datelor prelucrate şi poate să sesizeze organele de urmărire penală sau să intenteze acţiuni în justiţie;

· informează persoanele fizice şi/sau juridice asupra necesităţii respectării obligaţiilor şi îndeplinirii procedurilor prevăzute de Legea nr. 677/2001;

· păstrează şi pune la dispoziţia publicului registrul de evidenţă a prelucrărilor de date cu caracter personal;

· primeşte şi soluţionează plângeri, sesizări sau cereri de la persoanele fizice şi comunică soluţia dată ori, după caz, demersurile efectuate;

· efectuează controale prealabile în situaţia în care operatorul prelucrează date cu caracter personal care sunt susceptibile de a prezenta riscuri speciale pentru drepturile şi libertăţile persoanelor;

· efectuează investigaţii din oficiu sau la primirea unor plângeri ori sesizări;

· este consultată atunci când se elaborează proiecte de acte normative referitoare la protecţia drepturilor şi libertăţilor persoanelor, în privinţa prelucrării datelor cu caracter personal;

· poate face propuneri privind iniţierea unor proiecte de acte normative sau modificarea actelor normative în vigoare în domenii legate de prelucrarea datelor cu caracter personal;

· cooperează cu autorităţile publice şi cu organele administraţiei publice, centralizează şi analizează rapoartele anuale de activitate ale acestora privind protecţia persoanelor în privinţa prelucrării datelor cu caracter personal;

· formulează recomandări şi avize asupra oricărei chestiuni legate de protecţia drepturilor şi libertăţilor fundamentale în privinţa prelucrării datelor cu caracter personal, la cererea oricărei persoane, inclusiv a autorităţilor publice şi a organelor administraţiei publice;

· cooperează cu autorităţile similare din străinătate, în vederea asistenţei mutuale, precum şi cu persoanele cu domiciliul sau cu sediul în străinătate, în scopul apărării drepturilor şi libertăţilor fundamentale ce pot fi afectate prin prelucrarea datelor cu caracter personal;

· îndeplineşte alte atribuţii prevăzute de lege.

Autoritatea este condusă de un preşedinte a cărui funcţie este asimilată celei de secretar de stat.

Preşedintele Autorităţii este numit de Senat, pentru un mandat cu durata de 5 ani, care poate fi reînnoit o singură dată. Înainte de începerea exercitării mandatului, preşedintele Autorităţii depune în faţa plenului Senatului jurământul de credinţă.

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal a început să funcţioneze independent de instituţia Avocatul Poporului de la 1 ianuarie 2006.

La sfârşitul fiecărui an ANSPDCP emite un raport, care este prezentat Senatului, referitor la activitatea desfăşurată, în care sunt prezentate principalele activităţi desfăşurate de către aceasta.

5.2.Controale prealabile şi investigaţii

Autoritatea de supraveghere controlează, sub aspectul legalităţii, prelucrările de date cu caracter personal care cad sub incidenţa legii.

Activitatea de control se realizează prin:

a. Control prealabil – mijloc prevăzut de lege prin care autoritatea de supraveghere verifică ansamblul condiţiilor în care au loc prelucrările de date care sunt susceptibile să prezinte riscuri speciale.

b. Investigaţie – procedeu de exercitare a atribuţiilor ce revin autorităţii de supraveghere pentru controlul legalităţii prelucrărilor de date cu caracter personal care intră sub incidenţa legii.

Pentru respectarea legii şi protecţia persoanei vizate, în cazul în care constată încălcarea normelor legale, autoritatea de supraveghere poate dispune următoarele măsuri:

a. interzicerea efectuării unor prelucrări;
b. suspendarea provizorie a unora sau a tuturor operaţiunilor de prelucrare a datelor cu caracter personal;
c. încetarea prelucrării datelor;
d. ştergerea parţială ori integrală a datelor prelucrate;
e. intentarea unei acţiuni în justiţie pentru apărarea oricăror drepturi garantate de legislaţia în vigoare persoanelor vizate;
f. sesizarea organelor de urmărire penală.

5.3.Plângeri adresate autorităţii de supraveghere

În vederea apărării drepturilor prevăzute de prezenta lege; persoanele ale căror date cu caracter personal fac obiectul unei prelucrări care cade sub incidenţa legii pot înainta plângere către autoritatea de supraveghere.

Plângerea se poate face direct sau prin reprezentant. Plângerea către autoritatea de supraveghere nu poate fi înaintată dacă o cerere în justiţie, având acelaşi obiect şi aceleaşi părţi, a fost introdusă anterior.

În afara cazurilor în care o întârziere ar cauza un prejudiciu iminent şi ireparabil, plângerea către autoritatea de supraveghere nu poate fi înaintată mai devreme de 15 zile de la înaintarea unei plângeri cu acelaşi conţinut către operator.

Dacă plângerea este găsită întemeiată, autoritatea de supraveghere poate dispune suspendarea provizorie sau încetarea prelucrării datelor, ştergerea parţială sau integrală a prelucrării datelor şi poate să sesizeze organele de urmărire penală sau să intenteze acţiune în justiţie. Decizia trebuie motivată şi se comunică părţilor interesate în termen de 30 de zile de la data primirii plângerii.

5.4.Contravenţii şi sancţiuni

Autoritatea de supraveghere poate aplica sancţiuni contravenţionale operatorului pentru:

- omisiunea de a notifica şi notificarea cu rea-credinţă;
- prelucrarea nelegală a datelor cu caracter personal;

- neîndeplinirea obligaţiilor privind confidenţialitatea şi aplicarea măsurilor de securitate;
- refuzul de a furniza informaţii.

Sancţiunile contravenţionale se aplică de către autoritatea de supraveghere prin personalul împuternicit în acest scop. Cuantumul amenzilor care pot fi aplicate, în cazul săvârşirii contravenţiilor sus – menţionate, variază între 500 RON şi 50.000 RON.

Împotriva proceselor-verbale de constatare şi a deciziilor de sancţionare se poate face plângere la secţiile de contencios administrativ ale tribunalelor.

6. Autoritatea Europeană pentru Protecţia Datelor

Autoritatea Europeană pentru Protecţia datelor s-a înfiinţat în anul 2001 şi s-a format în conformitate cu art. 286 alin.(2) din Tratatul de Instituire a Comunităţii Europene şi pentru a asigura aplicarea Regulamentului CE 45/2001, atât tratatul cât şi regulamentul urmăresc alinierea protecţiei datelor în instituţiile din Comunitatea europeană.

6.1. Structura Autorităţii Europene pentru Protecţia Datelor.

Conducerea AEPD este asigurată de către un preşedinte şi de un adjunct al preşedintelui , ambii fiind aleşi de comun acord de către Consiliul Uniunii Europene şi de Parlamentul European. Atât preşedintele cât şi adjunctul acestuia sunt numiţi pe o perioadă de 5 ani. În momentul de faţă preşedintele AEPD este Peter HUSTINX iar adjunctul său este Giovanni BUTTARELLI. În structura AEPD mai intră şi secretariatul, în cadrul căruia lucrează 30 de angajaţi.

6.2. Funcţiile Autorităţii Europene pentru Protecţia Datelor

Autoritatea Europeană pentru Protecţia Datelor are 3 funcţii importante:
A- de supraveghere
B- de consultare
C- de cooperare

A. Supravegherea

Una dintre principalele sarcini ale AEPD "este de a supraveghea prelucrarea datelor cu caracter personal de către instituţiile şi organismele europene". Această activitate de supraveghere ia forme diferite. Cea mai mare parte a acestei funcţii se bazează pe notificarea operaţiunilor de prelucrare care prezintă riscuri specifice. Acestea trebuie verificate înainte de AEPD, care va examina prelucrarea datelor cu caracter personal astfel încât acestea să fie în conformitate cu prevederile Regulamentului (CE) nr. 45/2001. În majoritatea cazurilor, acest exerciţiu duce la un set de recomandări pe care instituţia sau organismul trebuie să le pună în aplicare, astfel încât să asigure respectarea normelor de protecţie a datelor.

AEPD primeşte plângeri din partea membrilor personalului UE, precum şi de la alte persoane care simt că datele lor cu caracter personal au fost greşit folosite de către o instituţie sau organism european.

AEPD poate adopta avize privind măsurile administrative referitoare la protecţia datelor adoptate de către instituţiile şi organismele europene.

AEPD poate efectua anchete din proprie iniţiativă. Anchete şi inspecţii sunt esenţiale pentru autoritatea de supraveghere.

În scopul de a monitoriza conformitatea cu Regulamentul (CE) nr. 45/2001, AEPD în mare măsură se bazează pe responsabilii cu protecţia datelor (RPD) care urmează să fie numiţi în fiecare instituţie / organism. În afară de întâlnirilor bilaterale şi a contactelor cu RPD, AEPD ia, de asemenea, parte la reuniunile periodice ale reţelei RPD.

Din ianuarie 2004, AEPD a asigurat supravegherea unităţii centrale Eurodac. Un aspect esenţial al acestei supravegheri este cooperarea cu autorităţile naţionale de supraveghere, precum şi întocmirea de recomandări pentru soluţii comune la problemele existente.

AEPD publică orientări tematice privind probleme critice pentru a servi ca documente de referinţă pentru administraţia europeană.

B . Consultarea

AEPD dă sfaturi instituţiilor şi organismelor UE pe probleme de protecţie a datelor cu caracter personal într-o gamă de domenii politice. Rolul său consultativ se referă la propuneri legislative noi, precum şi la instrumente de legi uşoare, cum ar fi comunicaţiile, care afectează protecţia datelor personale în UE. AEPD

monitorizează, de asemenea, tehnologii noi care pot avea un impact asupra protecţiei datelor cu caracter personal. Obiectivul este de a asigura că drepturile fundamentale cetăţenilor UE mai ales protecţia vieţii private şi a datelor cu caracter personal sunt menţinute, în timp ce societatea evoluează.

Una din sarcinile principale ale AEPD este de a examina impactul protecţia datelor cu caracter personal şi a vieţii private în noua legislaţie propusă.

Primul instrument este un instrument de planificare. În fiecare an în decembrie, AEPD publică un inventar al priorităţilor sale pentru anul următor.

Aceasta enumeră cele mai relevante propuneri ale Comisiei, care poate necesita o reacţie formală din partea AEPD.

Al doilea şi cel mai important instrument este avizul oficial public. Prin emiterea de opinii în mod regulat, AEPD stabileşte o politică coerentă cu privire la aspectele de protecţie a datelor.

Un al treilea instrument de intervenţie sunt comentariile AEPD, care abordează aspecte legate de protecţia datelor, de exemplu, în comunicările Comisiei. Un instrument final este posibilitatea de a interveni în cazuri în faţa Curţii de Justiţie, Tribunalul de Primă Instanţă şi a Tribunalului Funcţiei Publice.

C. Cooperarea

A treia funcţie de bază a AEPD-ului reprezintă o colaborare structurată cu celelalte autorităţi de protecţie a datelor cu caracter personal. Forum central pentru cooperare în cadrul UE este Grupul de lucru privind articolul 29.Acesta este în cazul în care autorităţile naţionale de protecţie a datelor cu caracter personal se întâlnesc pentru a face schimb de opinii privind problemele actuale, pentru a discuta despre o interpretare comună a legislaţiei privind protecţia datelor şi pentru a oferi consultanţă Comisiei Europene.

AEPD participă, de asemenea, la activităţile care urmăresc asigurarea protecţiei datelor cu caracter personal în al treilea pilon al UE, care se referă la cooperarea poliţienească şi judiciară. Aceasta include participarea la o serie de reuniuni cu Organismele de Supraveghere Comune ale sistemelor de informare din treilea pilon. Ea este, de asemenea, un membru al grupului de lucru privind poliţia, instituit de către Conferinţa Europeană, cu scopul de a pregăti consultanţă în materie in cadrul celui de-al treilea pilon. În plus, AEPD a luat de asemenea parte la reuniunile Autorităţi de Supraveghere comune a Sistemului de Informaţii Schengen, care intră atât sub incidenţa pilonului unu cât şi sub incidenţa celui de al treilea.

Una dintre cele mai importante sarcini de cooperare se referă la Eurodac, în cazul în care responsabilităţile pentru supravegherea protecţiei datelor cu caracter personal sunt împărţite. Eurodac este un sistem IT de mari proporţii care cuprinde amprentele digitale ale solicitanţilor de azil. Se compune din unităţile naţionale (în funcţie de legislaţia naţională), şi o unitate centrală (reglementate de Regulamentul 45/2001). O abordare coordonată este esenţială, ţinând cont de faptul că supravegherea depinde de o colaborare între autorităţile naţionale pentru protecţia datelor cu caracter personal şi AEPD. De aceea, AEPD organizează întâlniri bianuale de coordonare.

Două mari conferinţe de protecţie a datelor cu caracter personal sunt organizate în fiecare an. În fiecare primăvară, o conferinţă europeană asamblează oficiali autorităţilor de protecţie a datelor cu caracter personal din statele membre ale UE şi Consiliul Europei. Şi în fiecare toamnă, o gamă largă de experţi în protecţia datelor, atât din sectorul public cât şi din sectorul privat, se reunesc pentru Conferinţa Internaţionale.