chapter 1 clasificarea datelor

1.1 termeni de bază

Datele publice (în contextul acestui curs) sunt acelea care afectează (definesc) statutul legal (din pdv al legii) al unei entități.

1.2 criterii de clasificare

Datele (publice) pot fi clasificate după utmătoarele criterii:

- domeniul (aria de acoperire)
- obiectul datelor (entitățile la care se referă)
- caracterul lor temporal
- modalitatea de generare
- accesul la aceste date

Să detaliem puţin aceste concepte.

1.3 domeniile acoperite în acest curs

Domeniile de interes și documentele aferente acestora pentru acest curs sunt următoarele:

- starea civilă
- proprietăți imbiliare
- proprietăți mobile
- amenzi
- taxe și impozite
- sistemul notarial
- tranzacții
- profile personal
- cazier fiscal
- cazier judiciar
- sistem de vot electronic
- sistem guvernamental de informare
- creare și administrare firme

1.4 conținutul datelor

Algoritmii

1.5 caracterul temporal al datelor

Utilizarea

1.6 modalitatea de generare

Modalitatea de generare a datelor

1.7 accesarea datelor

Din nou, modalitatea și drepturile de acces la datele publice și private este dependent de natura și conținutul acestor date. Pentru domeniile acoperiteîn acest curs, modalitățile de acces și permisiunile avute asupra datelor vor fi detaliate în capitolul asociat acestor date.

chapter 2 controlul accesului

2.1 principii

o

2.2 liste de control al accesului (ACLs)

Un caz tipic

2.3 accesul la informații clasificate în România

Informații preluate de pe site-ul http://www.orniss.ro/ro/proceduri.html

2.3.1 accesul la informații secrete de stat

În România, accesul la informaţii secrete de stat este permis, cu respectarea principiului necesităţii de a cunoaşte, numai persoanelor care deţin certificat de securitate sau autorizaţie de acces, valabile pentru nivelul de secretizare al informaţiilor necesare îndeplinirii atribuţiilor de serviciu.
În practica protecţiei informaţiilor clasificate se face distincţie între informaţiile naţionale clasificate şi informaţiile NATO clasificate. Pagina de faţă conţine referiri la modul de acordare a accesului la informaţiile naţionale clasificate.

Acordarea accesului la informaţii NATO clasificate este descrisă într-o pagină separată.

Pentru a asigura accesul personalului propriu la informaţii naţionale clasificate, fiecare autoritate sau instituţie publică emitentă sau deţinătoare de astfel de informaţii va întreprinde următoarele:

- întocmirea listei cuprinzând informaţiile secrete de stat şi aprobarea acesteia prin hotărâre a Guvernului;
- întocmirea listei funcţiilor care necesită acces la informaţii secrete de stat;
- verificarea şi autorizarea personalului desemnat să ocupe aceste funcţii.

Întocmirea listelor cu informaţii secrete de stat

Lista informaţiilor secrete de stat elaborate sau deţinute de instituţie se va întocmi în conformitate cu prevederile art. 17 din Legea nr. 182/2002, care stabileşte conţinutul informaţiilor cuprinse în această categorie. Nivelurile de secretizare ce se vor atribui informaţiilor respective se vor stabili conform împuternicirilor prevăzute la art. 19 al aceleiaşi legi.

Lista cuprinzând informaţiile secrete de stat, pe niveluri de secretizare, se aprobă prin hotărâre a Guvernului. Tot prin hotărâre a Guvernului se aprobă orice actualizare ulterioară a acestei liste.
Pentru realizarea unei clasificări corecte şi unitare a informaţiilor secrete de stat, fiecare instituţie care elaborează sau lucrează cu astfel de informaţii va întocmi un ghid de clasificare.

La întocmirea listei funcţiilor ce necesită acces la informaţii secrete de stat, conducătorul instituţiei va

avea în vedere persoanele care încadrează structura de securitate (cărora urmează a li se elibera certificate de securitate), angajaţii care, în virtutea atribuţiilor de serviciu, vor lucra cu informaţii secrete de stat (cărora li se vor elibera autorizaţii de acces la informaţii clasificate), precum şi personalul administrativ care poate avea, tangenţial, acces la informaţii clasificate (tot în baza autorizaţiilor de acces). În listă se va menţiona nivelul de secretizare al informaţiilor la care urmează a avea acces fiecare dintre angajaţi.

Lista informaţiilor clasificate (după aprobarea prin HG) şi lista funcţiilor ce necesită acces la informaţii clasificate (aprobată de conducătorul instituţiei) vor fi comunicate la ORNISS şi la instituţiile cărora le revin sarcini de organizare a măsurilor specializate de protecţia a informaţiilor clasificate.

Verificarea personalului

Certificatul de securitate (HG nr. 585/2002, Anexa nr. 12) sau autorizaţia de acces la informaţii clasificate (HG nr. 585/2002, Anexa nr. 13) se eliberează numai în baza avizelor acordate de autoritatea desemnată de securitate (ADS) în urma verificărilor efectuate asupra persoanei în cauză, cu acordul scris al acesteia. Persoana pentru care se solicită acordarea accesului la informaţii secrete de stat îşi exprimă acordul privind efectuarea acestor verificări printr-o declaraţie scrisă, dată în prezenţa funcţionarului de securitate odată cu predarea formularului tip completat corespunzător nivelului de clasificare a informaţiilor respective (HG nr. 585/2002, anexele nr.15-17).

Acordarea certificatului de securitate sau a autorizaţiei de acces la informaţii clasificate, potrivit nivelului de secretizare, este condiţionată de avizul autorităţii desemnate de securitate şi de decizia ORNISS, comunicată instituţiei solicitante.

In vederea eliberării certificatelor de securitate/autorizaţiilor de acces conducătorul unităţii solicită ORNISS în scris (HG nr. 585/2002, Anexa nr. 14) efectuarea verificărilor de securitate asupra persoanelor care urmează să aibă acces la informaţii secrete de stat.

Solicitările privind efectuarea verificărilor de securitate în vederea avizării eliberării certificatelor de securitate/autorizaţiilor de acces la informaţii secrete de stat se vor face în funcţie de nivelul de secretizare al informaţiilor la care persoanele urmează să obţină acces în virtutea sarcinilor de serviciu. Categoriile de persoane, în funcţie de nivelul de secretizare al informaţiilor, sunt prezentate în continuare.

1. Pentru asigurarea accesului la informaţii clasificate SECRET vor fi avute în vedere persoane care:

- în exercitarea atribuţiilor profesionale lucrează cu date şi informaţii de nivel secret;
- fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intra în contact cu date şi informaţii de acest nivel;
- este de presupus că vor lucra cu date şi informaţii de nivel secret, datorită funcţiei pe care o deţin;
- se presupune că nu pot avansa profesional în funcţie, dacă nu au acces la astfel de informaţii.

2. Pentru eliberarea certificatelor de securitate/autorizaţiilor de acces la informaţii clasificate STRICT SECRET se efectuează verificări asupra persoanelor care:

- în exercitarea atribuţiilor profesionale lucrează cu date şi informaţii de nivel strict secret;
- fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intra în contact cu date şi informaţii de acest nivel;
- este de presupus că vor lucra cu date şi informaţii de nivel strict secret, datorită funcţiei pe care o deţin;
- se presupune că nu pot avansa profesional în funcţie, dacă nu au acces la astfel de informaţii.

3. Pentru eliberarea certificatelor de securitate/autorizaţiilor de acces la informaţii clasificate STRICT SECRETE DE IMPORTANŢĂ DEOSEBITĂ se efectuează verificări asupra persoanelor care:

- în exercitarea atribuţiilor profesionale lucrează cu date şi informaţii de nivel strict secret de

importanţă deosebită;

- fac parte din personalul de execuţie sau administrativ şi, în virtutea acestui fapt, pot intra în contact cu informaţii de acest nivel.Solicitarea iniţierii procedurilor de verificare în vederea eliberării certificatului de securitate/autorizaţiei de acces la informaţii secrete de stat va fi însoţită de formularele tip (HG nr. 585/2002, anexele nr.15-17) potrivit nivelului de secretizare al informaţiilor, completate de persoana în cauză, introduse în plic separat, sigilat.
  Structura/funcţionarul de securitate are obligaţia să pună la dispoziţia persoanei selecţionate formularele tip corespunzătoare nivelului de acces pentru care se solicită eliberarea certificatului de securitate/autorizaţiei de acces şi să acorde asistenţă în vederea completării acestora.

La primirea solicitării, ORNISS are obligaţia de a transmite, în termen de 7 zile lucrătoare, ADS competente cererea tip de începere a procedurii de verificare (HG nr. 585/2002, Anexa nr. 19), la care va anexa plicul sigilat cu formularele tip completate.
După primirea formularelor, instituţia abilitată va efectua verificările în termenele prevăzute de lege.
In funcţie de nivelul de secretizare a informaţiilor pentru care se solicită avizul de securitate, termenele de prezentare a răspunsului de către instituţiile abilitate să efectueze verificările de securitate sunt:

- pentru acces la informaţii strict secrete de importanţă deosebită - 90 de zile lucrătoare;
- pentru acces la informaţii strict secrete - 60 de zile lucrătoare;
- pentru acces la informaţii secrete - 30 de zile lucrătoare.

Dacă în cursul verificărilor, pentru orice nivel, apar informaţii ce evidenţiază riscuri de securitate, se va realiza o verificare suplimentară, cu folosirea metodelor şi mijloacelor specifice instituţiilor cu atribuţii în domeniul siguranţei naţionale.

În cazul verificării suplimentare menţionate mai sus, termenele de efectuare a verificărilor vor fi prelungite în mod corespunzător.

În cazul în care sunt identificate riscuri de securitate, ADS va evalua dacă acestea constituie un impediment pentru acordarea avizului de securitate.

In situaţia în care sunt semnalate elemente relevante din punct de vedere al protecţiei informaţiilor secrete de stat, în luarea deciziei de acordare a avizului de securitate vor avea prioritate interesele de securitate.

Procedura de verificare în vederea acordării accesului la informaţii secrete de stat are drept scop identificarea riscurilor de securitate relevante pentru activitatea de gestionare a informaţiilor secrete de stat.

In cadrul procedurilor de avizare se acordă atenţie specială persoanelor care:

- urmează să aibă acces la informaţii strict secrete şi strict secrete de importanţă deosebită;
- ocupă funcţii ce presupun accesul permanent la un volum mare de informaţii secrete de stat;
- pot fi vulnerabile la acţiuni ostile, ca urmare a importantei funcţiei în care vor fi numite, a mediului de relaţii sau a locului de muncă anterior.

Oportunitatea avizării va fi evaluată pe baza verificării şi investigării biografiei celui în cauză.

Principalele criterii de evaluare a compatibilităţii în acordarea avizului pentru eliberarea certificatului de securitate/autorizaţiei de acces vizează atât trăsăturile de caracter, cat şi situaţiile sau împrejurările din care pot rezulta riscuri şi vulnerabilităţi de securitate.

Sunt relevante şi vor fi luate în considerare, la acordarea avizului de securitate, caracterul, conduita profesională sau socială, concepţiile şi mediul de viaţă al soţului/soţiei sau concubinului/concubinei persoanei solicitante.

Următoarele situaţii imputabile atât solicitantului cât şi soţului/soţiei sau concubinului/concubinei

reprezintă elemente de incompatibilitate pentru acces la informaţii secrete de stat:

- dacă a comis sau a intenţionat să comită, a fost complice, a complotat sau a instigat la comiterea de acte de spionaj, terorism, trădare ori alte infracţiuni contra siguranţei statului;
- dacă a încercat, a susţinut, a participat, a cooperat sau a sprijinit acţiuni de spionaj, terorism ori persoane suspectate de a se încadra în această categorie sau de a fi membre ale unor organizaţii ori puteri străine inamice ordinii de drept din ţara noastră;
- dacă este sau a fost membru al unei organizaţii care a încercat, încearcă sau susţine răsturnarea ordinii constituţionale prin mijloace violente, subversive sau alte forme ilegale;
- dacă este sau a fost un susţinător al vreunei organizaţii prevăzute la lit. c), este sau a fost în relaţii apropiate cu membri ai unor astfel de organizaţii într-o formă de natură să ridice suspiciuni temeinice cu privire la încrederea şi loialitatea persoanei.

Constituie elemente de incompatibilitate pentru accesul solicitantului la informaţii secrete de stat oricare din următoarele situaţii:

- dacă în mod deliberat a ascuns, a interpretat eronat sau a falsificat informaţii cu relevanţă în planul siguranţei naţionale ori a minţit în completarea formularelor tip sau în cursul interviului de securitate;
- are antecedente penale sau a fost sancţionat contravenţional pentru fapte care indică tendinţe infracţionale;
- are dificultăţi financiare serioase sau există o discordanţă semnificativă între nivelul sau de trai şi veniturile declarate;
- consumă în mod excesiv băuturi alcoolice ori este dependent de alcool, droguri sau de alte substanţe interzise prin lege care produc dependenţă;
- are sau a avut comportamente imorale sau deviaţii de comportament care pot genera riscul ca persoana să fie vulnerabilă la şantaj sau presiuni;
- a demonstrat lipsă de loialitate, necinste, incorectitudine sau indiscreţie;
- a încălcat reglementările privind protecţia informaţiilor clasificate;
- suferă sau a suferit de boli fizice sau psihice care îi pot cauza deficienţe de discernământ confirmate prin investigaţie medicală efectuată cu acordul persoanei solicitante;
- poate fi supus la presiuni din partea rudelor sau persoanelor apropiate care ar putea genera vulnerabilităţi exploatabile de către serviciile de informaţii ale căror interese sunt ostile României şi aliaţilor săi.

După efectuarea verificărilor, în termenele menţionate mai sus, ADS va comunica, în scris (HG nr. 585/2002, Anexa nr. 20) la ORNISS, avizul privind acordarea certificatului de securitate/autorizaţiei de acces la informaţii clasificate.

In termen de 7 zile lucrătoare de la primirea răspunsului de la autoritatea desemnată de securitate, ORNISS va decide asupra acordării certificatului de securitate/autorizaţiei de acces la informaţii secrete de stat şi va comunica acest fapt unităţii solicitante (HG nr. 585/2002, Anexa nr. 21).

Decizia privind avizarea eliberării certificatului de securitate/autorizaţiei de acces va fi luată pe baza tuturor informaţiilor disponibile şi va avea în vedere:

- loialitatea indiscutabilă a persoanei;
- caracterul, obiceiurile, relaţiile şi discreţia persoanei, care să ofere garanţii asupra:
  - corectitudinii în gestionarea informaţiilor secrete de stat;
  - oportunităţii accesului neînsoţit în compartimente, obiective, zone şi locuri de securitate în care se află informaţii secrete de stat;
  - respectării reglementarilor privind protecţia informaţiilor secrete de stat din domeniul său de

activitate.

Adresa de comunicare a deciziei ORNISS se realizează în trei exemplare, din care unul se transmite unităţii solicitante, iar al doilea instituţiei care a efectuat verificările.

Acordarea accesului la informaţii secrete de stat

Dacă avizul este pozitiv, conducătorul unităţii solicitante va elibera certificatul de securitate sau autorizaţia de acces persoanei în cauză, după notificarea prealabila la ORNISS (HG nr. 585/2002, Anexa nr. 22).

Conducătorul unităţii va notifica la ORNISS eliberarea certificatului de securitate sau autorizaţiei de acces pentru fiecare angajat care lucrează cu informaţii clasificate.

Certificatul de securitate/autorizaţia de acces se emite în două exemplare originale, unul fiind păstrat de structura/funcţionarul de securitate, iar celălalt trimis la ORNISS, care va informa instituţia competentă care a efectuat verificările.

Persoanele cărora le-au fost eliberate certificate de securitate sau autorizaţii de acces vor fi instruite, atât la acordarea acestora cât şi periodic, cu privire la conţinutul reglementarilor privind protecţia informaţiilor clasificate. Instruirea va fi efectuată de către structura/funcţionarul de securitate.

Activităţile de instruire vor fi consemnate de structura/funcţionarul de securitate, sub semnătură, în fişa de pregătire individuală (HG nr. 585/2002, Anexa nr. 2).

Fiecare persoană căreia i s-a eliberat certificat de securitate/autorizaţie de acces va semna un angajament de confidenţialitate (HG nr. 585/2002, Anexa nr. 3).

Structura/funcţionarul de securitate din instituţia care gestionează informaţii secrete de stat asigură păstrarea şi organizează evidenţa, pe care o actualizează permanent, a certificatelor de securitate şi autorizaţiilor de acces la informaţii clasificate (HG nr. 585/2002, Anexa nr. 18).

Conducătorul unităţii aprobă listele cu personalul verificat şi avizat pentru lucrul cu informaţiile secrete de stat şi evidenţa deţinătorilor de certificate de securitate şi autorizaţii de acces, pe care le comunică la ORNISS şi la instituţiile abilitate să coordoneze activitatea şi controlul masurilor privitoare la protecţia informaţiilor clasificate, potrivit legii.

Valabilitatea certificatului de securitate/autorizaţiei de acces eliberate unei persoane este de până la patru ani, în această perioadă verificările putând fi reluate oricând, în situaţii care impun revalidarea avizului privind accesul la informaţii secrete de stat.

Revalidarea avizului privind accesul la informaţii clasificate presupune reverificarea persoanei deţinătoare a unui certificat de securitate/autorizaţie de acces în vederea menţinerii sau retragerii acestuia/acesteia.

Revalidarea poate avea loc la solicitarea unităţii în care persoana îşi desfăşoară activitatea, sau a ORNISS, în oricare din următoarele situaţii:

- atunci când pentru îndeplinirea sarcinilor de serviciu ale persoanei deţinătoare este necesar accesul la informaţii de nivel superior;
- la expirarea perioadei de valabilitate a certificatului de securitate/autorizaţiei de acces deţinute anterior;
- în cazul în care apar modificări în datele de identificare ale persoanei;
- la apariţia unor riscuri de securitate din punct de vedere al compatibilităţii accesului la informaţii clasificate.

La solicitarea revalidării nu se eliberează un nou certificat de securitate/autorizaţie de acces, în următoarele situaţii:

- în cazul în care se constată neconcordanţe între datele declarate în formularele tip şi cele reale;

- în cazul în care, pe parcursul perioadei de valabilitate a certificatului de securitate/autorizaţiei de acces s-au evidenţiat riscuri de securitate;
- în cazul în care ORNISS solicită acest lucru, în mod expres.

Pentru revalidarea accesului la informaţii secrete de stat se derulează aceleaşi activităţi ca şi la acordarea avizului iniţial, verificările raportându-se la perioada scursă de la eliberarea certificatului de securitate sau a autorizaţiei de acces anterioare.

Certificatul de securitate sau autorizaţia de acces îşi încetează valabilitatea şi se va retrage în următoarele cazuri:

- la solicitarea ORNISS;
- prin decizia conducătorului unităţii care a eliberat certificatul/autorizaţia;
- la solicitarea autorităţii desemnate de securitate competente;
- la plecarea din unitate sau la schimbarea locului de muncă al deţinătorului în cadrul unităţii, dacă noul loc de muncă nu presupune lucrul cu astfel de informaţii secrete de stat;
- la schimbarea nivelului de acces.

La retragerea certificatului de securitate/autorizaţiei de acces, în cazurile prevăzute mai sus la literele a-d, angajatului i se va interzice accesul la informaţii secrete de stat, iar conducerea unităţii va notifica despre aceasta la ORNISS.

După luarea deciziei de retragere, unitatea va solicita ORNISS înapoierea exemplarului 2 al certificatului de securitate/autorizaţiei de acces, după care va distruge ambele exemplare, pe bază de proces-verbal.

Accesul temporar la informaţii secrete de stat

În cazuri excepţionale, determinate de situaţii de criză, calamităţi sau evenimente imprevizibile, conducătorul unităţii poate acorda acces temporar la informaţii clasificate anumitor persoane care nu deţin certificat de securitate sau autorizaţie de acces, cu condiţia asigurării unui sistem corespunzător de evidenţă.

Persoanele care primesc dreptul de acces temporar la informaţii secrete de stat vor semna angajamentul de confidenţialitate şi vor fi comunicate la ORNISS, în cel mai scurt timp posibil, pentru efectuarea verificărilor de securitate, potrivit procedurilor.

În cazul informaţiilor strict secrete de importanţă deosebită, accesul temporar va fi acordat, pe cât posibil, persoanelor care deţin deja certificate de securitate pentru acces la informaţii strict secrete sau secrete.

Accesul cetăţenilor străini la informaţii secrete de stat în România

Cetăţenii străini, cetăţenii români care au şi cetăţenia altui stat, precum şi persoanele apatride pot avea acces la informaţii secrete de stat, cu respectarea principiului necesităţii de a cunoaşte şi a convenţiilor, protocoalelor, contractelor şi altor înţelegeri încheiate în condiţiile legii.

Persoanele din categoriile prevăzute mai sus vor fi verificate şi avizate conform standardelor stabilite de HG nr. 585/2002, la solicitarea conducătorului unităţii în cadrul căreia acestea urmează să desfăşoare activităţi care presupun accesul la informaţii secrete de stat.

Conducătorul unităţii va elibera persoanelor respective o autorizaţie de acces corespunzătoare nivelului de secretizare a informaţiilor la care urmează să aibă acces, valabila numai pentru perioada desfăşurării activităţilor comune, în baza acordului comunicat de ORNISS.

Persoanele din categoriile prevăzute mai sus care desfăşoară activităţi de asistenţă tehnică, consultanţă, colaborare ştiinţifică ori specializare vor purta ecusoane distincte faţă de cele folosite de personalul propriu şi vor fi însoţite permanent de persoane anume desemnate de conducerea unităţii respective.

Conducătorul unităţii este obligat să delimiteze strict sectoarele şi compartimentele în care persoanele respective pot avea acces şi va stabili măsuri pentru prevenirea prezenţei acestora în alte locuri în care se gestionează informaţii secrete de stat.

2.3.2 accesul la informații secrete de serviciu

Accesul personalului la informaţiile secrete de serviciu este permis numai în baza autorizaţiei scrise emise de conducătorul unităţii (HG nr. 781/2002, Anexa nr. 2).
Evidenţa autorizaţiilor de acces la informaţii secrete de serviciu se ţine centralizat de structura/funcţionarul de securitate în Registrul pentru evidenţa autorizaţiilor de acces la informaţii secrete de serviciu (HG nr. 781/2002, Anexa nr. 3).

În vederea eliberării autorizaţiei de acces la informaţii secrete de serviciu, persoana care urmează să ocupe o funcţie ce presupune accesul la astfel de informaţii prezintă structurii/funcţionarului de securitate, în condiţiile legii, recomandări şi referinţe asupra onestităţii şi profesionalismului, din partea persoanelor cu funcţii de conducere cărora li se subordonează direct sau a reprezentanţilor autorizaţi ai altor persoane juridice, după caz, şi va semna un angajament de confidenţialitate.

După ce verifică autenticitatea documentelor menţionate mai sus, structura/funcţionarul de securitate prezintă conducătorului unităţii propuneri privind oportunitatea eliberării autorizaţiei de acces la informaţiile secrete de serviciu.

Retragerea autorizaţiei de acces la informaţii secrete de serviciu se face de către conducătorul unităţii deţinătoare, în următoarele cazuri:

- la încetarea raporturilor de muncă ori de serviciu, după caz, dintre unitate şi deţinătorul autorizaţiei sau a calităţii de demnitate publică;
- când atribuţiile specifice postului pe care este încadrat deţinătorul autorizaţiei nu mai presupun accesul la astfel de informaţii;
- când deţinătorul autorizaţiei a încălcat reglementările privind protecţia informaţiilor secrete de serviciu.

După retragerea autorizaţiei de acces la informaţii secrete de serviciu, structura/funcţionarul de securitate procedează la distrugerea acesteia, pe bază de proces-verbal.

Accesul cetăţenilor străini, al cetăţenilor români care au şi cetăţenia altui stat, precum şi al persoanelor apatride la informaţii secrete de serviciu este permis în condiţiile stabilite prin Standardele naţionale de protecţie a informatiilor clasificate în România (HG nr. 585/2002), pe baza autorizaţiei speciale de acces.

Prezentul material a fost întocmit în baza prevederilor următoarelor acte normative:

- Legea nr. 182/12.04.2002 privind protecţia informaţiilor clasificate, publicată în Monitorul Oficial al României, Partea I, nr. 248 din 12.04.2002;
- Hotărârea guvernului nr. 781/25.07.2002 privind protecţia informaţiilor secrete de serviciu, publicată în Monitorul Oficial al României, Partea I, nr. 575 din 05.08.2002;
- Hotărârea guvernului nr. 585/13.06.2002 PENTRU APROBAREA Standardelor naţionale de protecţia a informaţiilor clasificate în România, publicată în Monitorul Oficial al României, Partea I, nr. 485 din 05.07.2002;
- Ordonanţa de urgenţă a Guvernului nr. 153/07.11.2002, publicată în Monitorul Oficial al României, Partea I, nr. 826 din 15.11.2002, aprobată prin Legea nr. 101/24.03.2003, publicată în Monitorul Oficial al României, Partea I, nr. 207 din 31.03.2003.

2.4 p

MD5 este

2.5 a

Începem cu

chapter 3 domenii acoperite

3.1 documente de stare civilă

Un c

3.2 proprietăți imobiliare

Un caz tipic

3.3 proprietăți mobile

MD5 este

3.4 amenzi

Începem cu

3.5 taxe și impozite

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

3.6 sistem notarial

În 1993, Den Boer

3.7 tranzacții

MD5 este

3.8 profil personal

Începem cu

3.9 cazier fiscal

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

3.10 cazier judiciar

În 1993, Den Boer

3.11 sistem de vot electronic

MD5 este

3.12 sistem guvernamental de informare

Începem cu

3.13 creare și administrare firme

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 4 actele de stare civilă și de identitate

Actele de stare civilă sunt înscrisuri autentice prin care se dovedește nașterea, căsătoria sau decesul unei persoane.

Documentele de stare civilă sunt

- certifcatul de naștere
- certificatul căsătorie
- certificatul de divorț
- certificatul de deces.

Primul și ultimul sunt obligatorii (ca borne ale vieții unei persoane). Celelalte două sunt opționale.

4.1 cadrul legislativ intern

Cadrul legislativ este definit prin Legea nr 119 din 16.10.1996 cu privire la actele de stare civilă – http://www.cdep.ro/pls/legis/legis_pck.htp_act?ida=8658.

Legea a fost modificată și republicată în mai multe rânduri, lista acestor modificări poate fi consultată la link-ul de mai sus.

Actul de identitate este documentul care se eliberează cetățeanului român și care face dovada identității, a adresei de domiciliu și, după caz, a adresei de reședință titularului acestuia. Acest document se eliberează începând cu vârsta de 14 ani.

4.2 cum funcționează la noi

Actele se întocmesc în registrele de stare civilă, în doua exemplare, ambele originale și se completeaza manual.

Întocmirea actului de naștere se face la autoritatea administrației publice locale în a cărei rază administrativ-terirorială s-a produs evenimentul, pe baza actului de identitate al mamei și al declarantului, a cerificatului medical constator al nasterii și, după caz, a certificatului de căsătorie al părinților.

Întocmirea actului de căsătorie se realizează de către ofițerul de stare civilă, la sediul autorității publice locale a municipiului, orașului sau comunei în a cărei rază administrativ-teritorială își are domiciliul sau reședința unul dintre viitorii soți. Aceștia trebuie să prezinte actele de identitate, certificatele de naștere, certificatele medicale privind starea sănătății acestora.

Întocmirea actului de deces se face la autoritatea administrației publice locale în a cărei rază administrativ-teritorială s-a produs decesul, pe baza declarației verbale făcute de către membrii familiei decedatului, iar în lipsa acestora, de către colocatari, vecini etc.

Întocmirea actelor de stare civilă privind pe cetățenii români aflați în străinătate se face la misiunile diplomatice, la oficiile consulare de carieră ale României sau la autoritățile locale competente.

4.3 cum funcționează în alte țări

FRANTA

Conform Codul civil francez, sunt cinci acte de stare civilă: actul de naștere , actul de căsătorie, actul de deces, actul de recunoaștere și actul copilului născut mort.

În mod frecvent, înregistrarea are forma unei mențiuni pe marginea înregistrărilor existente, în special, a înregistrării nașterii. Registrele în care sunt păstrate actele de naștere sunt registre centrale și joacă un rol major în garantarea stabilității, exactității și publicității stării civile.

În principiu, la fel ca în sistemul român de drept, terțele persoanele nu au acces la registrele de stare civilă și nici să obțină copii după acestea.

Inregistrarea nasterii

Codul civil francez prevede că nașterea trebuie declarată ofițerului de stare civilă în termen de 5 zile. Aceste termen începe să curgă din ziua nașterii.

Actul de naștere trebuie redactat imediat după momentul declarației. Pe baza actului de naștere se eliberează certificatul de naștere, care trebuie să indice ziua, ora, locul nașterii, sexul copilului, prenumele, numele copilului, precum și prenumele, numele, vârsta, profesia și adresa fiecărui părinte.

Inregistrarea casatoriei

În Franța, la fel ca și în România, căsătoria civilă nu exclude căsătoria religioasă. Dimpotrivă, căsătoria civilă este o condiție prealabilă și obligatorie pentru celebrarea căsătoriei religioase. Celebrarea căsătoriei are loc în localitatea în care se află domiciliul unuia sau a ambilor soți. Viitorii soți au obligația de a participa nemijlocit, unul în prezența celuilalt, la încheierea actului juridic al căsătoriei și să îndeplinească cerințele stabilite de lege.

Căsătoria celebrată de o autoritate franceză este înregistrată în registrul de căsătorie. Căsătoria este, de asemenea, menționată pe marginea actului de naștere al fiecărui soț, indicându-se numele celuilalt soț. Actul de căsătorie trebuie să fie întocmit imediat după ceremonia civilă și să fie semnat de soți, martori și de ofițerul de stare civilă.

Inregistrarea decesului

Codul civil francez nu impune, în mod direct, cel puțin în principiu, obligația de a declara decesul, care este în mod normal constatat de un medic desemnat de primar.

4.4 cum am vrea să funcționeze

MD5 este

4.5 structuri de date

Începem cu

4.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

4.7 cazuri de utilizare

În 1993, Den Boer

4.8 implementare software

MD5 este

4.9 implementare în viața reală

Începem cu

4.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 5 proprietăți imobiliare

5.1 cadrul legislativ intern

O **funcție criptografică de hash** este

5.2 cum funcționează la noi

Un caz tipic

5.3 cum funcționează în alte țări

Un caz tipic

5.4 cum am vrea să funcționeze

MD5 este

5.5 structuri de date

Începem cu

5.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

5.7 cazuri de utilizare

În 1993, Den Boer

5.8 implementare software

MD5 este

5.9 implementare în viața reală

Începem cu

5.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 6 proprietăți mobile

6.1 cadrul legislativ intern

Indiferent de unde cumpărați un autovehicul, acesta va trebui să fie înregistrat la RAR în județul în care locuiți. Exista mici excepții când autovehiculul circula cu numere provizorii (intre una si trei luni), în acest caz mașina este pe adresa vechiului proprietar, noului proprietar sau a reprezentanței de unde a fost cumpărata.

6.2 cum funcționează la noi

În momentul de față, la noi în țară sunt foarte mulți pași de urmat și multe acte atunci când vine vorba de înmatricularea unui autovehicul. Asta nu ar fi o cea mai pare problemă. Problema este durata înmatriculării unui autovehicul (chiar dacă este unui nou sau unul care deja există în circulație, durează destul de mult timp până să se rezolve toate lucrurile).

Toate informațiile necesare înmatriculării (indiferent de categoria unde se încadrează) se găsesc pe site-ul oficial DRPCIV.

6.3 cum funcționează în alte țări

Chiar și în alte țări există o serie de pași ce trebuie urmați atunci când vine vorba de înmatricularea unui autovehicul și gestionarea acestora la nivel intern.

6.4 cum am vrea să funcționeze

Sunt mai multe cazuri de utilizare pentru aceasta aplicație:

- autoturism nou din Romania: viitorul proprietar are nevoie de un cont în aplicație (pe baza de buletin) unde va încarcă toate actele mașinii pentru verificare, va introduce ce numere dorește și metoda prin care vrea să intre in posesia lor (fiind un autoturism nou, nu necesita foarte multe verificări);

- autoturism nou din străinătate: se încadrează în aceleași condiții;

- vânzarea unui autoturism: se va face o cerere online iar apoi se vor completa toate datele necesare;

Și altele în funcție de toate tipurile de înmatriculări disponibile;

6.5 structuri de date

Toate informațiile despre autovehiculele înmatriculate in Romania ar trebui stocate într-o baza de date iar aplicația care folosește datele sa limiteze accesul la ele in funcție de tipul de utilizator și de scopul aplicației in sine.

Datele ce urmează a fi prelucrate prin intermediul aplicației sunt:

- date personale ale proprietarilor de autovehicule;

- datele autovehiculelor înregistrate;

- istoricul autovehiculelor;

6.6 controlul accesului

Accesul in aplicație ar trebui sa fie pe mai multe nivele:

- vizitator (doar poate citi informații și verifica starea unui autovehicul pe baza serie de șasiu);

- proprietar (poate vedea tot de ce întâmpla cu autovehiculele înregistrate pe numele său și poate face rezervări sau depune cereri direct din aplicație în funcție de nevoile acestuia);

- operator service auto (care are obligația de a actualiza datele autovehiculului pe baza lucrărilor efectuate);

- operator RAR (care are obligația de a actualiza datele autovehiculul în funcție de starea acestuia);

- administrator general (care are obligația de a menține aplicația într-o stare perfecta de funcționare si de a aduce îmbunătățiri in interesul tuturor);

Conectarea în aplicație făcându-se pe baza de CNP, parola utilizator și confirmare prin SMS.

6.7 cazuri de utilizare

Cazurile de utilizare sunt:

- punerea in circulație a unui autovehicul nou;

- vânzarea unui autovehicul + schimbarea proprietarului;

- vizualizarea istoricului unui autovehicul;

- eliminarea fraudei in ceea ce privește mașinile lovite și kilometraj modificat;

6.8 implementare software

Cea mai simpla implementare software poate fi o aplicație de tip Web cu o baza de date. Aplicația poate extrage informații din baza de date curenta sau din alte baze de date externe.

Mai târziu se poate crea un API care permite dezvoltarea aplicațiilor pe mobil.

6.9 implementare în viața reală

Pentru o bună implementare în viața reală avem nevoie de următoarele lucruri:

- un program software bine pus la punct și de o echipă de programatori care să se ocupe de mentenanța aplicației;

- documente bine explicate despre modul în care se utilizează aplicația;

- oamenii de la RAR si de la servisele auto trebuie învățați sa folosească noul sistem;

- toți pașii necesari (pentru înmatriculare, vânzare, etc...) ar trebui simplificați pentru a putea fi integrați cu succes in aplicație;

Implementarea acestui sistem in viată reala poate dura intre câteva luni și câțiva ani.

6.10 sugestii legislative

Adăugarea unor legi atât în interesul proprietarilor cât și în interesul statului pentru a evita orice tip de fraudă posibil prin utilizarea unui sistem informatic în domeniul auto. Iar pentru cei ce încearcă să evite sistemul sau nu își respectă îndatoririle, să fie pedepsiți conform legii in vigoare.

chapter 7 amenzi

7.1 cadrul legislativ intern

Legislația din Romania nu permite momentan afisarea sau transmiterea anumitor date cu character personal in mediul virtual. Din diferite motive se considera înca faptul că cea mai sigura metodă de pastrare si prelucrare ale acestor date sensibile este prin intermediu hârtiei.

În momentul de față există diferite metode prin care transferul de informații cu character personal poate circula in siguranță și cu viteză acceptată de zilele modern în care trăim. Este mult mai sigur să ținem datele pe servăre în camera securizate in diferite parti ala țării, astfel putem accesa oriunde și oricând anumite informații care necesită deplasare si asteptare la cozi interminabile.

Dacă discutăm concret despre amenzi putem observa că ar fi imperios un sistem online care să gestioneze non-stop cerința cetățenilor care doresc să afle informații utile. În momentul de față dacă primești o amendă mai ales rutieră există șansa sa afli de ea la un interval de 3-5 luni în poștă. Clar nu este o metoda modern și nici una fezabilă.

7.2 cum funcționează la noi

Dacă primești o amendă din cauză că nu ai taxa de drum platită o sa afli de aceasta peste 3-5 luni de la poștasul care v-a lasa o citație in poșta ta. În urma citației ai la dispozitie o anumita perioadă de timp pentru o a plati la un ghișeu fizic la care trebuie sa te deplasezi într-un interval de timp stabilit si unde trebuie să astepți la o posibilă coadă interminabilă.

Tot acest process interminabil care îți v-a rapi ore bune din timpul tau poate fi înlocuit de o platformă online unde orice cetățean poate să verifice dacă pe numele sau s-a inregistrat vre-o amendă.

7.3 cum funcționează în alte țări

În multe țări acest proces este similar cu cel din țara noastra, adică primești o citație la adresa din buletin, iar apoi începe acel process complex care îti consumă timp și îți pune rabdarea la încercare.

Însă, în unele țări straine cum ar fi Italia și Qatar poți accesa aceste date prin intermediul platformelor online sigur și rapid fără ați perde timp. Sunt dezvoltate platforme complexe unde poti vdea informațiile dorite și unde poti apela la plata online care este securizată și rapidă, fără a sta la cozi interminabile.

7.4 cum am vrea să funcționeze

Soluția potrivită pentru necesitatea noastra este o aplicație web care să fie conectată la o bază de date care să se afle într-un loc bine securizat. Datele cu character personal care vor circula prin intermediul aplicației vor fi criptate spre exemplu printr-o metodă de criptare comună MD5.

MD5 care este acronim de la Message Digest Algorithm 5 este este o funcție hash criptografică care primeste un input si produce o valoare de hash de 128-biti pe care o tipareste în mod tipic ca un numar hexazecimal de 32 de caractere.

Aceste hash-uri pot fi sparte rapid cu metode de tip brute force. Multe din datele transmise sunt informații generale la care pot avea acces indivizi rau intentionați care vor sa afle anumite informații despre o terță. Spre exemplu daca stii numele de familie si prenumele poți cu usurință sa folosești un algoritm care sa genere toate posibilițile până când gasește un hash similar cu cel găsit în system.

Solutia acestei probleme se poate rezolva prin utilizarea unor noi algiritmi de hash-ing mult mai solizi: Sha-256 si Sha-512.

7.5 structuri de date

La creearea aplicației s-a folosit o bază de data complexă care înregistrează în primă fază contul utilizatorului cu datele aferente, iar după îi pune la dispoziție amenzile, respectiv datele atribuite numelui și CNP-ului său.

Ca tot acest process să funcționeze rapid fără al pune pe utilazor să astepte un interval de timp ridicat din cauza unei baze de date mega incarcată cu date din toată țara se folosește cautare pe arbori care furnizează un raspuns rapid si satisfacator.

7.6 controlul accesului

Controlul accesului în aplicația online se va face prin intermediul unui cont de tip utilizator de bază pe care orice cetățean roman și îl poate creea. Pentru a putea creea un astfel de cont este nevoie ca utilizatorul să își introducă date cu character personal cum ar fi:

- CNP
- Serie
- Nr.
- Dată eliberare CI
- Adresă
- Prenume părinți

Astfel putem fi siguri ca acea persoana este validă din punct de vedere al identității și îi putem oferi accesul la platforma online de Amenzi. Pentru o protecție și mai sporită a identității cetațeanului se poate inregistra și cu IP-urile de pe care v-a accesa aplicația online, adrese IP care sunt atribuie prin contract de provideri de telefonie si internet, pe numele sau.

7.7 cazuri de utilizare

Aplicația poate fi accesată de oriunde, cât timp ai o conexiune la internet și dispui de un cont valid. Dacă dorești sa verifici dacă s-a inregistrat vre-o amendă pe numele tau o poți face ușor și rapid prin intermediul aplicației online, astfel ești scutit de eventualele neplaceri create de modelul classic existent la noi.

Practic aplicația noastra online de amenzi îți oferă o alternativă rapidă și la îndemână în cazul în care dorești să afli informații referitoare la posibile amenzi care să fi fost inregistrate pe numele dumneavoastră.

7.8 implementare software

MD5 este Spring Boot este o platformă open-source pentru simplificarea scrierii aplicațiilor în limbajul Java, dar există extensii pentru crearea de aplicații web pe platforme cum ar fi Java EE(Enterprise Edition).

Deși este folosit în principal pentru platforma Java EE, Spring poate fi utilizat pe orice aplicație Java. Este văzut în comunitatea programatorilor ca o alternativă la modelul Enterpise JavaBeans (EJB).

Partea de logare a utilizatorului se securizează prin intermediul criptării. Ca să protejăm parola utilizatorui folosim criptare cu metoda Sha-256 (Secure Hash Algorithm 256 bits). Sha-256 este o funcție de hash criptografică care primește un input numeric și produce o output de 256 de biți (32 de octeți) și este redată de obicei ca un număr hexazecimal cu o lungime de 64 de cifre.

Arhitectura aplicației este una simpla având o bază de date fizică și un server prin care putem accesa informațiile cerute de utilizator. Utilizatorul v-a interactiona printr-un UI cu server-ul care v-a accesa baza de date și v-a returna inapoi utilizatorul intr-un mod graphic informațiile cerute.

7.9 implementare în viața reală

În primul rând trebuie sa se realizeze infrastructura hardware necesară, care consta efectiv în servere ce trebuie stocate in locuri sigure cu surse de current auxiliare care sa sustină nevoia de electricitate în cazuri de itreruperi de la liniile centrale. După ce sunt puse la punct serverele trebuie construita baza de date cu informații personale a tururor cetațenilor care vor fi ulterior prelucrate de aplicația noastra. După finalizare se va conecta baza de date cu serverele, iar apoi serverele cu aplicația noastra.

Aplicația v-a comunica direct cu serverele care controlează pe deplin totalitatea informațiilor cu character personal introduce in baza de date.

Foarte important de precizat este faptul că vor exista trei tipuri de utilizator:

- Admin
- SuperUser
- User

Fiecare utilizator are anumite drepturi și roluri. Adminul este acela care are acces la tot sistemul și probabil este unul din programatorii care au construit aplicația. SuperUser-ul are drepturi depline in prelucrarea datelor din baza de date, adică este acea persoană care introduce initial date despre o persoană si monitorizează posibile neconcordanțe în legatură cu datele personale. Ultimul tip de utilizator este User-ul care are dreptul doar să își acceseze informațiile atribuite contului sau.

O posibilă problemă care poate să apară cu acest system online este acela ca nu toate persoanele dispun de o masină de calcul si de conexiune la internet sau pur și simplu nu au cunoștințele necesare petru a ccesa o astfel de aplicație. Pentru acești oameni se poate face un serviciu telefonic cu autentificare in timp real sau pu și simplu va trebui să existe un punct fizic care să le asigure aceste informații cu character personal.

7.10 sugestii legislative

Ca sugestii legislative putem recomanda adoptarea acestor aplicatii online în diferite zone de interes care ar micșora timpul petrcut la cozi și ar reduce consumul de hartie. Astfel am deveni o societate modernă în pas cu trendul tehnologic și am putea spune ca sistemul nostru informational devine unul care tine cont de mediu inconjurător ne mai facând risipă de atat de multa hartie.

chapter 8 taxe și impozite

8.1 cadrul legislativ intern

O **funcție criptografică de hash** este

8.2 cum funcționează la noi

Un caz tipic

8.3 cum funcționează în alte țări

Un caz tipic

8.4 cum am vrea să funcționeze

În forma ideală, procedura de colectare a taxelor ar trebui să fie complet automatizată, fără a fi nevoie de intervenția persoanelor fizice sau juridice.

Acestea ar putea fi informate, pentru domeniile de interes, asupra oricăror tranzacții din care fac parte.

Dacă exsită operații care implică transferuri din conturi care aprțin persoanelor fizice sau juridice, acestea trebuie anunțate și detaliate din timp, de preferat prin intermediul sistemului guvernamental de informare, care să permită confirmarea primirii și deschiderii acestora de către utilizator.

8.5 structuri de date

Începem cu

8.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

8.7 cazuri de utilizare

În 1993, Den Boer

8.8 implementare software

MD5 este

8.9 implementare în viața reală

Începem cu

8.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 9 sistem notarial

9.1 cadrul legislativ intern

O **funcție criptografică de hash** este

9.2 cum funcționează la noi

Un caz tipic

9.3 cum funcționează în alte țări

Un caz tipic

9.4 cum am vrea să funcționeze

MD5 este

9.5 structuri de date

Începem cu

9.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

9.7 cazuri de utilizare

În 1993, Den Boer

9.8 implementare software

MD5 este

9.9 implementare în viața reală

Începem cu

9.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 10 tranzacții

10.1 cadrul legislativ intern

O **funcție criptografică de hash** este

10.2 cum funcționează la noi

Un caz tipic

10.3 cum funcționează în alte țări

Un caz tipic

10.4 cum am vrea să funcționeze

MD5 este

10.5 structuri de date

Începem cu

10.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

10.7 cazuri de utilizare

În 1993, Den Boer

10.8 implementare software

MD5 este

10.9 implementare în viața reală

Începem cu

10.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 11 profil personal

11.1 cadrul legislativ intern

O **funcție criptografică de hash** este

11.2 cum funcționează la noi

Un caz tipic

11.3 cum funcționează în alte țări

Un caz tipic

11.4 cum am vrea să funcționeze

MD5 este

11.5 structuri de date

Începem cu

11.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

11.7 cazuri de utilizare

În 1993, Den Boer

11.8 implementare software

MD5 este

11.9 implementare în viața reală

Începem cu

11.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 12 cazier fiscal / credit score

12.1 cadrul legislativ intern

O **funcție criptografică de hash** este

12.2 cum funcționează la noi

Un caz tipic

12.3 cum funcționează în alte țări

Un caz tipic

12.4 cum am vrea să funcționeze

MD5 este

12.5 structuri de date

Începem cu

12.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

12.7 cazuri de utilizare

În 1993, Den Boer

12.8 implementare software

MD5 este

12.9 implementare în viața reală

Începem cu

12.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 13 cazier judiciar

Cazierul judiciar se ține în scopul prevenirii și combaterii faptelor prevăzute și pedepsite de legea penală, ca un mijloc de cunoaștere și identificare operativă a persoanleor care au comis infracțiuni contra persoanei și a libertății acesteia, a patrimoniului și, în general, a ordinii de drept. Cazierul judiciar reflectă situația judiciară a unei persoane. Situația judiciară a unei persoane se referă la evidența condamnărilor ori a altor măsuri cu caracter penal sau administrativ conform Codului penal, precum și a măsurilor procesual-penale luate față de o persoană. În cazierul judiciar nu vor fi înscrise sancțiunile penale pronunțate pentru fapte săvârșite în timpul minorității, măsurile de siguranță luate fără aplicarea unei pedepse, cu excepția internării medicale și a interzicerii ocupării unei funcții sau a exercitării unei profesii și nici datele referitoare la persoanele față de care s-a dispus punerea în mișcare a acțiunii penale sau față de care a fost luată una dintre măsurile preventive prevăzute de Codul de procedură penală.

13.1 cadrul legislativ intern

Legea cadru privind cazierul judiciar este Legea 290/2004, conform căreia este definită organizarea Cazierului Judiciar.

Instituția care se ocupă de organizarea Cazierului Judiciar este Ministerul Administrației și Internelor. Evidența cazierului judiciar și a evidenței operative se ține de unitățile Poliției Române, prin structuri specializate în acest domeniu.

Reglementarea, dată prin Legea nr. 290/2004, republicată în Monitorul Oficial nr. 777/2009, a suferit ulterior modificări în temeiul Legii nr. 255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală şi pentru modificarea şi completarea unor acte normative care cuprind dispoziţii procesual penale, precum şi a Ordonanței de urgență nr. 54/2010 privind unele măsuri pentru combaterea evaziunii fiscale.

13.2 cum funcționează la noi

Organizarea activității de cazier judiciar

În țara noastră, activitatea de cazier judiciar este organizată la ***nivel central*** prin Direcţia Cazier Judiciar, Statistică şi Evidenţe Operative, care este o structură specializată în cadrul Inspectoratului General al Poliției Române, iar la ***nivel local***, prin Inspectoratele de Poliție Județene și Direcţia Generală de Poliţie a Municipiului Bucureşti.

În cazierul judiciar se ține evidența persoanelor fizice și a persoanelor juridice condamnate ori împotriva cărora s-au luat alte măsuri cu caracter penal sau administrativ conform Codului penal, precum și a celor față de care au fost dispuse măsuri procesual-penale.

Înregistrările privind situația judiciară ale persoanelor fizice și juridice sunt păstrate într-o bază de date a cazierului central, de către Inspectoratul General al Poliției Române. Această bază de date este o parte a platformei informatice ROCRIS, platformă care permite obținerea de informații în timp real despre infractorii din România. Această platformă este conectată la platforma europeană ECRIS, care oferă informații în timp real despre infractorii din Uniunea Europeană.

În această bază de date se ține evidența următoarelor persoane:

- a persoanelor fizice și juridice române și
- a persoanelor născute în afara României și a persoanelor juridice străine,

care fac obiectul cazierului judiciar, al evidenței operative și al evidențelor speciale ale poliției, care au

comis infracțiuni pe teritoriul României și au fost condamnate sau față de care a fost pronunțată renunțarea ori amânarea aplicării pedepsei sau față de care au fost dispuse măsurile preventive.

La nivel local există structuri specializate din cadrul Inspectoratelor Județene de Poliție, care actualizează această bază de date cu evidența stării de condamnare a persoanelor născute în România. Aceste structuri sunt responsabile de ținerea la zi a acestor înregistrări.

Documentele care sunt eliberate din această bază de date sunt :

Certificatul de cazier judiciar este documentul eliberat persoanelor, prin care se atestă situația juridică a acestora. Situația juridică cunoaște două posibilități: fie nu figurează în cazierul judiciar, fie figurează, și atunci sunt trecute toate condamnările pe care le-a avut persoana respectivă pentru savârșirea unor infracțiuni.

Extrasul din cazierul judiciar este documentul emis cu ocazia schimbului de informații din cazierele judiciare, efectuat cu statele membre și statele terțe. State membre sunt statele din Comunitatea Europeană, iar stat terț este un stat din afara Comunității Europene.

Extrasul de pe cazierul judiciar este documentul eliberat instituțiilor publice și organelor de specialitate ale administrației publice în baza consimțământului expres al persoanei pentru care se efectuează verificări specifice.

Copia de pe cazierul judiciar este documentul eliberat autorităților române competente. Sunt autorități române competente, organele de urmărire penală, instanțele de judecată, Instituțiile din sistemul de apărare, ordine publică, siguranță națională și justiție.

Din lista documentelor eliberate din baza de date a evidenței cazier judiciar observăm că pentru ***persoa*** se eliberează **doar *certificatul de cazier judiciar***.

Certificatul de cazier judiciar atestă situația juridiciară a unei persoane, astfel că acesta este solicitat de către alte ***instituții ale statului*** în vederea emiterii altor documente (ambasade, consulate - pentru dobândire/redobândire/retragere/renunțare la cetățenia română, direcția/serviciul regim permise și înmatriculare a autovehiculelor – pentru eliberarea permisului de conducere, direcția/serviciul arme – pentru eliberarea autorizațiilor de deținere, păstrare și utilizare a armelor, instanțele de judecată – în cursul fazei de judecată din cadrul proceselor penale) și de către unele ***persoane juridice***, pentru stabilirea situației juridice ca viitori angajați.

Cine Poate solicita eliberarea unui certificat de cazier judiciar?

Pot solicita eliberarea unui certificat de cazier judiciar persoanele fizice române cu domiciliul în România, persoanele fizice române cu domiciliul în străinătate, persoanele fizice și juridice străine care au rezidența în România și persoanele juridice străine care sunt înregistrate în România.

*1. Înțelegem prin **persoane** atât persoanele fizice cât și persoanele juridice. Persoana fizică este omul, în mod individual, ca membru al societății, având calitatea de subiect de drept, iar persoana juridică, o reprezintă o colectivitate de persoane fizice, cu o organizare de sine stătătoare, cu un patrimoniu propriu și îndreptate spre realizarea unui anuit scop.*

2. De pildă, unei persoane condamnate definitiv pentru infracțiuni la regimul circulației pe drumurile publice îi este restricționat dreptul de a conduce autovehicule. Având în vedere acest aspect, la înscrierea la examenul pentru obținerea permisului de conducere se solicită candidaților certificatul de cazier judiciar. În cazul în care în acesta apare o condamnare cu interzicerea dreptului de a conduce, persoana respectivă nu poate susține examenul respectiv

Pentru eliberarea propriului certificatul de cazier judiciar, ***persoanele fizice depun personal*** o cerere-tip motivată, la unitatea de poliție de la locul de naștere, domiciliu sau reședință. După darea în exploatare a Sistemului Național de Evidență Informatizată a Cazierului Judiciar, această cerere poate fi depusă la orice unitate/subunitate de poliție conectată la acest sistem.

Persoanele fizice pot solicita eliberarea propriului certificat de cazier judiciar și prin depunerea cererii de către un împuternicit, în țară, în baza unei procuri autentificate de către un notar public, iar în străinătate, pe baza unei procuri autentificate de către misiunile diplomatice sau oficiile consulare ale României, ori de către un notar străin, însă cu respectarea cerințelor legalizării actelor oficiale străine (pentru țările membre ale UE, apostila).

Persoanele juridice depun cererea-tip completată cu datele complete de identificare și motivată, prin ***reprezentantul legal***, care trebuie să își dovedească calitatea, la unitatea de poliție pe raza căreia își are

sediul social, sucursala, filiala sau punctul de lucru, persoana juridică.

Termenul prevăzut de lege pentru eliberarea certificatului de cazier judiciar este de până la 3 zile, pentru cererile-tip depuse în țară și de 30 zile pentru cererile-tip depuse în străinătate.

Pentru obținerea unui certificat de cazier dintr-un alt stat membru al Ununii Europene, persoana fizică adresează o cerere Direcției de Cazier Judiciar și Statistică din cadrul Inspectoratului General al Poliției Române. Aceștia solicită statului respectiv eliberarea unui extras din cazierul judiciar, eliberând apoi, în baza acestui document, certificatul de cazier judiciar.

Un caz particular prevăzut în mod expres de către lege ca o excepție prin care solicitarea eliberării certificatului de cazier judiciar poate fi făcută și de către alte persoane, este cel în care certificatul de cazier judiciar este necesar pentru depunerea la dosarul de grațiere individuală. În acest caz, eliberarea certificatului de cazier judiciar poate fi solicitată de către persoana condamnată, apărătorul ori reprezentantul legal al acesteia, soțul/soția condamnatului, copii, ascendenții frații sau surorile persoanei condamnate sau ai soțului acesteia, însă trebuie să depună documente care dovedesc această calitate.

Eliberarea certificatului de cazier judiciar se face, de regulă persoanei care a solicitat acest document sau, cu procură, altei persoane desemnate de către titularul certificatului să realizeze acesastă activitate.

Certificatul de cazier judiciar conține următoarele date: antetul emitentului, seria și numărul certificatului, numele și prenumele, data nașterii, codul numeric personal, locul nașterii, ultimul domiciliu, situația judiciară și motivul pentru care a fost eliberat documentul, data și organul de poliție emitent, semnătura șefului cazieruliui judiciar și ștampila unității emitente a documentului.

Certificatul de cazier judiciar este valabil o perioadă de 6 luni.

13.3 cum funcționează în alte țări

Există un sistem european de informații cu privire la cazierele judiciare, ECRIS, care a fost creat în aprilie 2012 cu scopul de a facilita schimbul de informații privind cazierele judiciare între statele membre ale UE. Prin intermediul acestuia se stabilesc conexiuni electronice între statele membre conform unor reguli prin care se asigură faptul că informațiile privind condamnările, astfel cum sunt cuprinse în cazierele judiciare ale statelor membre, pot fi transmise în formate electronice standardizate, uniform, rapid și respectând termenele legale scurte.

ECRIS se bazează pe o arhitectură informatică descentralizată, în cadrul căreia datele cu privire la cazierele judiciare sunt stocate doar în bazele de date naționale ale statelor membre și, la cerere, fac obiectul unui schimb electronic între autoritățile centrale ale statelor membre.

Statul membru, a cărui cetățenie o deține o persoană, devine depozitarul central al tuturor condamnărilor pronunțate împotriva acesteia. Acesta are obligația de a stoca și de a actualiza toate informațiile primite, precum și de a transmite aceste informații altor state membre atunci când îi sunt solicitate. Prin urmare, fiecare stat membru ar trebui să fie în măsură să furnizeze informații complete și actualizate privind condamnările propriilor cetățeni, indiferent de locul în care au fost pronunțate condamnările respective.

Un stat membru care condamnă o persoană de altă cetățenie are obligația de a transmite cât mai repede posibil informațiile, inclusiv orice actualizări aferente, cu privire la condamnarea respectivă statului (statelor) membru (membre) a cărui (căror) cetățenie o deține autorul infracțiunii.

Transmiterea informațiilor cu privire la condamnări se face electronic, prin intermediul unui format european standardizat, cu două tabele de referință privind categoriile de infracțiuni și categoriile de pedepse. Aceste tabele facilitează traducerea automată și înțelegerea reciprocă a informațiilor transmise. Atunci când transmit informații cu privire la o condamnare, statele membre trebuie să utilizeze categoriile referitoare la tipul infracțiunii și pedeapsa aplicată. Codurile permit traducerea automată în limba destinatarului, astfel încât acesta poate reacționa imediat ce a primit informația.

GERMANIA

În Germania, Oficiul Federal al Justiției este instituția care eliberează certificatul de cazier judiciar.

Există posibilitatea solicitării online a unui certificat de cazier judiciar denumit „certificat de bună

conduită". Pentru a intra în posesia acestui document, trebuie ca cel ce aplică să dețină un document de identitate sau un permis de ședere de tip nou și să aibă activată funcția de identificare online, un cititor de crduri sau o cameră video, o aplicație informatică și un scaner, un calculator conectat la internet. Camera video, scanerul și cititorul de carduri sunt necesare pentru încărcarea documentelor necesare eliberării certificatului de cazier judiciar. Portalul online pentru emiterea acestor documente se află la adresa : https://www.fuehrungszeugnis.bund.de/ffw/form/display.do?%24context=A06BC7DC333D9905205F. Aplicația online nu funcționează de pe terminalele de telefonie mobilă. Link-urile de pe portal indică spre descărcarea unei aplicații informatice.

ITALIA

În Italia, certificatul de cazier judiciar poartă denumirea de „Certificato Casellario Giudiziale" și se eliberează în general contra cost. Există însă și excepții (adopția, remedierea erorilor judiciare, etc) în care acesta se eliberează gratuit. Se pot depune solicitări online ale certificatului de cazier judiciar, la adresa: https://www.giustizia.it/giustizia/it/mg_3_3_2.wp, care însă trebuiesc ridicate personal de la Biroul Judiciar al Parchetului local de la locul de domiciliu al solicitantului.

FRANȚA

În Franța este posibilă solicitarea certificatului de cazier judiciar on-line, de la adresa: https://casier-judiciaire.justice.gouv.fr/mai-web-b3-presentation/pages/accueil.xhtml?cid=1. Și în Franța acest tip de document este eliberat de către Ministerul Justiției – Casier Judiciaire Național. Portalul oferă informațiile în limba franceză, în limba engleză, în limba germană și în limba spaniolă.

Dacă dorești să soliciți eliberarea documentului ești ghidat pe un site în care trebuie să completezi un minim de date personale, o adresă de e-mail validă și un security code (CAPTCHA), la adresa: https://casier-judiciaire.justice.gouv.fr/mai-web-b3-presentation/pages/accueil.xhtml .

ANGLIA

În Anglia serviciul Cazier se numește ACRO (A Criminal Record Office) și pentru eliberarea certificatului de cazier judiciar (criminal record) trebuie să faci online, dovada identității, să depui solicitarea, la adresa: https://www.acro.police.uk/Subject-Access-Online.aspx și să declari o adresă de e-mail validă. Procesarea solicitării durează o lună iar rezultatul va fi trimis fie prin e-mail, fie prin poștă, la adresa declarată.

SPANIA

Și în Spania, certificatul de cazier judiciar este eliberat de către Ministerul Justiției și se numește „Certificado de Antecedentes Penales". Solicitarea se poate depune personal, prin poștă sau online și se plătește o taxă pentru eliberarea certificatului. Plata taxei se poate face și online, se cere însă dovada plății. Portalul online se află la adresa: https://sede.mjusticia.gob.es/cs/Satellite/Sede/es/tramites/certificado-antecedentes . Solicitarea se prelucrează de regulă în 24 de ore de la depunerea documentelor, certificatul emis, se poate descărca online. Termenul legal de emitere a certificatului este de 10 zile, dar ca regulă se emite între 24 de ore și 3 zile de la depunerea solicitării. Pentru utilizarea acestui document în străinătate el trebuie legalizat, pentru aceasta există o opțiune în cererea de certificare.

13.4 cum am vrea să funcționeze

Cazierul judiciar este o baza de date a statului, gestionată, exploatată și actualizată de către Inspectoratul General al Poliției Române, prin structuri specializate care funcționează la nivel local. Întrucât acest sistem funcționează în principal pentru interesul statului, considerăm că este oportun a se distinge între partea de interes operativ, partea strict juridică, cooperare judiciară internațională, care sunt necesare și trebuie să rămână centralizate la nivel de stat, și partea așa numită civilă, în care fiecare persoană să poată avea acces ușor și rapid la datele sale personale, inclusiv la înregistrările din cazierul judiciar. Desigur, că ideal ar fi ca de pe orice calculator sau terminal mobil, legat la internet, să putem depune o solicitare online și la adresa de e-mail să primim, într-un timp rezonabil de 24 ore – 3 zile, un certificat de cazier judiciar în format electronic, (pdf) semnat digital, și care să poată fi apoi listat sau trimis prin e-mail și să poată face dovada situației noastre judiciare.

Ar fi util și foarte comod ca autentificarea noastră pe portalele ce eliberează documente să se poată face prin CNP și parolă. Această autentificare ar fi însă suficientă pentru a face dovada identității? În ce privește

solicitarea online de emitere de documente trebuie însoțită de alte documente doveditoare, care trebuiesc încărcate în platformă în anumite formate specifice. Am putea oare să scăpăm de folosirea unor documente pentru emiterea altor documente? Am putea oare să folosim avantajele enorme ale tehnicii de calcul în mod constructiv, pentru a ne ușura viața?

Am vrea ca lucrurile să fie simple, să fie ușor de utilizat, eficiente, să folosească cât mai puține resurse și cât mai puțin timp, documentele emise în format electronic să aibă aceeași valoare ca și cele realizate pe suport din hârtie. Să nu mai întâlnim ghișee care se închid în fața noastră după ce am stat un timp îndelungat, neputincioși în fața lor și nici lucrători frustrați și plictisiți de monotonia slujbei lor.

Răspunsul este: DA! Putem face lucrurile să funcționeze simplu și eficient, rapid și sigur, promt și corect. Este posibil să obținem online un document tip certificat de cazier judiciar, însă pentru aceasta trebuie mai întâi modificată Legea 290/2004, conform căreia este definită organizarea Cazierului Judiciar.

13.5 structuri de date

Baza de date „cazier” conține 6 tabele considerate a fi necesare și suficiente pentru realizarea dezideratului propus și anume gestionarea și eliberarea unui certificat de cazier judiciar.

Tabelele sunt:

1. „CERERI”, cu coloanele „CERERE_ID”, Type Int(16) și „DATA_SOLICIT” Type date, default curent_timestamp; conține registrul de înregistrare al cererilor cu numărul de înregistrare al solicitării și data solicitării.

2. „ELIBERARI”, cu coloanele „DATA_ELIB” Type date, default curent_timestamp, „ISTORIC_ACT” Type varchar(200) și „NR_ACT” Type int(10); conține registrul de eliberări a cererilor de cazier și istoricul cererilor care au fost eliberate până în prezent.

3. „MASURI”, cu coloanele „ACCESORII” Type varchar(200) conține pedepsele accesorii ale pedepsei principale, respectiv interzicerea anumitor drepturi „CONDAMNĂRI” Type varchar(200) conține pedepsele pronunțate de către instanța de judecată, rămase definitive și executorii, „ISTORIC” Type varchar(200) conține înregistrări privind actele de Amnistie, Grațiere și Reabilitare judiciară și „MASURI DE SIGURANTA” Type varchar(200), conține înregistrările privind obligarea persoanei de a îndeplini sau a nu îndeplini o anumită activitate, pentru a înlătura astfel o stare de pericol generatoare de noi fapte prevăzute de legea penală.

4. „MOTIV ELIBERARE”, cu coloanele „PERS_EXT” Type varchar(200), conține înregistrări privind motivele solicitării eliberării certificatului de cazier judiciar pentru persoanele cu cetățenie română și cu domiciliul în străinătate, „PERS_FIZICE” Type varchar(200) conține înregistrări privind motivele solicitării eliberării certificatului de cazier judiciar pentru persoanele cu cetățenie română și cu domiciliul în țară „PERS_JURIDICE” Type varchar(200) conține înregistrări privind motivele solicitării eliberării certificatului de cazier judiciar pentru persoanele juridice.

5. „PEOPLE”, cu coloanele „PEOPLE_ID” Type bigint(16) Extra AUTO_INCREMENT, „FAMILY_NAME” Type varchar(32) - nume „MIDDLE_NAME” Type varchar(32) – al doilea prenume „FIRST NAME” Type varchar(64) – nume de familie „PREV_FAM_NAME” Type varchar(32) – prenume anterior „PREV_FIRST_NAME” Type varchar(64) – nume anterior „PREN_TATA” Type varchar(30) „PREN_MAMA”Type varchar(30) „EMAIL_OFICIAL” Type varchar(128) „LOC_NASTERE”Type varchar(200) „DATA_NASTERII” date „LOC_DOMICILIU” Type varchar(200) „JUD_NASTERE” Type varchar(200) „JUD_DOMICILIU” Type varchar(200) „STRADA” Type varchar(200) „NR_DOM” smallint(10) „BLOC” Type varchar(10) „SCARA” Type varchar(10) „AP” Type varchar(10) „CNP” Type varchar(13).

6. „TRANZACTII” cu coloanele „TRANZACTIE_ID” și „DATA_TIMP”

13.6 controlul accesului

Funcție de tipul utilizatorului, accesul la baza de date se face pe nivele în care drepturile sunt foarte clar definite. Introducerea de date, actualizarea acesteia, se face la nivelul Inspectoratului General al Poliției Române, de către Direcția Cazier Judiciar și Evidență Operativă. La acest nivel există un administrator al bazei de date, care are drepturi depline, de a introduce, șterge și modifica tabele, coloane și linii ale bazei de date, de a crea și implementa linii de cod PHP sau SQL pentru crearea și modificarea relațiilor dintre tabelele bazei de date și a gestiona ceilalți utilizatori. Clasa utilizatorilor se împarte în utilizatori de rangul 1 care au dreptul de a vizualiza datele din întreaga bază de date și de a adăuga înregistrări în baza de date. Nu au dreptul de a modifica/șterge tabele și nici de a crea și implementa linii de cod PHP sau SQL (doar dreptul de a le rula) și nici dreptul de a gestiona utilizatori. Clasa utilizatorilor de rangul 2 de regulă ofițerii și agenții de poliție, care au dreptul de a vizualiza date din întrega bază de date și de a solicita copii ale înregistrărilor de interes operativ. Clasa utilizatorilor de rangul 3, cei care au dreptul de a vizualiza doar datele lor personale. Aceștia din urmă vor fi persoanele fizice sau juridice, române sau străine care, odată cu modificarea Legislativă în domeniu își pot accesa direct datele personale și numai acestea, după o autentificare biometrică sau după ce realizează dovada identității.

Crearea unui nou cont de utilizator de rangul 3 se va putea realiza direct pe interfața web, după scanarea biometrică și asocierea datelor biometrice cu cele din baza de date.

13.7 cazuri de utilizare

În viitor, astfel de interfețe web și accesul persoanei la propriile date, în scopul emiterii unor documente se vor utiliza frecvent datorită faptului că se vor elimina cheltuielile cu personalul, cu sedii, cu energie electrică și termică, aparatură. Eficiența unei astfel de aplicații va fi apreciată de către toți utilizatorii.

Se vor realiza economii substanțiale la hârtie și toner, și toate consumabilele de birotică necesare.

13.8 implementare software

Este necesară implementarea scanării biometrice, fapt care va efectua foarte ușor dovada identității solicitantului. Datele personale sunt păstrate în siguranță accesul la aceste date fiind controlat și personalizat.

Este de asemenea necesară implementarea semnăturii digitale, care să confirme autenticitatea datelor conținute și a emitentului actului.

13.9 implementare în viața reală

Implementarea în viața reală trebuie să pornească de la modificarea legislației care reglementează documentele de identitate, de călătorie, permise de conducere, certificate de înmatriculare, etc, care pot fi toate în format electronic, utilizatorii de rangul 2 având acces la verificarea și vizualizarea lor.

13.10 sugestii legislative

Modificarea Legii 290/2004 privind organizarea și funcționarea Cazierului Judiciar astfel încât să

permită eliberarea documentelor online. Totodată trebuie să se permită crearea și administrarea de utilizatori care să completeze cererile-tip online iar soluțiile acestor cereri să poată avea – în format electronic fiind - valoarea unui document emis în mod clasic. Generalizarea noțiunii de semnătură electronică și aplicarea ei la semnarea documentelor online.

chapter 14 sistem de vot electronic

14.1 cadrul legislativ intern

Guvernele și organizațiile democratice trebuie să aibă mecanisme de votare a membrilor lor.În mod tradițional, alegerile au servit ca mecanisme oficiale pentru ca oamenii să își exprime opiniile guvernelor lor, în timp ce sondajele au mărit alegerile ca măsuri neoficiale - dar totuși valoroase - ale opiniei publice.Atât în, cadrul sondajelor, cât și al alegerilor, este de obicei dorită confidențialitatea și securitatea, dar nu întotdeauna realizabile simultan la un cost rezonabil.Mecanismele care asigură securitatea și confidențialitatea unei alegeri pot fi consumatoare de timp și costisitoare pentru administratorii de alegeri și incomode pentru alegători.Organizarea alegerilor sigure și private poate deveni și mai dificilă atunci când alegătorii sunt distribuiți geografic.

14.2 cum funcționează la noi

Înainte de începerea fiecărui mandat parlamentar trebuie să aibă loc alegeri generale. De vreme ce durata unui mandat parlamentar este de patru ani, alegerile pentru Camera Deputaților și pentru Senat se desfășoară în cel mult 3 luni de la expirarea mandatului sau de la dizolvarea Parlamentului. Cei patru ani încep de la prima întrunire a Parlamentului la convocarea presedintelui . Data alegerilor se află la discreția prim-ministrului. Organizațiile cetățenilor aparținând minorităților naționale, chiar când nu întrunesc în alegeri numărul de voturi pentru a fi reprezentate în Parlament, au totuși dreptul la câte un loc de deputat, putând fi reprezentate de o singură organizație. Din 1990 încoace toate alegerile generale s-au ținut duminica: o dată în mai, o dată în septembrie și de două ori în noiembrie. Pragul electoral al partidelor este de 5% din voturi. În 2004, numărul de mandate va scădea cu 5%, datorită scăderii numărului de locuitori. Comisia electorală a stabilit durata campaniei electorale la 30 de zile.

Oricine este cetățean român, are domiciliul stabil în Romania și a împlinit până în ziua alegerilor inclusiv vârsta de 23 de ani pentru Camera Deputaților sau respectiv 33 de ani pentru Senat, poate deveni membru al Parlamentului Romaniei. Excepție fac debilii și alienații mintali puși sub interdictie precum și persoanele condamnate care prin hotărâre judecătorească definitivă și-au pierdut drepturile electorale. Cetățenii români din străinătate sunt și ei eligibili.

Legea electorală din România a fost criticată pentru faptul că împiedică micile formațiuni să se înregistreze ca partide politice, prin impunerea strângerii unui minim de 200.000 de semnături.De asemenea, marile partide au fost acuzate de fraude uriașe în procesul electoral premergător alegerilor parlamentare programate, criticii susținând că formațiunile politice de calibru din România au sute de mii de semnături false pe listele de adeziuni obligatorii prin lege.

14.3 cum funcționează în alte țări

Scrutinul pentru Casa Albă este unul indirect, în care delegaţii şi electorii din Colegiul Electoral iau locul votanţilor direcţi. Scopul sistemului este ca statele cu o populaţie redusă să nu fie ignorate în procesul electoral.Toate cele 50 de state federale americane au un număr prestabilit de „electori” în Colegiul Electoral – aproximativ proporţional cu populaţia statului.În total, Colegiul este format din 538 de electori, din care 435 sunt distribuiţi în funcţie de populaţia statelor, iar 100 sunt distribuiţi câte doi pentru fiecare stat american. Alţi trei electori sunt desemnaţi pentru capitala Washington D.C. Pentru ca un candidat să câştige alegerile are nevoie de susţinerea a cel puţin 270 de electori – jumătate plus unul.

Distribuirea electorilor se face, aproape în toate statele, după principiul „câştigătorul ia totul”, astfel

candidatul care obţine majoritatea votului popular într-un stat va obţine toţi electorii acelui stat. Există, însă, două excepţii: Maine şi Nebraska, unde electorii sunt repartizaţi proporţional. Principalul dezavantaj al sistemului electoral american este faptul că unele voturi sunt mai valoroase decât altele, mai ales în cazul aşa-numitelor „swing states”, state cu o populaţie însemnată şi care oscilează între republicani şi democraţi. Acestea sunt principalele “câmpuri de luptă” pentru candidaţi şi decid, de regulă, soarta scrutinului.

Practic, americanii votează pentru electori, nu pentru candidaţii propriu-zis. Electorii sunt oficiali din stat sau membri ai partidelor, dar numele lor nu apare, de regulă, pe buletinul de vot. Numărul de electori pe care îi are fiecare stat este egal cu numărul de reprezentanţi pe care îi are în Camera Reprezentanţilor şi în Senat. California, de exemplu, cel mai mare stat, are 55 de electori, în timp ce Wyoming, stat cu populaţie redusă, are numai trei.

14.4 cum am vrea să funcționeze

Se organizează în circumscripții uninominale și prezintă următoarele caracteristici. Sistemul electoral majoritar se numește și *the winner takes it all* sau *first past the post*, în sensul că acel candidat care obține cel mai mare număr de voturi, fie printr-o majoritate relativă fie printr-o majoritate absolută, câștigă cursa electorală, obținând toate mandatele puse în joc în circumscripția respectivă. Cei care pierd, deci, nu vor fi reprezentați, chiar dacă numărul lor depășește 50%. Acest lucru se poate întâmpla când regula câștigării este majoritatea relativă. De exemplu, Candidatul X obține în urma alegerilor 37% din opțiunile alegătorilor, fiind plasat pe primul lor în circumscripția uninominală respectivă. El va primi toate mandatele, chiar dacă 63% din totalul alegătorilor nu își regăsesc opțiunile reprezentate de Candidatul X. Sistemul electoral majoritar este foarte competitiv, generând antagonismul părților. Nu se poate vorbi de o colaborare a partidelor sau a liderilor într-un astfel de sistem. Si pentru că majoritatea populației rămâne nereprezentată, sistemul este mai corect denumit: metoda pluralității sau cea mai mare majoritate. O altă caracteristică a sistemului electoral majoritar este aceea că distorsionează rezultatele, suprareprezentând partidele mari care câștigă de obicei cursa electorală și subreprezentând partidele perdante, de obicei mai mici. Acest sistem încurajează teoria votului util: diminuează șansele unui partid mic deoarece raționamentul spune că un vot pentru un partid care nu are șanse să câștige cursa electorală este un vot irosit.

14.5 structuri de date

În informatica, o structură de date este o metodă sistematică de stocare a informațiilor și a datelor într-un calculator, în așa fel încât ele să poată fi folosite în mod eficient. Deseori o alegere bine făcută a structurii de date va permite și implementarea unu algoritm eficient. Structura de date aleasă este derivată de multe ori dintr-un tip de data abstract. O structură de date bine concepută permite efectuarea unei varietăți de operații de bază, utilizând puține resurse (ca de exemplu memoria necesară și timpul de execuție). Structurile de date se implementează utilizând tipuri de date,referinte și operații asupra acestora, toate facilitate de către un limbaj de programare.

14.6 controlul accesului

14.7 cazuri de utilizare

14.8 implementare software

14.9 implementare în viața reală

Implementare

14.10 sugestii legislative

O cerință

chapter 15 sistem guvernamental de informare

15.1 cadrul legislativ intern

O **funcție criptografică de hash** este

15.2 cum funcționează la noi

Un caz tipic

15.3 cum funcționează în alte țări

Un caz tipic

15.4 cum am vrea să funcționeze

MD5 este

15.5 structuri de date

Începem cu

15.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

15.7 cazuri de utilizare

În 1993, Den Boer

15.8 implementare software

MD5 este

15.9 implementare în viața reală

Începem cu

15.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 16 creare și administrare firme

16.1 cadrul legislativ intern

O **funcție criptografică de hash** este

16.2 cum funcționează la noi

Un caz tipic

16.3 cum funcționează în alte țări

Un caz tipic

16.4 cum am vrea să funcționeze

MD5 este

16.5 structuri de date

Începem cu

16.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

16.7 cazuri de utilizare

În 1993, Den Boer

16.8 implementare software

MD5 este

16.9 implementare în viața reală

Începem cu

16.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 17 integrarea componentelor sistemului

17.1 cadrul legislativ intern

O **funcție criptografică de hash** este

17.2 cum funcționează la noi

Un caz tipic

17.3 cum funcționează în alte țări

Un caz tipic

17.4 cum am vrea să funcționeze

MD5 este

17.5 structuri de date

Începem cu

17.6 controlul accesului

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

17.7 cazuri de utilizare

În 1993, Den Boer

17.8 implementare software

MD5 este

17.9 implementare în viața reală

Începem cu

17.10 sugestii legislative

Valorile de hash ale unor șiruri sunt specificate în RFC 1321, astfel:

chapter 18 gdpr – general data protection regulation

Conținutul acestui capitol provine în mare măsură din articolul: Ce este GDPR? Regulament GDPR explicat în 5 minute - https://legalup.ro/regulament-gdpr/ [GDPR-SCURT].

18.1 ce este GDPR?

„GDPR” este abrevierea a „General Data Protection Regulation”, iar scopul acestei dispoziții legale este de a proteja datele cu caracter personal și a delimita clar modul în care acestea pot fi prelucrate.

Textul legislativ care face referire la protecția datelor personale este Regulamentul UE nr. 679/2016, cunoscut drept GDPR, și care înlocuiește Directiva CE nr. 46/1995. El vizează datele cu caracter personal, adică orice informație referitoare la o persoană și care poate duce la identificarea sa directă sau indirectă, indiferent dacă introducerea datelor are loc manual sau printr-un mijloc automatizat, de tip formular online.

Aceste date se împart în două categorii:

- Date personale: nume, CNP, localizare geografica, adresă IP, adresă email
- Data personale sensibile: starea de sănătate, informații biometrice, informații genetice, orientare sexuală, orientare politică

18.2 context istoric

Deși conceptele de bază ale respectării vieții private au fost expuse vag în anii 1950 în timpul unei convenții a UE privind drepturile omului, ele nu erau specifice stocării electronice a datelor cu caracter personal. Prin anii 1980, când computerul începea să fie folosit pentru prelucrarea datelor cu caracter personal, consiliul european a organizat o convenție. Aceasta stabilește orientări pentru membrii UE cu privire la ceea ce este greșit și ce este bine. Din aceasta, Marea Britanie a creat Legea privind protecția datelor din 1984.

Acesta a fost un început bun, dar de când a fost adoptat, utilizarea computerelor și disponibilitatea acestora au crescut exponențial. Această creștere fără precedent a condus la o altă convenție a UE în 1995 - Directiva privind protecția datelor. Scopul principal al acestui lucru a fost de a stabili un standard general mai înalt, modul în care datele UE pot părăsi UE și modul în care această directivă se poate aplica statelor din afara UE. Ulterior, Marea Britanie a creat apoi Legea privind protecția datelor din 1998. Alte țări au urmat exemplul, creându-și propriile versiuni. Acesta a fost un început bun, dar erau în mare parte incompatibili între ei.

În anul 2012, a devenit evident că este nevoie de un teren comun în întreaga UE, având în vedere că aceasta era o directivă care, în general, este doar sugestivă. Legislația GDPR a fost propusă și apoi negociată în cadrul consiliului UE și al parlamentului european. La aproape 2 ani după aceasta, în 2014, parlamentul european a ajuns la un acord. Anul următor au avut loc negocieri suplimentare care au dus la aprobare. Apoi, în primăvara anului 2016, regulamentul a fost pe deplin adoptat și pus în aplicare.

Fiind în vigoare, s-a decis că va fi o fază de implementare de doi ani și că actul va începe să se aplice la 25 mai 2018.

18.3 document oficial

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. Acest text include rectificarea publicată în JOUE din 23 mai 2018.

Regulamentul este un pas esențial pentru consolidarea drepturilor fundamentale ale oamenilor în era digitală și pentru clarificarea normelor pe piața unică digitală, în beneficiul întreprinderilor și al organismelor publice. În același timp, această reglementare unică va pune capăt fragmentării actuale din diferitele sisteme naționale și va elimina sarcinile administrative inutile.

Regulamentul a intrat în vigoare la 24 mai 2016 și s-a aplicat din data de 25 mai 2018.

Directiva (UE) 2016/680 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date.

Directiva protejează dreptul fundamental al cetățenilor la protecția datelor ori de câte ori datele cu caracter personal sunt utilizate de autoritățile de aplicare a dreptului penal pentru a asigura respectarea legii. Ea va garanta în special protecția adecvată a datelor personale ale victimelor, martorilor și suspecților și va facilita cooperarea transfrontalieră în combaterea criminalității și a terorismului.

18.4 principii GDPR

GDPR introduce șapte principii care trebuie respectate de către orice organizație care prelucrează date așa cum sunt ele descrise pe scurt mai jos:

- **Legalitate, echitate și transparență** – acesta este un principiu esențial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate ”în mod legal, echitabil şi transparent faţă de persoana vizată” și explică-i de ce îi prelucrezi într-un limbaj pe care îl poate înțelege, fără jargon juridic.
- **Limitarea scopului** – datele personale trebuie să fie colectate în scopuri bine determinate, explicite şi legitime, iar prelucrările ulterioare nu trebuie să se abată de la aceste scopuri;
- **Minimizarea datelor** - prin acest principiu operatorii sunt avizați de faptul că orice colectare de date personale trebuie foarte bine analizată înainte de obținerea efectivă a datelor, care trebuie să fie cele mai relevante și strict limitate la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate;
- **Verificarea corectitudinii datelor și actualizarea acestora** - operatorii trebuie să se ia toate măsurile pentru a asigura validitatea datelor, iar cele dovedite inexacte trebuie actualizate rapid sau șterse;
- **Integritate și confidențialitate** – prelucrarea datelor personale trebuie făcută în cele mai proprii condiții de siguranță, care să includă ”protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare” (ex. certificări ISO 27001);
- **Responsabilitate** – documentează procesele și fii capabil să demonstrezi respectarea principiilor de mai sus;
- **Limitări legate de stocare** - datele trebuie păstrate fix atâta timp cât sunt necesare pentru pelucrarea asumată. Perioadele mai lungi de stocare sunt excepții asociate cu activități publice de arhivare, cercetare sau statistică.

18.5 legalitatea operațiunilor asupra datelor

Operațiunile asupra datelor trebuie să fie bazate pe cel puțin unul din principiile enunțate mai jos:

- **Consimțământul** – persoana și-a dat în mod explicit consimțământul
- **Contractul** – există sau urmează a se semna un contract
- **Obligația legală** – există o obligație legală
- **Interesul vital** – atunci când este necesară protecția vieții sau a proprietăților persoanei
- **Interesul public**
- **Interesul legitim al procesatorului** – atâta timp cât nu e în conflict cu interesul persoanei

Indiferent de temei (consimțământul, contractul, obligația legală etc), trebuie să respecți GDPR și să pui în practică politici adecvate de protecție a datelor.

Cele șase temeiuri enumerate mai sus se află pe poziție de egalitate. Consimțământul este important, însă el vine cu dezavantaje, cum ar fi dreptul de retragere a consimțământului, imposibilitatea de a obține consimțământul tuturor persoanelor, refuzul de a-și da consimțământul.

Interesul legitim se va folosi cu precauție. El se folosește, de regulă, pentru situații în care nu există nu se poate sau nu se dorește obținerea consimțământului și nu există alt temei (supraveghere CCTV, monitorizare locație gps, recrutare, organizări evenimente etc).

18.6 consimțământul

Consimțământul persoanei trebuie să îndeplinească o serie de condiții, printre care să fie **cert** și **informat**. Căsuțele pre-bifate, tăcerea sau inacțiunea nu înseamnă consimțământ. Persoana trebuie să îți dea consimțământul printr-o acțiune reală, precum bifarea unei căsuțe, o semnătură, un DA categoric înregistrat.

Pentru a fi valabil, consimțământul trebuie să îndeplinească cumulativ următoarele condiții:

1. să fie dat în mod liber;
2. să fie specific;
3. să fie informat;
4. să fie lipsit de ambiguitate;

Cu privire la anumite categorii de date sensibile (de exemplu, datele medicale, genetice, biometrice, datele care dezvăluie originea rasială, etnică, convingerile religioase, filozofice), în situația transferurilor către state terțe UE fără garanții adecvate și în situația deciziilor automate cu efect semnificativ, consimțământul trebuie să îndeplinească o cerință suplimentară: să fie explicit.

Potrivit Grupului de Lucru, consimțământul trebuie să fie o alegere reală pentru persoana vizată. Dacă persoana nu are o alegere reală, se simte obligată să își dea consimțământul sau urmează să suporte consecințe negative dacă nu își dă acordul, consimțământul nu este valabil.

În situația în care consimțământul este asociat unor termeni și condiții care nu pot fi negociați sau în situația în care nu poate fi acordat sau retras fără prejudicii, vorbim despre un consimțământ nevalid.

Utilizarea unui serviciu condiționată de acordarea consimțământului este permisă doar dacă prelucrarea datelor este necesară pentru executarea respectivului contract. Grupul de Lucru precizează că această condiționare trebuie interpretată strict: “trebuie să existe o legătură directă și obiectivă între prelucrarea datelor și scopul executării contractului”.

Exemplu oferit de Grupul de Lucru:

„O aplicație pentru editarea fotografiilor solicită utilizatorilor să aibă locația GPS activată pentru utilizarea serviciilor, datele privind geolocalizarea fiind colectate în scopuri de publicitate comportamentală. Geolocalizarea nu este necesară pentru furnizarea serviciului de editare foto. Dacă utilizatorul nu poate folosi aplicația fără a fi de acord cu prelucrarea acestor date, contimțământul nu este acordat în mod liber.”

În situația unui dezechilibru de putere, ca de exemplu, în relația angajator – angajat, consimțământul nu este valabil decât în cazuri excepționale. Prin urmare, recomandarea Grupul este ca temeiul legal de prelucrare a datelor angajaților să nu fie consimțământul.

Datele personale nu pot fi oferite drept plata pentru serviciile online gratuite, consimțământul fiind valabil numai dacă sunt puse la dispoziție servicii echivalente care nu depind de utilizarea datelor cu caracter personal, fără costuri suplimentare, subiectul având, astfel, libertatea de a alege. Similar, dacă persoana decide să își retragă consimțământul, nu sunt permise costuri suplimentare sau dezavantaje.

Pentru a fi liber, consimțământul trebuie acordat separat pentru fiecare scop specific al prelucrării.

Pentru copii sub 16 ani, își vor da părinții consimțământul. Iar în anumite cazuri, precum prelucrarea datelor sensibile sau transferul international de date, consimțământul trebuie să fie explicit: verificare în doi factori, semnătură scrisă, semnătură electronica etc.

18.7 drepturile persoanei fizice

Regulamentul GDPR introduce un set de drepturi pentru persoanele fizice, drepturi pe care operatorul de date personale are obligația de a le respecta. Totodată, acesta trebuie să răspundă în timp util cererilor persoanei în timp util, de obicei în maximum o lună.

1. dreptul la informare
2. dreptul de acces
3. dreptul la verificare
4. dreptul la ștergere
5. dreptul la restricționarea prelucrării
6. dreptul la portabilitate
7. dreptul la obiecție
8. dreptul de a nu fi supusă unei decizii automate, inclusiv crearea de profiluri
9. dreptul de a depune o plângere la Autoritatea de supraveghere
10. dreptul de a se adresa instanței de judecată

Detaliem în continuare aceste drepturi.

1. dreptul la informare

Regulamentul GDPR oferă posibilitatea oricărui individ de a se informa asupra datelor sale personale. Acesta are dreptul să solicite informații privind scopul, temeiul legal pentru care datele sale personale sunt prelucrate, destinatarii acestor date, perioada de stocare, dacă sunt transferate către țări terțe, precum și datele de contact ale operatorului.

2. dreptul de acces

Persoanele a căror date sunt procesate au dreptul de a primi o confirmare din partea operatorilor de date cu caracter personal, un drept de acces la informațiile respective dar și despre modul în care vor fi prelucrate. În acest sens, operatorul va furniza informații despre scopul prelucrării, destinatarii datelor, dreptul de a depune o plângere în fața autorității competente, transferul lor către țări terțe și garanțiile oferite pentru un transfer cât mai sigur.

În plus, persoanele vizate pot obține o copie a datelor cu caracter personal. Un exemplu destul de simplu pentru a înțelege cât mai bine mecanismul acestui drept este conferit chiar de raporturile de muncă. Între angajator și angajat se încheie un contract de muncă; ulterior salariatul poate cere oricând accesul la dosarul personal. Cu toate acestea dreptul de acces conține și anumite limite.

3. dreptul la rectificare

Dreptul la rectificare poate fi exercitat în cazul în care datele sunt inexacte, incomplete, echivoce sau perimate. Persoana vizată va aduce la cunoștința operatorului aceste nereguli, iar acesta le va rectifica în cel mai scurt timp. Totodată operatorul este obligat să transmită rectificările destinatarilor datelor cu caracter personal.

4. dreptul la ștergere

Dreptul la ștergere este unul fundamental deoarece dă persoanelor vizate un drept de dispoziție asupra datelor cu caracter personal. Astfel, orice persoană poate cere ștergerea datelor pentru următoarele motive:

- scopul pentru care au fost colectate sau procesate a fost atins;
- persoana vizată *„își retrage consimţământul pe baza căruia are loc prelucrarea şi nu există niciun alt temei juridic pentru prelucrarea;”*
- persoana se opune prelucrării datelor (dreptul de opoziție prevăzut de Regulamentul GDPR în art. 21)
- datele au fost ilegal procesate;
- există o obligație legală a operatorului prevăzută de dreptul Uniunii Europene sau de dreptul intern de a șterge aceste date;
- datele cu caracter personal au fost „colectate în legătură cu oferirea de servicii ale societăţii informaţionale menţionate la articolul 8 alineatul (1).” Articolul 8 alin. 1 se referă la prelucrarea datelor copiilor cu vârsta de 16 ani (prelucrare legală) și a celor sub 16 ani (prelucrarea este legală dacă titularul autorității părintești își dă consimțământul, în caz contrar, este ilegală).

5. dreptul la restricționarea prelucrării

Prin intermediul acestui drept o persoană poate limita modul în care un operator îi folosește datele cu caracter personal. Cu toate acestea, dreptul nu este unul discreționar, fiind exercitat în anumite circumstanțe prevăzute de articolul 18 din Regulamentul GDPR:

- persoana vizată contestă exactitatea datelor personale- este o restricționare temporară operatorul făcând toate verificările necesare
- datele au fost prelucrate ilegal, iar persoana vizată se opune ștergerii și solicită restricția în schimb;
- operatorul nu mai are nevoie de datele personale dar persoana i le solicită pentru exercitarea sau apărarea dreptului în instanță;
- persoana vizată s-a opus prelucrării datelor în conformitate cu articolul 21 alineatul (1)- operatorul va verifica dacă interesul său legitim prevalează asupra interesului personal.

Operatorul poate refuza cererea de restricționare a persoanei vizate dacă este nefondată sau are caracter repetitiv.

6. dreptul la portabilitate

Acest drept a fost introdus prin Regulamentul GDPR și oferă posibilitatea persoanelor vizate de a primi datele personale într-o manieră cât mai clară și structurată. În plus ele pot fi stocate și transmise ușor de la un operator la altul. Orice date furnizate pot face obiectul dreptului la portabilitate? Răspunsul este nu. Doar datele prelucrate pe bază de consimțământ dat în mod legal conform articolului 6 alineatul (1) litera (a) sau al articolului 9 alineatul (2) litera (a)-adică consimțământul dat pentru scopuri specifice și cel dat pentru executarea unui contract.

7. **dreptul la opoziție**

   Dreptul la opoziție constă din refuzul de a permite prelucrarea datelor pentru motive ce țin de *„situația particulară”* a oamenilor. Astfel, se va analiza fiecare caz în parte înainte de a se da curs unei cereri privind acest drept. Totodată dreptul nu este limitat în timp, persoana vizată având posibilitatea de a se opune în orice moment prelucrării. La fel se întâmplă și în cazul colectării de date în scop de marketing direct.

   Dacă datele au început deja să fie prelucrate se poate solicita ștergerea lor (dreptul de a fi uitat). Operatorul are totuși o pârghie de salvare dacă dovedește că are motive legitime justifică prelucrarea şi care prevalează asupra drepturilor persoanei vizate sau dacă aceste date au ca scop constatarea, exercitarea sau apărarea unui drept în instanţă.

8. **dreptul de a nu fi supusă unei decizii automate, inclusiv crearea de profiluri**

   Persoana are dreptul la intervenție umană în cazul deciziilor importante care o privesc.

9. **dreptul de a depune o plângere la Autoritatea de supraveghere**

   Atunci când este nemulțumită de modalitatea în care i se prelucrează datele sau când drepturile nu i-au fost respectate

10. **dreptul de a se adresa instanței de judecată**

    Pentru a obține daune materiale și/sau morale dacă a rezultat un prejudiciu.

18.8 adoptarea GDPR în alte țări

Adoptarea GDPR are implicații și asupra entităților din afara UE care operează direct sau indirect pe teritoriul Uniunii Europene.

În România, Autoritatea care se ocupă de aplicarea, reglementarea și controlul este ANSPDCP. Campaniile de informare a populației române sunt practic inexistente. Persoanele care vor sa afle mai multe despre GDPR trebuie să se documenteze singure. Fie că vorbim de operatori de date sau de persoane vizate, lipsa informării exacte a dus la greșeli în aplicare, la amenzi, la imposibilitatea exercitării drepturilor și a încălcării securității datelor cu caracter personal.

Din experiența ultimului an de GDPR România, putem spune cu siguranță că operatorii și implicit conducerea companiilor sau a instituțiilor publice, sunt mai preocupate de supravegherea angajaților, marketing agresiv, neasumarea răspunderii sau lipsa cafelei din birou, decât protejarea datelor cu caracter personal. Conformarea la GDPR în România este de sub 15%.

Cele mai multe companii, au folosit informările cu privire la prelucrarea datelor cu caracter personal pentru a interpreta după bunul plac Regulamentul, pentru a ascunde sau a masca anumite practici pe care nu doreau să le elimine. Mai mult decât atât, au obținut viciat consimțământul persoanelor fizice, invocând scopuri legale, folosind căsuțe pre-bifate, sau folosindu-se de lipsa de informare a persoanelor fizice.

DREPTURILE PERSOANEI VIZATE	Legea nr. 677/2001	Regulamentul nr. 679/2016 (GDPR)
Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate		√
Dreptul la informare	√	√
Dreptul de acces la date	√	√
Dreptul de intervenţie asupra datelor / Dreptul la rectificare	√	√
Dreptul de opoziţie	√	√
Dreptul de a nu fi supus unei decizii individuale luate în baza unei prelucrări automate	√	√
Dreptul de a se adresa justiţiei	√	√
Dreptul la ştergerea datelor ("dreptul de a fi uitat")		√
Dreptul la restricţionarea prelucrării datelor		√
Dreptul la portabilitatea datelor		√
		cyberm.ro

chapter 19 GDPR în legislația din România

19.1 cadrul legislativ intern

Punerea în aplicare a GDPR (regulamentul UE 2016/679) este obiectul legii 190/2018, publicată în Monitorul oficial, partea I nr. 651 din 26.07.2018, intrată în vigoare pe 31.07.2018.

19.2 prevederi principale ale legii 190/2018

Legea nr. 190/2018 definește “numărul de identificare național” ca fiind acel număr prin care prin care se identifică o persoană fizică într-un anumit sistem de evidență și care are aplicabilitate generală, cum ar fi:

- codul numeric personal;
- seria și numărul actului de identitate;
- numărul pașaportului;
- numărul permisului de conducere;
- numărul de asigurare socială de sănătate.

Legea nr. 190/2018 stabilirea o serie garanții adecvate cumulative pentru prelucrarea numărului de identificare național pentru a realiza interesele legitime ale operatorului, respectiv:

- punerea în aplicare de măsuri tehnice și organizatorice în conformitate cu art. 32 din GDPR pentru respectarea principiilor de prelucrare a datelor;
- numirea unui responsabil pentru protecția datelor în condițiile legii;
- stabilirea unor termene de stocare, revizuire și ștergere în funcție de natura datelor și scopul prelucrării.
- instruirea periodică a personalului cu atribuții privind prelucrarea acestor date cu caracter personal,

atât de către operator, cât și de persoanele împuternicite de acesta pentru astfel de prelucrări.

Este de remarcat faptul că Legea nr. 190/2018 instituie un caz expres pe lângă prevederile art. 37 din GDPR pentru desemnarea obligatorie a responsabilului pentru protecția datelor, în contextul prelucrării unui număr de identificare național, atunci când această prelucrare este bazată pe interesul legitim al operatorului.

19.3 responsabilul cu protecția datelor

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în calitate de autoritate publică centrală autonomă cu competență generală în domeniul protecției datelor personale, reprezintă garantul respectării drepturilor fundamentale la viaţă privată și la protecţia datelor personale, statuate cu precădere de art. 7 și 8 din Carta Drepturilor Fundamentale a Uniunii Europene, de art. 16 din Tratatul privind Funcționarea Uniunii Europene și de art. 8 din Convenția europeană pentru apărarea drepturilor omului și libertăților fundamentale.

19.4 evidența activităților de prelucrare

Un Regulament GDPR obligă operatorii și persoanele împuternicite să țină o evidență a activităților de prelucrare, în următoarele situații:

- atunci când entitatea are mai mult de 250 angajați;
- prelucrarea este susceptibilă să genereze un risc pentru drepturile și libertățile persoanei vizate prelucrarea include categorii speciale de date;
- prelucrarea nu este ocazională.

Având în vedere că, în general, în activitatea unei firme, prelucrarea nu este ocazională, ar trebui ca fiecare organizație să aibă o evidență internă a activităților care să fie revizuită periodic.

Evidența poate fi ținută sub forma unui registru și trebuie să cuprindă:

- numele și datele de contact ale operatorului;
- descrierea activiților de prelucrare;
- scopurile prelucrării;
- categoriile de date prelucrate;
- categoriile de persoane vizate;
- categoriile de destinatari;
- transferurile internaționale de date, dacă e cazul;
- durata de stocare;
- măsurile tehnice și organizatorice luate.

19.5 acordurile dintre operator și împuternicit

GDPR este foarte clar într-o privință: trebuie să existe acorduri scrise între operatorul de date și persoana împuternicită (furnizorul care are acces la date) și stabilește ce anume trebuie să conțină acest contract. Împuternicitul trebuie să respecte termeni clari în materie de protecție a datelor, iar contractele existente trebuie actualizate cu acorduri de prelucrare. Chiar dacă nu există un contract scris între operator și furnizor, Regulament GDPR cere un contract scris în materie de protecție a datelor.

19.6 autoritățile de supraveghere

Fiecare stat membru UE are o autoritate de supraveghere independentă responsabilă, printre altele, cu monitorizarea respectării legislației în materie de protecție a datelor, efectuarea investigațiilor, aplicarea sancțiunilor și spirijinul persoanelor vizate. În România, funcționează Autoritatea Națională de Supraveghere a Prelucării Datelor cu Caracter Personal.

19.7 transferuri internaționale de date

Transferul de date ale cetățenilor europeni către state din afara UE ridică întrebări despre cât de bine pot fi protejate aceste date. RGPD nu interzice în mos expres transferurile internaționale, ci precizează că acestea pot avea loc dacă există garanții corespunzătoare, de exemplu:

- decizii adecvate;
- reguli corporatiste obligatorii;
- clauze standard.

19.8 căi de atac

Persoanele nemulțumite de modul în care organizație le prelucrează datele au drepturile de a depune o plângere la Autoritatea de supraveghere și de a se adresa instanțelor de judecată pentru obținerea despăgubirilor.

19.9 răspundere și sancțiuni

Amenda poate ajunge până la 4% din cifra de afaceri. ANSPDCP când optează între a aplica un avertisment sau o amendă, iar în cazul amenzii, cuantumul acesteia ia în calcul mai mulți factori printre care

- gradul de conformare;
- măsurile implementate;
- gravitatea abaterii;
- numărul încălcărilor;
- prejudiciile aduse persoanelor vizate și măsurile întreprinse de operator sau împuternicit pentru prevenirea limitarea prejudiciului.

19.10 exemple de sancțiuni

Vodafone Romania S.A – noiembrie – 4000 de euro sancțiune

Din informațiile primite aflăm că o persoană a depus plângere că nu i s-a oferit răspuns unor cereri de exercitare a drepturilor de acces și de ștergere. Acest lucru a fost probat pe parcursul investigației când Vodafone nu a putut face dovada solicitării acestor cereri.

DADA CREATION S.R.L. – noiembrie – 5000 euro sancțiune

A fost reclamat următorul fapt: prin website (magazin online https://botezdepoveste.ro/) operatorul a făcut publice o serie de înregistrări detaliate ale tranzacțiilor recepționate, astfel următoarele date ale clienților (persoane fizice) au fost expuse: e-mail, numere de telefon, nume și prenume clienți (persoane adulte și minori), vârstă minori, adrese de livrare, număr comandă, suma totală a comenzii, produsele comandate și data efectuării comenzii. În total vorbim de 1091 de persoane vizate (persoane fizice) ale căror date au fost divulgate și expuse unui acces neautorizat!

De ce s-a ajuns la această situație? Autoritatea ne menționează că această încălcare a securității datelor a fost posibilă datorită faptului că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării.

Unicredit Bank – iunie 2019 – 130000 euro sancțiune

În acest caz principala problemă reieșită din comunicatul Autorității din România este faptul că în situația în care o persoană efectua o plată online prin Unicredit, beneficiarul plății primea și CNP-ul și adresa plătitorului în cazul plăților spre conturi din alte bănci, respectiv adresa plătitorului în cazul plăților interne.

Aceste informații apăreau în '*documentele ce conțin detaliile tranzacțiilor şi care sunt puse on-line la dispoziţia clienţilor beneficiari ai plăţilor*' – adică în extrasele de cont/detalii.

Deși Unicredit, are categoric dreptul să colecteze CNP-urile respective, aspectele problematice au fost că:

- informațiile divulgate reprezentau o scurgere de date cu caracter personal;
- plătitorul nu a fost informat cu privire la transmiterea datelor sale spre persoanele spre care făcea plățile;
- nu s-a respectat principiul privacy by design și privacy by default în direcția conformării aplicațiilor / platformei de plăți a operatorului vizat de sancțiune. O posibilă soluție ar fi fost ca în loc să apară CNP-ul complet să apară doar ultimele 6 cifre.

ENEL ENERGIA MUNTEA S.A – martie 2020 – 3000 euro sancțiune

O situație aparte o privește comunicările electronice pe email și atenția pe care trebuie să o acordăm atunci când trimtem un email. Uneori suntem grăbiți, alteori obosiți sau pur si simplu ni se întâmplă să fim neatenți, să compunem un email și să greșim numele destinatarului sau să introducem o adresă greșită iar emailul nostru să ajungă la altcineva. Fiecăruia dintre noi ni s-a întâmplat acest lucru, însă ANSPDCP ne arată foarte clar că dacă o astfel de comunicare presupune o divulgare de date nepermisă, operatorul va fi sancționat.

Acesta este cazul operatorului Enel Energie Muntenia SA, care a fost sancționat ca urmare a unei investigații declanșate la sesizarea unui client. Clientul, vătămat în drepturile sale, depunând dovezi, adresează Autorității o plângere prin care prezintă în ce fel i s-a adus atingere drepturilor. Constatând veridicitatea lucrurilor ANSPDCP a aplicat o amendă de 3000 euro sau mai specific de 14.423,7 lei pentru că într-adevăr unul din angajații operatorului a trimis la o adresă greșită: numele și prenumele, adresa, emailul, codul de client și codul eneltel unui alt client!

Banca Transilvania S.A – noiembrie 2020 – 100000 euro sancțiune

Un client, obosit de formularistica băncii, a completat într-un mod aparte, amuzant pentru angajații băncii declarația cu privire la modul în care clientul intenționează să folosească suma împrumutată (85.000 euro).

Amuzându-se de această situație, unul din angajații băncii a distribuit-o pe emailul colegilor de serviciu. Ulterior altul dintre angajați a listat emailul care conținea această declarație dar și conversația internă între aganajații operatorului. Ul al treilea angajat a fotografiat cu telefonul mobil înscrisul listat și l-a distribuit prin aplicația WhatsApp cunoscuților. De aici, în foarte scurt timp înscrisul a fost postat și distribuit pe Facebook și pe un website.

Toată această situație a ajuns înapoi în fața clientului care s-a declarat foarte nemulțumit de situație întrucât a condus la dezvăluirea și accesul neautorizat al datelor sale cu caracter personal dar și a angajaților băncii: nume, prenume, email, date comportamentale, preferințe personale, valoarea tranzacției, adresa locului de muncă, funcție, număr de telefon.

Aflând despre incident, operatorul a luat imediat poziție cu privire la acest eveniment, însă, nu a fost suficient pentru a evita sancțiunea de 100.000 euro.

Sesizată ANSPDCP, a demarat o investigație la Banca Transilvania și a constatat că operatorul nu a luat suficiente măsuri pentru a se asiura că salariații acesteia, care au acces la date cu caracter personal nu prelucrează date decât la cererea băncii. Totodată, Autoritatea menționează că această dezvăluire produsă în spațiul public dovedește INEFICIENȚA instruirii angajaților privind respectarea normelor de protecție a datelor cu caracter personal!

chapter 20 optimizarea impactului GDPR

20.1 scopul acestei optimizări

O

20.2 principiile optimizării

Un caz tipic

20.3 cum am vrea să funcționeze

MD5 este

20.4 sugestii legislative

Valorile

Bibliografie

[DCL-DEF] – Data classification definition - https://digitalguardian.com/blog/what-data-classification-data-classification-definition

[SHA1C] - https://phys.org/news/2017-02-cwi-google-collision-industry-standard.html

[GDPR] - General Data Protection Regulation - https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=RO

[GDPR-SCURT] - GDPR pe scurt - https://legalup.ro/regulament-gdpr/

[LEGEA-119] – Legea 119/2996 - http://www.cdep.ro/pls/legis/legis_pck.htp_act?ida=8658

[LEGEA-190] – Legea 190/2018 - http://legislatie.just.ro/Public/DetaliiDocument/203151

[NORMATIVE] – ACTE NORMATIVE RELEVANTE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL -

https://anmcs.gov.ro/web/acte-normative-relevante-pentru-prelucrarea-datelor-cu-caracter-personal/