Aprobat prin Ordinul nr.16/1 din 31.03.2017
Vitalie BANARU
Director General CA„General Asigurări"SA

POLITICA

de asigurare a securităţii datelor cu caracter personal în cadrul CA„General Asigurări"SA

PREAMBUL

Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale şi mecanice de date cu caracter personal au drept scop stabilirea regulilor de implementare de către **CA„General Asigurări"SA** a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi mecanice de date cu caracter personal şi/sau registrelor ţinute manual, în conformitate cu prevederile Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal; Legii nr.71-XVI din 22 martie 2007 cu privire la registre; Hotărârii Guvernului nr.1123 din 14.12.2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal"; Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiată la Strasbourg la 28.01.1981, publicată în European Treaty Series, nr.108, ratificată de Republica Moldova prin Hotărârea Parlamentului nr. 483-XIV din 02.07.1999.

I. DISPOZIŢII GENERALE

1. În sensul prezentei Politici, se definesc următoarele noţiuni:

autentificare– verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

fişiere temporare – ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat până la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare – atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

integritate – certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal – mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

politica de securitate a datelor cu caracter personal – document, elaborat de către CA„General Asigurări"SA, care oferă o descriere generală a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinându-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sunt expuse acestea;

perimetru de securitate – zonă care reprezintă în sine o barieră de trecere asigurată cu mijloace de control tehnic al accesului;

control de securitate – acţiuni întreprinse de către deţinătorii de date cu caracter personal sau Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (Centrul) în vederea verificării şi/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute manual, în conformitate cu prezentele Cerinţe;

persoana responsabilă de politica de securitate a datelor cu caracter personal– persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei care conţine date cu caracter personal, precum şi de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

protecţia informaţiei contra acţiunilor neintenţionate – ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

purtător de date cu caracter personal – suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia;

restaurarea datelor – procedurile cu privire la reconstituirea datelor cu caracter personal în starea în care se aflau până la momentul pierderii sau distrugerii acestora;

tehnologie informaţională (TI) – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal – mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

utilizator – persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

sesiune de lucru – perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi până la momentul opririi acestora;

sistem informaţional de date cu caracter personal– totalitatea resurselor şi tehnologiilor informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caracter personal;

stocare – păstrarea pe orice fel de suport a datelor cu caracter personal;

asigurat – persoană fizică sau persoană juridică având încheiat un contract de asigurare obligatorie de răspundere civilă auto;

autoritate de supraveghere – Comisia Naţională a Pieţei Financiare;

autovehicul – sistem mecanic terestru cu autopropulsie, cu excepţia celui care circulă pe şine, pentru transportul de călători, bagaje şi mărfuri sau care execută orice alte lucrări şi servicii aferente transporturilor – autoturisme, autobuze, microautobuze, troleibuze, autocamioane, inclusiv specializate, motocicluri, tractoare;

intermediar în asigurări – persoană fizică sau persoană juridică ce desfăşoară activitate de intermediere în asigurări în schimbul unei remuneraţii şi are calitatea de broker de asigurare , agent de asigurare sau agent bancassurance;

persoană păgubită – orice persoană îndreptăţită să primească despăgubire de asigurare pentru orice pagubă sau vătămare corporală provocată în urma unui accident de autovehicul;

posesor de autovehicul – proprietarul de drept al autovehiculului, precum şi persoana care posedă autovehiculul în temeiul unui contract de locaţiune, contract de leasing sau al unor alte titluri prevăzute de legislaţie;

CERINŢE GENERALE

2. Măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemelor informaţionale de date cu caracter personal şi vor fi efectuate neîntrerupt de către persoanele responsabile angajate **al CA„General Asigurări"SA.**

3. Protecţia datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

4. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale şi mecanice de date cu caracter personal ale **CA"General Asigurări"SA** se înfăptuiesc ţinându-se cont de necesitatea asigurării confidenţialităţii acestor măsuri.

5. Sunt supuse protecţiei, toate resursele informaţionale ale **CA„General Asigurări" SA**, care conţin date cu caracter personal, inclusiv:

1) Suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;

2) Sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei.

6. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată în scopul:

a) Preîntâmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

b) Preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;

c) Respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;

d) Asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele telecomunicaţionale şi resurselor informaţionale;

e) Păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.

7. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:

1) Preîntâmpinarea conexiunilor neautorizate la reţelele informaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;

2) Excluderea accesului neautorizat la datele cu caracter personal prelucrate;

3) Preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

4) Preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor angajaţi ai deţinătorului de date cu caracter personal, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program.

5) Preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, inclusiv cu utilizarea măsurilor organizaţionale, tehnice şi de regim.

6) Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă.

8. Ordinea de acces la informaţia care conţine date cu caracter personal, prelucrată în cadrul sistemelor informaţionale, se stabileşte de **CA„General Asigurări" SA** conform Regulamentului sistemului informaţional utilizat.

POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

9. CA„General Asigurări"SA nominalizează responsabil de întocmirea, menţinerea, modificarea şi actualizarea politicii de securitate pe **<u>şeful subdiviziunii juridice din cadrul societăţii</u>** *(persoana responsabila de politica de securitate).*

10. Măsurile de securitate emise sunt stabilite conform regulamentelor de securitate ale fiecărui sistem care prelucrează date cu caracter personal. În acest sens, la **CA"General Asigurări"SA** sunt create următoarele sisteme/registre de prelucrare a datelor cu caracter personal:

a) Registru dosarelor de daună;
b) Registru de evidenţă a contractelor de asigurare/reasigurare;
c) Registru de evidenţă a corespondenţei intrare/ieşire;
d) Registru de evidenţă a petiţiilor;
e) Registru de evidenţă a litigiilor judiciare;
f) Registru de evidenţă a pretenţiilor înaintate;
g) Registru de evidenţă a agenţilor de asigurare;
h) Registru de evidenţă contabilă (Registru 1C);
i) Registru de evidenţă a angajaţilor;
j) Registru de evidenţă a angajamentelor nereflectate în bilanţul contabil;

11. Se numesc responsabili de administrarea sistemelor următoarele persoane:

a) Conducătorul Departamentului Juridic:
- *Registru de evidenţă a pretenţiilor înaintate;*
- *Registru de evidenţă a litigiilor judiciare;*
- *Registru de evidenţă a petiţiilor*

b) Conducătorul Departamentului Regularizarea Daunelor
- *Registru dosarelor de daună;*

c) Conducătorul Direcţiei Resurse Umane:
- *Registru de evidenţă a angajaţilor;*
- *Registru de evidenţă a corespondenţei intrare/ieşire;*

d) Conducătorul Departamentului Asigurări şi Underwriting:
- *Registru de evidenţă a contractelor de asigurare/reasigurare*

e) Conducătorul Departamentului Vînzări
- *Registru de evidenţă a agenţilor de asigurare*

f) Conducătorul Departamentului Financiar:
- *Registru de evidenţă contabilă (Registru 1C);*

-Registru de evidență a angajamentelor nereflectate în bilanțul contabil;

Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitor responsabilităţi cu referire la securitatea datelor cu caracter personal (prevenire, supraveghere,detectare şi prelucrare), desigur şi operarea cu ele.

12. Mecanismul de punere în aplicare a măsurilor de securitate pentru toate categoriile sistemelor informaționale de date cu caracter personal este prevăzut de prezenta Politică de Securitate.

13. În cadrul activităţii CA„General Asigurări""SA colectează şi prelucrează cu acordul subiectului de date cu caracter personal, următoarele date cu caracter personal:

1) numele şi prenumele;
2) sexul;
3) data şi locul naşterii;
4) cetăţenia;
5) IDNP;
6) datele personale ale membrilor de familie;
7) datele din permisul de conducere;
8) datele din certificatul de înmatriculare;
9) datele privind bunurile deţinute;
10) datele bancare;
11) semnătura;
12) situaţia familială;
13) situaţia militară;
14) datele din actele de stare civilă;
15) codul personal de asigurării sociale (CPAS);
16) codul asigurării medicale (CPAM);
17) numărul de telefon/fax;
18) numărul de telefon mobil;
19) adresa (domiciliului/reşedinţei);
20) adresa e-mail;
21) profesia şi/sau locul de muncă;
22) formarea profesională – diplome – studii;

14. CA„General Asigurări""SA în cadrul activității de asigurare pe care o desfășoară, utilizează şi informaţia cu privire la starea de sănătate a asiguraţilor cît şi informaţie legată de răspunderea contravenţională a persoanelor vizate. Această informaţie este necesară la instrumentarea dosarelor de daună, conform cerinţelor obligatorii stabilite în legislaţia specială din domeniul asigurărilor şi a condiţiilor de asigurare aprobate de Comisia Naţională a Pieţii Financiare. Prezenta informaţie este preluată nemijlocit de la subiectul de date cu caracter personal, care suplimentar îşi exprimă acordul pentru procesarea acestor categorii speciale de date cu caracter personal sau este preluată de la autorităţile publice de resort în urma cererilor şi demersurilor înaintate.

15. CA„General Asigurări""SA nu transmite date cu caracter personal ale asiguraţilor/beneficiarilor şi/sau ale angajaţilor în afara ţării, cu excepţia cazurilor prevăzute de lege sau expres acceptate de către aceştia.

16. CA „General Asigurări"SA asigură angajaţilor săi dreptul de acces, de stocare, de prelucrarea informaţiei ce conţine date cu caracter personal.

17. CA„General Asigurări"SA acordă accesul angajaţilor săi la prelucrarea datelor cu caracter personal, numai după ce au semnat o Declarație de Confidențialitate prin care s-au obligat

să nu divulge informaţia ce conţine date cu caracter personal obţinută în timpul exercitării atribuţiilor de serviciu. Modelul Declaraţiei de Confidenţialitate este anexat la prezenta Politică.

18. Documentaţia tehnică cu privire la controalele de securitate este ţinută sub formă de registre de către persoana responsabilă, numită prin Ordinul **CA„General Asigurări"SA** pentru fiecare sistem informaţional în parte.

19. Orarul controalelor de securitate este stabilit de către persoana numită responsabilă, în conformitate cu regulamentul de securitate al fiecărui Sistem care prelucrează date cu caracter personal.

20. Rapoartele despre incidentele de securitate sunt înregistrate în registrele respective de către persoanele responsabile. Fiecare incident urmează a fi adus la cunoştinţa conducerii **CA„General Asigurări"SA** în mod de urgenţă, pentru a putea fi identificată procedura de soluţionare a incidentului.

SECURITATEA MEDIULUI FIZIC ŞI A TEHNOLOGIILOR INFORMAŢIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Autorizarea accesului fizic

21. Accesul în sediile/oficiile/birourile ori spaţiile unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul programului de muncă.

22. Accesul se efectuează în baza permiselor de muncă eliberate tuturor angajaţilor.

23. Accesul în camera de servere este permisă doar personalului IT şi conducătorul CA„**General Asigurări**"SA. Persoanele terţe au acces în această încăpere doar sub stricta supraveghere a unui specialist IT. Toate operaţiunile de acces la servere sau alte mijloace tehnice sau software se face de către personalul IT al **CA„General Asigurări"SA.**

Administrarea şi monitorizarea accesului fizic

24. Se interzice accesul fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, cu excepţia personalului autorizat la prelucrarea informaţiei ce conţine date cu caracter personal.

25. Înainte de acordarea accesului fizic la sistemele informaţionale de date cu caracter personal se verifică competenţele de acces. Persoanele noi angajate sunt instruite în domeniul prelucrării datelor cu caracter personal şi semnează declaraţia de confidenţialitate emisă în acest sens.

26. În procesul monitorizării se utilizează mijloace de supraveghere şi alarmă în regim real de timp a tuturor cazurilor de acces autorizat şi/sau neautorizat în sediul **CA"General Asigurări"SA.**

27. Sunt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat şi iniţierea acţiunilor de blocare a accesului.

28. Toate fişele personale ale fiecărui angajat, inclusiv carnetele de muncă sunt păstrate în safeu metalic, ocrotit împotriva incendiilor.

29. Este asigurată securitatea şi accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

Securitatea sediilor/oficiilor/birourilor şi mijloacelor de prelucrare a datelor cu caracter personal

30. Perimetrul sediilor şi încăperii în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal sunt păstrate integre din punct de vedere fizic, toţi pereţii sunt întregi, uşile se încuie, iar ferestrele se închid. Se asigură că sunt clar stabilite zonele de securitate, iar mijloacele de control şi nivelul de securitate aferent fiecărei zone corespunde tipului zonei de securitate.

31. Pereţii exteriori ai încăperilor sunt rezistenţi, intrările echipate cu lacăte. Birourile amplasate la parter au ferestrele echipate cu gratii.

32. Computerele, serverele şi alte terminale de acces, în limita posibilităţii sunt amplasate în locuri cu acces limitat pentru persoane străine.

33. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii.

34. Pe timpul nopții și în zilele de odihnă sediile şi încăperile **CA„General Asigurări"SA** sunt protejate de pază particulară.

35. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

36. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii deţinătorului de date cu caracter personal.

37. Se vor implementa sisteme de constatare a intruziunilor pentru uşile exterioare şi ferestrele amplasate în locuri accesibile.

38. Utilajul de rezervă şi purtătorii de informaţii care conţin date cu caracter personal se păstrează în locuri care permit evitarea distrugerilor sau deteriorărilor ca rezultat al calamităţilor în sediul/oficiul/biroul de bază.

Controlul vizitatorilor

39. Trebuie asigurat controlul accesului fizic al vizitatorilor în încăperile unde sunt amplasate sistemele informaţionale de date cu caracter personal.

40. Vizitatorii sistemelor informaţionale de date cu caracter personal şi alte persoane care accesează sediile CA„General Asigurări"SA sunt supravegheaţi în încăperile unde aceştia au acces. În birourile cu acces interzis aceştia pot intra doar sub supravegherea personalului autorizat. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, aceşti vor fi rugaţi să părăsească încăperea în mod cît mai urgent. Incidentul va fi adus la cunoştinţa administraţiei **CA„General Asigurări"SA.**

Securitatea electroenergetică

41. Se asigură securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI. **CA„ General Asigurări"SA** va depune efortul pentru a procura surse autonome de alimentare cu energie electrică de scurtă şi lungă durată, care sunt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

Securitatea cablurilor de reţea

42. Cablurile de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, sunt protejate contra conectărilor nesancţionate sau deteriorărilor. Cablurile de tensiune sunt separate de cele comunicaţionale pentru a exclude bruiajul. Specialiştii IT al **CA„General**

Asigurări"SA efectuează controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de reţea.

Asigurarea securităţii antiincendiare a sistemelor informaţionale de date cu caracter personal

43. CA„General Asigurări"SA dispune de mijloace de asigurare a securităţii antiincendiare a sediilor/oficiilor/birourilor unde sunt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

Controlul instalării şi scoaterii componentelor TI

44. Se exercită controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaţionale de date cu caracter personal. Toate echipamentele ce conţin medii de stocare se verifică minuţios înainte de casare sau transmitere, pentru a asigura că orice date importante sau produse soft licenţiate au fost înlaturate sau suprascrise într-un mod ce să asigure irecuperabilitatea lor.

Măsurile generale de administrare a securităţii informaţionale

45. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie. Computerele, terminalele de acces şi imprimantele sunt deconectate la terminarea sesiunilor de lucru. Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere. Accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis şi controlat. Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a Directorului General **CA„General Asigurări"SA**. Schimbul de informaţie dintr-o entitate şi terţele părţi se efectuează în baza unui acord semnat, ce să includă mijloacele, cerinţele şi responsabilităţile aferente securităţii informaţiei.

IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

Identificarea şi autentificarea utilizatorului

46. Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. În cazul în care a fost depusă cererea de demisie, în cazul cînd contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare şi autentificare se revocă în mod automat în decursul a două săptămîni de la ultimul acces, sau în mod individual imediat la momentul introducerii modificării în raportul de muncă.

47. Se utilizează autentificarea multifactorială, care include parole complexe, cu includerea simbolurilor, literelor, cifrelor în combinaţie complexă. În mod obligatoriu fiecare parolă conţine

una sau mai multe litere scrise cu majusculă. Parola nu va conţine iniţialele sau date care pot caracteriza o anumită persoană (data de naştere, adresă etc).

Identificarea şi autentificarea echipamentului

48. Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal.

Administrarea identificatorilor utilizatorilor

49. Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;

2) verificarea autenticităţii fiecărui utilizator;

3) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declaraţiei de confidenţialitate şi trecerii procedurii de instruire;

4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;

5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (2 săptămîni);

6) executarea copiilor de arhivă a ID-urilor utilizatorilor.

Asigurarea conexiunii bilaterale în cazul introducerii informaţiei de autentificare a utilizatorilor

50. Se asigură conexiunea bilaterală a **CA„General Asigurări"SA** cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

Utilizarea parolelor în procesul asigurării securităţii informaţionale

51. Se respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

1) păstrarea confidenţialităţii parolelor;

2) modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;

3) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sunt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sunt compuse integral din grupuri de cifre sau litere;

4) modificarea parolelor peste intervale de maximum 6 luni;

5) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

Administrarea parolelor utilizatorilor

52. Se folosesc identificatoare individuale pentru fiecare utilizator şi parole individuale ale acestora pentru asigurarea posibilităţii de stabilire a responsabilităţii. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. Se asigură blocarea accesului după trei tentative greşite de autentificare. Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioada de un an) şi prevenirea folosirii repetate a acestora. La momentul introducerii, parolele nu se reflectă în clar pe monitor. Parolele se păstrează în formă cifrată, utilizându-se algoritmul criptografic unilateral (funcţia hash).

ADMINISTRAREA ACCESULUI UTILIZATORILOR

Administrarea accesului

53. Se implementează mecanisme de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

Administrarea conturilor de acces (accounturilor)

54. Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Sunt folosite mijloace automatizate de suport în scopul administrării conturilor de acces. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (180 zile de inactivitate a contului). Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

Acordarea accesului

55. Este autorizat accesul la sistemele informaţionale de date cu caracter personal în conformitate cu prezenta Politică de securitate de către persoanele numite la pct. 11 şi 12.

Revizuirea drepturilor de acces ale utilizatorilor

56. Drepturile de acces ale utilizatorilor la sistemele informaţionale de date cu caracter personal sunt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) şi după oricare schimbare de statut al utilizatorului.

Repartizarea obligaţiilor şi învestirea cu minimul de drepturi şi competenţe

57. Repartizarea obligaţiilor subiecţilor care asigură funcţionarea sistemelor informaţionale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competenţe corespunzătoare de acces, prin ordinul Directorului General al **CA„General Asigurări"SA** întocmit în acest sens. Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/competenţe, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

Informaţii de avertizare

58. Înainte de acordarea accesului în sistem, utilizatorii sunt informaţi despre faptul că folosirea sistemelor informaţionale de date cu caracter personal este controlată şi că folosirea neautorizată a acestora se urmăreşte în conformitate cu legislaţia.

Blocarea sesiunii de lucru

59. Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează automat, după maxim 10 minute de perioadă inactivă a utilizatorului fapt care face imposibil accesul de mai departe până în momentul când utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

Controlul administrării accesului

60. Se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Marcarea documentelor

61. Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicându-se prescripţii pentru prelucrarea ulterioară şi răspândirea acesteia, inclusiv indicându-se numărul de identificare unic al deţinătorului de date cu caracter personal.

Accesul de la distanţă

62. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum şi sunt documentate, supuse monitorizării şi controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de **CA„General asigurări"SA** şi este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Limitarea folosirii tehnologiilor fără fir

63. Accesul fără fir la sistemele informaţionale de date cu caracter personal este documentat, supus monitorizării şi controlului. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar cu acordul Directorul General al **CA„General Asigurări"SA** prin coordonarea cu personalul IT.

Administrarea accesului echipamentului portativ şi mobil

64. Accesul la sistemele informaţionale de date cu caracter personal cu folosirea echipamentului portativ şi mobil se documentează, este monitorizat şi controlat. Folosirea echipamentului portativ şi mobil este autorizată de Directorul General al **CA„General Asigurări"SA** prin coordonare cu Serviciul Tehnologii Informaţionale.

PROTECŢIA SISTEMELOR INFORMAŢIONALE ŞI COMUNICAŢIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

Divizarea programelor aplicative

65. Se asigură separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale de date cu caracter personal.

Informaţia restantă

66. Sunt preîntâmpinate tentativele dezvăluirii neautorizate sau neintenţionate a informaţiei restante care conţine date cu caracter personal, prin intermediul resurselor informaţionale general accesibile.

Priorităţile resurselor

67. Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sunt prelucrate date cu caracter personal.

Protecţia perimetrului sistemelor informaţionale în care sunt prelucrate date cu caracter personal

68. Se efectuează monitorizarea permanentă şi controlul comunicaţiilor la perimetrul exterior al sistemelor informaţionale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaţionale.

Amplasarea resurselor general accesibile se asigură în spaţiile special destinate a reţelei de calcul cu interfeţele fizice de reţea.

Este asigurată imposibilitatea accesului din exterior a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal.

Asigurarea integrităţii şi confidenţialităţii datelor cu caracter personal transmise

69. Se asigură integritatea şi confidenţialitatea datelor cu caracter personal transmise, utilizându-se mijloacele de protecţie criptografică.Transmiterea sau expedierea componentelor şi modulelor soft pe cale electronică se efectuează în baza acordurilor semnate, care vor stabili şi mijloacele de producţie necesare a fi implimentate în scopul asigurării cofidenţialităţii, integrităţii, autenticităţii mesajelor şi fişierelor recepţionate.

AUDITUL SECURITĂŢII ÎN SISTEMELE INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

70. Responsabilul fiecărui sistem informaţional este obligat să întocmească următoarele proceduri obligatorii de audit al sistemului:

1) Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:

a) data şi timpul tentativei intrării/ieşirii;

b) ID-ul utilizatorului;

c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.

2) Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:

a) data şi timpul tentativei de pornire;

b) denumirea/identificatorul programului aplicativ sau procesului;

c) ID-ul utilizatorului;

d) rezultatul tentativei de pornire – pozitivă sau negativă.

3) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

a) data şi timpul tentativei de obţinere a accesului (executare a operaţiunii);

b) denumirea (identificatorul) aplicaţiei sau procesului;

c) ID-ul utilizatorului;

d) specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);

e) tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.);

f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

4) Se efectuează înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi

statutului obiectelor de acces, conform următorilor parametri:

a) data şi timpul modificării competenţelor;

b) ID-ul administratorului care a efectuat modificările;

c) ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

71. În caz de deranjament al auditului securităţii în sistemele informaţionale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal şi întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

72. Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobişnuite

sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul.

73. Rezultatele auditului securităţii în sistemele informaţionale de date cu caracter personal, care reprezintă operaţiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidenţialităţii şi integrităţii acestora.

74. Durata stocării rezultatelor auditului securităţii în sistemele informaţionale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de 1 an, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigaţii sau procese judiciare.

ASIGURAREA INTEGRITĂŢII INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAŢIONALE

Înlăturarea deficienţelor de soft destinat prelucrării datelor cu caracter personal

75. Se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri.

Asigurarea protecţiei contra programelor dăunătoare (virusilor)

76. Se asigură protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus.

77. Se asigură administrarea centralizată a mecanismelor de protecţie contra programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal.

Tehnologiile şi mijloacele de constatare a intruziunilor

78. Se vor utilizează tehnologii şi mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaţionale de date cu caracter personal şi constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaţionale.

Asigurarea integrităţii soft-urilor şi informaţiei

79. Se asigură protecţia şi posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal şi informaţiei care conţine date cu caracter personal.

Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

80. Se asigură testarea funcţionării corecte a funcţiilor de securitate a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI IT

Copiile de rezervă ale informaţiei care conţine date cu caracter personal

81. Copiile de siguranţă a informaţiilor care conţin date cu caracter personal şi soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate odată la 24 ore, fiind păstrate cel puţin 3 ani în locuri sigure, cu acces limitat (safeu).

Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei care conţine date cu caracter personal.

Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

Instructajul de reacţionare la incidentele de securitate a sistemelor informaţionale de date cu caracter personal

82. Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal va trece, de regulă o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

83. În cazul depistării unui incident de securitate, este asigurat mecanismul de informare neîntârziată a Directorului General a **CA„General Asigurări"SA.**

84. Prelucrarea incidentelor include în mod obligatoriu depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii iniţiale, precum şi crearea unor mecanisme de evitare a ulterioarelor incidente asemănătoare.

85. Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent.

Anexe:

1. Modelul Declaraţiei de Confidenţialitate;
2. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de Daune în cadrul **CA„General asigurări"SA;**
3. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a pretenţiilor înaintate în cadrul **CA„General asigurări"SA;**
4. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a Litigiilor Judiciare în cadrul **CA„General Asigurări"SA;**
5. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a contractelor de asigurare/reasigurare în cadrul **CA„General Asigurări"SA;**
6. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a agenţilor de asigurare în cadrul **CA„General Asigurări"SA;**
7. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a angajaţilor în cadrul **CA„General Asigurări"SA;**
8. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a corespondenţei intrare/ieşire în cadrul **CA„General Asigurări"SA;**
9. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a petiţiilor în cadrul **CA„General Asigurări"SA;**
10. Regulamentul cu privire la asigurarea securităţii datelor cu caracter personal din Registru de evidenţă contabilă în cadrul **CA„General Asigurări"SA;**
11. Regulamentul cu privire de asigurarea securităţii datelor cu caracter personal din Registru de evidenţă a angajamentelor nereflectate în bilanţul contabil în cadrul **CA„General Asigurări"SA;**