POLITICA DE SECURITATE
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL SI PRELUCRAREA ACESTORA IN CADRUL CENTRULUI DE EXCELENȚĂ ÎN ADMINISTRAREA AFACERILOR

	ELABORAT	COORDONAT și VERIFICAT	APROBAT
Responsabil	Djulieta Prodan	Liliana Dandara	Liliana Dandara, director al CEAA, conf. univ., dr.
Data	21.08.2020	23.08.2020	Proces-verbal nr. 1 al Consiliului Profesoral CEAA din 28.08.2020
Semnătura			

I. DISPOZIŢII GENERALE

Prezenta Politică de securitate privind protecția datelor cu caracter personal și prelucrarea acestora în cadrul Centrului de Excelență în Administrarea Afacerilor (în continuare CEAA) este elaborată în conformitate cu prevederile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal și reglementează modul de colectare și utilizare acestor date, precum și condițiile de utilizare a informației în cadrul CEAA.

Reglementările prezentei Politici reprezintă un standard minim pentru CEAA, inclusiv toți angajații CEAA. Pornind de la aceasta reglementare, toți angajații CEAA urmează sa respecte strict prevederile Politicii și regulilor interne ale CEAA privind protecția datelor cu caracter personal și sistemelor IT.

I. OBIECTIVE MAJORE

Politica de securitate are ca scop primordial asigurarea integrității, disponibilității și confidențialității informației.

Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului informațional (SI). Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a SI.

Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat. Utilizatorul răspunde personal de asigurarea confidențialității datelor încredințate prin procedurile de acces la SI.

Prezenta Politică de securitate are ca scop, de asemenea, stabilirea cadrului normativ necesar pentru elaborarea regulamentelor şi procedurilor de securitate în cadrul CEAA. Acestea sânt obligatorii pentru toți utilizatorii SI.

III. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

1. Datele cu caracter personal sunt prelucrate cu buna-credință și în conformitate cu dispozițiile legale în vigoare.
2. Datele cu caracter personal sunt colectate numai în scopuri determinate, explicite și legitime, iar prelucrarea ulterioară nu va fi incompatibilă cu aceste scopuri.
3. Datele cu caracter personal care fac obiectul prelucrării sunt adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate.
4. Datele cu caracter personal care fac obiectul prelucrării sunt exacte și, dacă este cazul, actualizate.
5. Datele cu caracter personal nu se stochează pentru o perioadă mai lungă decât este necesar pentru realizarea scopurilor în care au fost colectate.
6. Datele cu caracter personal se prelucrează în conformitate cu drepturile persoanei vizate prevăzute de Legea privind protecția datelor cu caracter personal Nr. 133 din 8 iulie 2011.
7. Asigurarea și păstrarea confidențialității datelor cu caracter personal se efectuează în conformitate cu prevederile legislației în vigoare și ale părților semnatare în contracte.
8. Datele inexacte sau incomplete din punct de vedere al scopului în care sunt colectate și pentru care vor fi prelucrate vor fi șterse sau rectificate.

9. Asigurarea măsurilor tehnice şi organizatorice (procedurale) adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat.

IV. METODE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL

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

- preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate; preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
- preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
- 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, precum şi utilizarea canalelor VPN;
- 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;
- preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;
- stabilirea exactă a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenţă instituite atât pentru utilizatorii interni cit şi pentru cei externi.

V. PROCEDURI ORGANIZATORICE ŞI TEHNICE CARE URMEAZĂ A FI RESPECTATE ÎN CADRUL UCCM LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

1. Proceduri generale de administrare a securităţii informaţionale

a) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.

b) Computerele, terminalele de acces şi imprimantele sânt deconectate la terminarea sesiunilor de lucru.

c) Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.

d) 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.

e) Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sânt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.

2. Securitatea mediului fizic şi a tehnologiilor informaţionale folosite în procesul prelucrării datelor cu caracter personal

a) Accesul în sediile/oficiile/birourile ori spaţiile unde sânt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară, conform listei autorizate de conducerea CEAA.

b) Se asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal.

c) Perimetrul de securitate al CEAA reprezintă spaţiile oficiilor în care se prelucrează/stochează date cu caracter personal.

d) Perimetrul clădirii sau încăperilor în care sânt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sânt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare.

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

f) Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii.

g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

h) Accesul cu utilaje foto/video neautorizate este interzis în perimetrul de securitate a clădirii UCCM unde se prelucrează/stochează date cu caracter personal, ţinînd cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de art.29 şi art. 30 ale Legii privind protecţia datelor cu caracter personal, precum şi pct. 26 din Cerinţe.

i) Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezentei unei permisiuni speciale a conducerii CEAA.

3. Identificarea şi autentificarea utilizatorilor

a) Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.

b) Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, personalul CTIC) au un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele nivelului de accesibilitate al utilizatorului.

c) Pentru confirmarea ID-ului utilizatorului sînt utilizate parole.

d) În cazul în care 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 sau se suspendă de către CTIC din cadrul CEAA.

4. Identificarea şi autentificarea echipamentului

Echipamentele tehnice, inclusiv cele folosite în operaţiunile de prelucrare a datelor cu caracter personal sînt identificate şi autentificate prin număr de inventariere.

5. Administrarea identificatorilor utilizatorilor include
- identificarea univocă a fiecărui utilizator,
- verificarea autenticităţii fiecărui utilizator.

6. Utilizarea parolelor în procesul asigurării securităţii informaţionale

Sunt respectate regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:
- păstrarea confidenţialităţii parolelor;
- interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;
- alegerea parolelor calitative cu o mărime de minimum 5-8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere;
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7. Controlul administrării accesului

Controlul sistematic al acţiunilor utilizatorilor în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal este efectuat de către personalul CTIC.

8. Accesul de la distanta

a) Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se criptarea, cifrarea etc.), precum şi sânt documentate, supuse monitorizării şi controlului.

b) Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale CEAA şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

9. Securitatea electroenergetică

a) Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.

b) 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.

10. Controlul instalării şi scoaterii componentelor T.I.

a) 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 este exercitat de către CTIC.

b) La expirarea perioadei de valabilitate, informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcţiilor standarde de nimicire.

11. Dezvăluirea datelor cu caracter personal

a) Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. În cazul în care reţelele comunicaţionale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmânarea personală, etc.).

b) Este interzisă dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor (spre exemplu: expedierea informaţiei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.).

c) Volumul şi categoriile datelor cu caracter personal colectate în scopul ţinerii evidenţei UCCM, este limitat la strictul necesar pentru realizarea scopurilor declarate.

d) Acces la sistemele informaţionale gestionate în cadrul CEAA, din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 Cod de procedură penală.

12. Drepturile subiecţilor de date cu caracter personal

a) În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecţia datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informaţii, exceptînd cazul în care el deţine deja informaţiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidenţă al operatorilor de date cu caracter personal);
- privind scopul concret al prelucrării datelor cu caracter personal colectate;
- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existenţa drepturilor la informare şi de acces la datele colectate; de intervenţie asupra datelor (în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate;

b) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine.

c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităţile ce asigură mentenaţa sistemului şi sau prestează servicii externalizate ale operatorului) tuturor persoanelor supuse prelucrării.

d) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenţie, datele inexacte vor fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (acte de identitate, de stare civilă, resurse informaţionale principale de stat etc.), modificarea urmînd a fi efectuată în toate sistemele informaţionale şi de evidenţă gestionate.

13. Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate

a) Accesul în spaţiile/perimetrul unde sînt amplasate sistemele informaţionale şi de evidenţă a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia

necesară conform politicii de securitate respective, ordinului şi alte acte aprobate de conducerea UCCM cu privire la reglementarea protecţiei datelor cu caracter personal.

b) Este interzisă stocarea şi păstrarea formatului electronic al datelor cu caracter personal în computere care sînt conectate la internet şi nu sînt echipate cu mijloace de protecţie speciale tehnice şi de program, precum şi nu au instalate programe antivirus licenţiate, sisteme de control al securităţii soft-ului.

c) Este interzisă introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu. Mai mult, accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredinţate doar persoanelor din cadrul CTIC.

d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie 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, este asigurată prin plasarea acestora în safeuri sau dulapuri care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

14. Auditul sistemelor informaţionale gestionate

a) Înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri se efectuează astfel:

- data şi timpul tentativei intrării/ieşirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

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

- data şi timpul tentativei de obţinere a accesului (executate a operaţiunii),
- denumirea (identificatorul) aplicaţiei sau procesului, ID-ul utilizatorului,
- specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.),
- tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.),
- rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

c) Înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces, este efectuată conform următorilor parametri:

- data şi timpul modificării competenţelor,
- ID-ul administratorului care a efectuat modificările,
- ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

d) Înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, se efectuează conform următorilor parametri:

- data şi timpul eliberării;
- denumirea informaţiei şi căile de acces la aceasta;
- specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic);
- ID-ul utilizatorului, care a solicitat informaţia.

15. Asigurarea protecţiei contra programelor dăunătoare (viruşilor)

Protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal este asigurată prin existența programelor licențiate anti-virus.

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

Testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal se asigură de către personalul CTIC.

17. Gestionarea incidentelor de securitate

a) Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacționare la incidentele de securitate.

b) Personalul CEAA informează neîntârziat conducerea despre incidentele privind securitatea sistemelor informaționale de date cu caracter personal.

c) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securității.

18. Marcarea documentelor

Toată informația care se intenționează a fi dezvăluită, şi care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.

19. Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum şi a informațiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, semnatari a anexei nr. 1, pentru nerespectarea dispozițiilor prezentei Politici de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 741 Cod contravențional) şi penală (art.art. 177, 178, 180 Cod penal).

VI. MIJLOACE DE PROTECŢIE A DATELOR CU CARACTER PERSONAL

Protecția datelor cu caracter personal în cadrul UCCM este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Sânt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate:

- pe suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale şi baze de date;
- în sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date şi alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informației.

ANEXA 1

Subsemnat (ul/a), _____,
născut (ă) la data de _____,
cu domiciliul în _____,
angajat (ă) al(a) _____,
în funcția de _____,

declar pe propria răspundere că am luat cunoștință de prevederile legale referitoare la protecția datelor cu caracter personal și consimt să păstrez confidențialitatea datelor cu caracter personal a căror prelucrare o efectuez în condițiile legii, în virtutea atribuțiilor de serviciu, inclusiv și după încetarea activităților de prelucrare a acestor date.

Cunosc faptul că încălcarea normelor legale privind protecția datelor cu caracter personal atrage răspundere administrativă, disciplinară, materială, civilă ori penală, în raport cu gravitatea faptei, potrivit legii.

Data _____
Numele, Prenumele, Patronimicul _____
Semnătura _____