INSTITUȚIA PRIVATĂ DE ÎNVĂȚĂMÂNT SUPERIOR „UNIVERSITATEA AMERICANĂ DIN MOLDOVA”

REGULAMENTUL

REGULAMENTUL
PRIVIND PRELUCRAREA INFORMAȚIILOR CE CONȚIN DATE CU CARACTER PERSONAL ÎN SISTEMUL DE EVIDENȚĂ PRIVIND STUDENȚII

APROBAT
de Senatul Universității Americane din Moldova
proces verbal nr.3 din 15 decembrie 2020
Președintele Senatului UAM,
Dr., hab., prof.,univ. AVORNIC Gheorghe

CHIȘINĂU 2020

I. DISPOZIŢII GENERALE

I.1. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în sistemul de evidență privind Studenții/Masteranzii/Doctoranzii (în continuare Regulament) este elaborat în vederea implementării în cadrul IPÎS "Universitatea Americană din Moldova" (în continuare "Operator") a prevederilor:

- Legii nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal
- Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010,
- Regulamentului (UE) nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulatie a acestor date,

I.2. Prezentul Regulament stabilește condițiile generale și cerințele față de prelucrarea datelor cu caracter personal ale subiecților sau altor persoane vizate în cadrul procesului educațional.

I.3. Sistemul de evidenta va fi notificat Centrului Național pentru Protecția Datelor cu Caracter Personal (în continuare CNPDCP) pentru examinarea corespunderii acestuia cu exigențele legale stabilite în Legea privind protecția datelor cu caracter personal. La notificarea către CNPDCP va fi anexat și prezentul Regulament.

I.4. Regulamentul va intra în vigoare în momentul emiterii aprobării acestuia de către conducătorul unității.

I.5. Regulamentul constituie o parte integrantă a Politicii de securitate la prelucrarea datelor cu caracter personal în cadrul Operatorului și reprezintă actul regulator secundar care stabilește măsurile necesare pentru prelucrarea datelor cu caracter personal ale studenților/masteranzilor/doctoranzilor (în continuare "subiecților").

I.6. Prezentul Regulament se aplică tuturor operațiunilor de prelucrare a datelor cu caracter personal efectuate de Operator în format electronic, manual sau mixt, indiferent de soluțiile software și suporturile hardware utilizate.

1.7 Prin operator se înțelege IPÎS "Universitatea Americană din Moldova" , IDNO 1002600041457, cu adresa fizică: mun. Chișinău, bd. Ștefan cel Mare și Sfînt, 200, înregistrat la CNPDCP cu nr. 0003264.

II. SCOPUL PRELUCRĂRII, CATEGORII DE DATE PRELUCRATE ȘI DESTINATARII

2.1. Prelucrarea datelor cu caracter personal în sistemul de evidență constă în asigurarea obținerii, păstrării, prelucrării, transmiterii și distrugerii conform legislației în vigoare a datelor cu caracter personal ale Subiecților.

2.2. În cadrul sistemului de evidență sunt prelucrate următoarele date personale

- Numele, prenumele
- Nr. de contact (telefon/mobil/fix)
- E-mail
- Domiciliu
- Semnătura
- Cetățenia
- IDNP
- Data nașterii
- Imaginea
- Situația familială
- Situația militară
- Date bancare
- Datele personale ale membrilor de familie
- Codul asigurării medicale (CPAM)
- Datele din certificatele medicale
- Originea etnică
- Datele reprezentantului legal (după caz)
- Formare profesională – diplome – studii
- Locul de muncă și/sau profesia
- Alte date necesare pentru realizarea scopurilor indicate în prezentul regulament, conform legislației în vigoare.

2.3. Principalele operațiuni/seturi de operațiuni de prelucrare pot consta în:

- colectarea sau înregistrarea și organizarea datelor cu caracter personal
- stocarea, respectiv păstrarea pe orice fel de suport a datelor cu caracter personal colectate
- adaptarea ori modificarea sau utilizarea acestora
- extragerea datelor cu caracter personal
- consultarea datelor cu caracter personal
- dezvăluirea către terți prin transmitere, diseminare sau in orice alt mod

- blocarea, ştergerea sau distrugerea datelor cu caracter personal.

2.4. Datele cu caracter personal vor fi prelucrate pentru realizarea următoarelor scopuri:

- Desfăşurarea etapelor premergătoare procesului de înmatriculare
- Înmatricularea subiecţilor
- elaborarea/înregistrare/eliberarea şi prelucrarea diferitor tipuri de acte, ce vizează subiecţii
- Comunicarea către CNAM şi CMT a evidenţei nominale a noilor subiecţi înmatriculaţi, cît şi a celor exmatriculaţi.
- Completarea rapoartelor statistice
- Ţinerea dosarelor personale ale subiecţilor
- Întocmirea documentelor universitare (contract, acorduri adiţionale, cataloage, carnete elevi, note);
- Întocmirea şi eliberarea actelor de studii (diplome, certificate, foi matricole);
- Eliberarea unor documente solicitate (adeverinţa student, adeverinţe de studii);
- Întocmirea situaţiilor universitare;
- Fotografierii sau înregistrării audio sau video în timpul activităţii universitare în scopuri didactice şi/sau în scopul promovării şi popularizării imaginii Universităţii;
- Reducerii taxelor de studii;
- Siguranţa studenţilor/masteranţilor/doctoranţilor şi a bunurilor acestora pe timpul derulării cursurilor (prin sistem de supraveghere video a holurilor şi a curţii universităţii);
- alte scopuri, necesare pentru executarea contractului, obligaţiilor legale sau a intereselor legitime ce-i revin operatorului.

2.5. Orice utilizare a datelor cu caracter personal, introduse în prezentul sistem de evidenţă în alte scopuri decît cele menţionate mai sus este interzisă, decît dacă există un temei în acest sens, ce justifică acest fapt.

2.6. Necomunicarea categoriilor de date cu caracter personal enunţate mai sus, poate duce la imposibilitatea realizării unor drepturi sau obligaţii ce-i revin Operatorului

2.7. Operatorul poate dezvălui datele cu caracter personal către:

- subiectul de date sau reprezentantul său legal;
- organele de control/autorităţilor de stat la solicitarea motivată a acestora;

2.8. Transmiterea datelor cu caracter personal către alte persoane terţe este interzisă.

III. COLECTAREA ŞI PRELUCRAREA DATELOR CU CARACTER PERSONAL ALE SUBIECŢILOR

3.1. Datele cu caracter personal pot fi colectate şi prelucrate în temeiul contractului, interesului legitim şi/sau consimţământului subiectului de date sau în baza unor prevederi legale.

3.2. Datele cu caracter personal sunt prelucrate de către operatorul de date în mod mixt. Datele cu caracter personal prelucrate manual se referă la datele care pot fi colectate şi ulterior prelucrate pe suport de hîrtie prin completarea unor formulare.

3.3. Operatorul va prelucra datele cu caracter personal mixt, cu excepţia situaţiilor în care subiectul datelor îşi va manifesta dreptul de a nu fi supus unei decizii individuale sau a dreptului de opoziţie.

3.4. În scopul încheierii contractului sau executării acestuia, la cererea subiectului de date, în calitate de temei pentru prelucrarea datelor cu caracter personal serveşte raportul juridic declanşat sau încheiat.

3.5. Operatorul informează că datele personale pot fi utilizate şi în alte scopuri prevăzute expres de lege, cum ar fi: la solicitarea organelor de poliţie sau organelor cu funcţie de control - activităţi pe care operatorul de date nu le poate anticipa, însă le ia în considerare la colectarea datelor cu caracter personal. În cazul unor astfel de situaţii, operatorul de date va verifica corespunderea solicitării sub aspect de respectare a principiilor de protecţie a datelor cu caracter personal şi le va executa doar în cazul justificării existenţei scopului şi temeiului legal.

3.6. Încheierea contractelor cu subiecţii – persoane fizice se efectuează de către angajaţii Operatorului, ulterior fiind introduse în resursa informaţională utilizată de Operator, la care acesta are acces unic.

3.7. Prelucrarea datelor cu caracter personal în prezentul sistem de evidenţă se efectuează pe următoarele perioade:

- Pentru perioada executării contractului, din momentul colectării/obţinerii datelor cu caracter personal pînă la încetarea raporturilor contractuale.
- În cazul în care normele legale prevăd alte termene de stocare (Ordinul nr. 57 din 27.07.2016 al Agenţiei Naţionale de Arhivă privind Indicatorul documentelor-tip şi al termenelor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile RM sau de alte acte legale aplicabile (după caz).

3.8. În cazul în care, datele personale sunt prelucrate pentru realizarea unor interese legitime sau a unor obligaţii legale ale Operatorului, datele personale vor fi prelucrate pe durata perioadei de timp necesare pentru realizarea acestora.

3.9. În format electronic, datele subiecţilor cu ajutorul bazei de date creată prin intermediul softului Microsoft SQL pe platforma Microsoft Server 2008R2, serverele de stocare a datelor fiind localizate în biroul departamentului Contabilitate, accesul fiind restricţionat.

3.10. După realizarea scopurilor legitime de prelucrare şi stocare şi după expirarea perioadei legale pentru arhivarea datelor/documentelor care conţin date cu caracter personal, dacă persoana vizată nu

și-a dat consimțământul pentru o procesare viitoare și nu este aplicabilă vreuna din excepțiile prevăzute de legislația privind protecția datelor, se va proceda după cum urmează:

- datele cu caracter personal din sistemele de evidențe/aplicații IT vor fi șterse sau
- datele cu caracter personal din sistemele de evidente/aplicații IT vor fi transformate în date anonime
- datele existente în documente pe suport de hartie vor fi distruse cu shreidere, special destinate documentelor clasificate ca documente confidențiale/restricționate.

PRINCIPIILE PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

4.1. Operatorul are obligația de a respecta principiile legale de prelucrare a datelor cu caracter personal prevăzute de legislația privind protecția datelor, după cum este detaliat mai jos.

4.2. **Principiul legitimității prelucrării datelor cu caracter personal**

Acesta stabilește în sarcina Operatorului, a salariaților și colaboratorilor săi următoarele obligații:

IV.2.1. Datele cu caracter personal vor fi prelucrate în mod corect și cu respectarea legii

IV.2.2. Datele cu caracter personal vor fi prelucrate numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare, sau în situația aplicabilității uneia dintre excepțiile sus-menționate

IV.2.3. Datele cu caracter personal se vor obține numai pentru unul sau mai multe scopuri specifice și nu vor fi prelucrate într-un mod care nu este în concordanță cu respectivele scopuri.

Prelucrarea în scopuri ulterior identificate este permisă numai în situațiile în care intră în categoria celor pentru care nu este necesar consimțământul, sub condiția realizării unei informări prealabile a persoanelor vizate.

4.3. Principiul transparenței prelucrării datelor cu caracter personal

Persoana vizată va fi informata în prealabil cu privire la datele cu caracter personal care urmează a fi prelucrate, scopul prelucrării și temeiul juridic al acestuia, identitatea operatorului, interesul legitim urmărit de operator prin prelucrarea datelor cu caracter personal, dacă este cazul, destinatarii sau categoriile de destinatari ai datelor, dacă este cazul, intenția Operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională, dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza, perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă, existența unui proces decizional automatizat incluzând crearea de profiluri precum și, cel puțin în cazurile respective, informații privind logica utilizată, importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată, drepturile persoanei vizate prevăzute de legislația din domeniul protecției datelor precum

și condițiile în care pot fi exercitate, respectiv cu privire la orice alte informații specifice scopului de prelucrare propriu-zis.

Ori de cîte ori, persoana vizată, ale cărei date sunt prelucrate va solicita informații cu privire la prelucrarea datelor sale, departamentul care primește o asemenea solicitare va cere punct de vedere de la Responsabilul cu protecția datelor. Operatorul are obligația de a răspunde cererilor mai sus menționate in cel mult 30 de zile din momentul primirii acestora, în conformitate cu prevederile legislației privind protecția datelor.

4.4. Principiul proporționalității prelucrării datelor cu caracter personal

Operatorul prelucrează datele cu caracter personal în mod rezonabil, relevant față de scopul procesării și neexcesiv, limitat la ceea ce este necesar în raport cu scopurile legitime în care datele sunt prelucrate.

Înainte de procesarea datelor cu caracter personal, Operatorul, prin departamentele relevante, cu avizul Responsabilului cu protecția datelor, determină dacă și în ce măsură procesarea datelor cu caracter personal este necesară pentru atingerea scopului în vederea căruia au fost colectate.

4.5. Principiul ștergerii datelor după expirarea perioadei legale de deținere

În ceea ce privește perioada de arhivare a datelor cu caracter personal, acestea vor fi stocate în sistemele Operatorului pentru îndeplinirea scopurilor legitime urmărite prin prelucrare, pentru o perioadă necesară scopului prelucrării sau pentru perioada prevăzută de legislația aplicabilă, pentru fiecare categorie de date cu caracter personal în parte. Durata de stocare este stabilită pentru fiecare operațiune identificată, avînd în vedere dispozițiile legale obligatorii.

Operatorul are obligația de a păstra dovada existenței consimțământului exprimat de subiecți, în cazul în care prelucrarea datelor lor personale este efectuată în baza consimțământului acestora.

După realizarea scopurilor legitime de prelucrare și stocare și după expirarea perioadei legale pentru arhivarea datelor/documentelor care conțin date cu caracter personal, dacă persoana vizată nu și-a dat consimțământul pentru o procesare viitoare si nu este aplicabilă vreuna din excepțiile prevăzute de legislația privind protecția datelor, se va proceda după cum urmează:

- datele cu caracter personal din sistemele de evidențe/aplicații IT vor fi șterse sau
- datele cu caracter personal din sistemele de evidente/aplicații IT vor fi transformate în date anonime
- datele existente în documente pe suport de hartie vor fi distruse cu tocatoare special destinate documentelor clasificate ca documente confidențiale/restricționate.

4.6. Principiul exactității prelucrării datelor cu caracter personal

Datele cu caracter personal vor fi exacte și, dacă este necesar, actualizate. Operatorul adoptă măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, sunt șterse sau rectificate fără întârziere în conformitate cu scopul legitim al prelucrării.

4.7. **Principiul confidențialității datelor cu caracter personal și principiul necesității de cunoaștere a datelor („need to know")**

Operatorul adoptă măsurile tehnico-organizatorice necesare pentru asigurarea securității adecvate a datelor cu caracter personal, pentru a preveni accesul neautorizat, prelucrarea ilegală, dezvăluirea neautorizată inclusiv pierderea, distrugerea, sau deteriorarea accidentală a acestora. Detalii despre cerințele minime de securitate sunt menționate și în secțiunile următoare.

Accesul angajaților/partenerilor Operatorului la datele cu caracter personal prelucrate de către Operator, respectiv stocate în sistemele informatice ale Operatorului se acordă numai pe baza criteriului „necesității de a cunoaște". Trebuie să existe un proces de autorizare și aprobare documentată pentru a acorda, menține și înlătura accesul la informațiile care sunt date cu caracter personal. Astfel, pentru acordarea drepturilor de acces al unor subiecți, aceștia vor depune o cerere în adresa secției studii în acest sens

4.8. Principiul responsabilității în realizarea prelucrării datelor cu caracter personal

Operatorul asigură respectarea principiilor legale de protecție a datelor cu caracter personal atât pentru prelucrările de date realizate în mod direct, asigurînd includerea clauzelor contractuale prevăzute de legislația privind protecția datelor în contractele încheiate cu contractorii săi.

Toate măsurile tehnice și organizatorice vor fi aplicate pentru a împiedica accesul neautorizat, prelucrarea neautorizată și nelegală a datelor cu caracter personal, dezvăluirea neautorizată și distrugerea, alterarea, sau pierderea accidentală a datelor cu caracter personal.

V. DREPTURILE PERSOANELOR VIZATE

5.1. În calitate de operator de date cu caracter personal, Operatorul garantează respectarea drepturilor privind protecția datelor cu caracter personal ce le revin subiecților, precum și, după caz, altor persoane vizate.

5.2. În conformitate cu principiile de protecție a datelor cu caracter personal, persoanele vizate beneficiază de următoarele drepturi: la informare, de acces la date, de intervenție, de opoziție asupra datelor cu caracter personal ce-i vizează, precum și dreptul de a se adresa în justiție.

5.3. Toate persoanele implicate în activitatea de administrare și/sau prelucrare a informațiilor din sistemul de evidență vor respecta procedura de acces la datele cu caracter personal.

5.4. Acordarea dreptului de acces a angajaților la informațiile ce vizează subiecții se efectuează prin solicitarea expresă, în formă scrisă, cu acordul nemijlocit al conducerii. Informațiile furnizate vor fi acordate astfel, încît să nu prejudicieze drepturile subiecților. Subiecții datelor cu caracter personal care solicită date cu caracter personal trebuie să indice scopul solicitării, precum și perioada concretă pentru care solicită informațiile.

5.5. Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu, dacă în informaţiile solicitate apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul acestora sau nu pot fi extrase, prin editare, datele cu caracter personal nerelevante.

VI. Măsuri tehnice şi organizatorice implementate de Operator pentru a asigura protecţia datelor din momentul conceperii şi în mod implicit (privacy by design şi privacy by default)

6.1. Operatorul se angajează să protejeze datele cu caracter personal ale persoanelor vizate care au fost prelucrate urmare a interacţiunilor cu acestea, precum şi cu orice alte persoane fizice.

6.2. Ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de drepturile şi libertăţile persoanelor fizice vizate, Operatorul implementează măsuri tehnice şi organizatorice adecvate" pentru a garanta şi a fi în măsură să demonstreze că prelucrarea datelor cu caracter personal se efectuează în conformitate cu legislaţia în vigoare, atât naţională cât şi europeană. Aceste măsuri se revizuiesc periodic de către Responsabilul cu protecţia datelor, Direcţia IT, Direcţia Securitate şi se actualizează în conformitate cu cerinţele legale aplicabile.

6.3. Măsuri organizatorice:

- Accesul în perimetrul de securitate al operatorului de date cu caracter personal este interzis, cu excepţia cazurilor de control autorizat.
- Angajaţii operatorului de date cu caracter personal sînt în drept de a avea acces la spaţiile şi/sau locaţiile asupra cărora au acceptul din partea administratorului. Accesul altor persoane în perimetrul de securitate poate avea loc doar în cazul supravegherii din partea angajaţilor. Pot avea acces în perimetrul de securitate organele de drept sau organele de control în cazul existenţei unor împuterniciri corespunzătoare (în original) a cărei copii se oferă reprezentanţilor operatorului;
- Sediul în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic. Pereţii exteriori ai încăperilor sînt rezistenţi, intrările sunt echipate cu lacăte. Cheile de la lacătele uşilor se păstrează la administrator. Administratorul ţine evidenţa cheilor şi persoanelor care au acces în perimetrul de securitate al operatorului de date cu caracter personal. Uşile şi ferestrele din perimetrul de securitate se încuie în cazul în care angajaţii părăsesc sediul;
- Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul existenţei permisiunii din partea responsabililor;
- În cazul în care contractul de muncă al angajatului a încetat sau a fost suspendat, administratorul operatorului de date cu caracter personal este obligat ca în aceeaşi zi să-i retragă cheile de la căile de acces precum şi de la dulapurile sau safeurile metalice, precum şi drepturile de acces de la computer;

- Înaintea accederii în funcție tuturor angajaților li se aduce la cunoștință sub semnătură Politica de securitate, inclusiv se semnează clauza de nedivulgare a informațiilor cu accesibilitate limitată cu care vor intra în posesie în cadrul operatorului în contextul exercitării sarcinilor și atribuțiilor prestabilite. Nu se permite dezvăluirea datelor cu caracter personal sau a altor informații confidențiale prin intermediul unor mijloace electronice către persoane neidentificate;
- În cazul neutilizării temporare a purtătorilor de informație pe suport de hîrtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în spațiu special amenajat care se încuie. Computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru.
- Salariații Operatorului vor asigura implementarea recomandărilor primite din partea Responsabilului cu protecția datelor în cadrul operațiunilor de prelucrare a datelor pe care le realizează în numele Operatorului;
- Toate dezvoltările și actualizările vizând sistemele și echipamentele implicate în prelucrarea datelor cu caracter personal se vor face cu respectarea principiilor "data protection by design" și "data protection by default", respectiv respectarea dreptului la protecției datelor începând cu momentul conceperii și în mod implicit;
- Doar personalul care are nevoie să acceseze datele cu caracter personal pentru realizarea atribuțiilor sale de serviciu urmează a fi autorizat pentru a avea acces la bazele de date, sistemele și aplicațiile Operatorului(principiul „need to know basis").
- Salariații și colaboratorii Operatorului care au primit autorizarea de acces la baze de date sau care au drepturi de administrare a acestora, respectiv a sistemelor și aplicațiilor IT care le stochează, vor participa în mod regulat la programe de instruire privind protecția și securitatea datelor cu caracter personal.

6.4. Măsuri tehnice:
- Datele cu caracter personal se vor transmite numai în condiții de siguranță, orice transmitere de date cu caracter personal în afara Operatorului, care nu se încadrează în prevederile avizate de Responsabilul cu protecția datelor va fi efectuata numai cu avizul prealabil al acestuia.
- Copiile de siguranță: reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către operator în intervalul de timp în care se execută copiile de siguranță a informațiilor din softurilor folosite pentru prelucrările automatizate ale acestora. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației indicate. Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.
- În situația prelucrărilor de date cu caracter personal realizate de Operator prin intermediul persoanelor împuternicite, Operatorul se va asigura că și acestea implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător al datelor, incluzand în

contractele încheiate cu aceştia clauze privind cerinţele minime de securitate a datelor cu privire la măsurile tehnice şi organizatorice adecvate identificate.

Aceste măsuri vor putea include, fără a se limita la:

a) Măsuri privind minimizarea cantităţii datelor cu caracter personal prin filtrare şi eliminare, reducerea senzitivitatii prin conversie, reducerea acumulării de date, restricţionarea accesului, reducerea capacităţii de identificare a naturii datelor, conform instrucţiunilor Operatorului.

b) Măsuri privind trasabilitatea – existenţa unei politici de trasabilitate şi management al log-urilor, cu păstrarea acestora pe toata durata operaţiunilor de prelucrare a datelor, dar minim 2 ani.

c) Măsuri privind relaţiile Persoanelor împuternicite cu subcontractorii - existenţa unor reglementări şi a unor procese de reducere a riscurilor de acces neautorizat la date.

d) Măsuri în vederea ştergerii, anonimizarii şi/sau returnării datelor cu caracter personal de către persoana împuternicită după finalizarea prelucrării în numele operatorului, exceptând situaţiile în care există o cerinţă legală de stocare a datelor cu caracter personal şi după finalizarea prelucrării.

- Operatorul ţine evidenţa mijloacelor de calcul care stochează datele cu caracter personal şi alte informaţii confidenţiale gestionate;

- Este interzisă utilizarea mijloacelor personale de calcul de tip: laptop, tabletă, stick-uri media etc. în scopul realizării sarcinilor operatorului de date cu caracter personal;

- Accesul la computere se efectuează în bază de profil de utilizator şi parolă care este confidenţială şi nu poate fi transmisă nimănui sau transcrisă sau afişată spre acces nerestricţionat. Parolele conţin minim 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. Parolele se vor modifica peste intervale de 3 luni;

- Dispozitivele de calcul sunt dotate cu program antivirus şi sisteme de operare licenţiate;

- Dispozitivele de calcul pentru fiecare utilizator sunt configurate individual cu filtre de acces şi de utilizare a suportului hardware în dependenţă de sarcinile acestuia şi atribuţiile funcţionale;

- Este interzisă scoaterea din perimetrul de securitate a informaţiilor cu accesibilitate limitată în lipsa unei permisiuni din partea operatorului de date;

- Este interzisă utilizarea programelor de acces la distanţă la tehnica de calcul.

- Sunt asigurate condiţii tehnice şi administrative de securitate electroenergetică şi antiincendiară;

- În cazul extragerii datelor cu caracter personal, documentele se marchează, indicandu-se prescripţii pentru prelucrarea ulterioară şi răspândirea acesteia, inclusiv indicîndu-se numărul de identificare unic al operatorului de date cu caracter personal conform modelului de avertizare: „Documentul conţine informaţii cu accesibilitate limitată. Operator înregistrat/autorizat de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal cu nr. XXXXXX din www.registru.datepersonale.md.

VII. Responsabilul cu protecția datelor cu caracter personal

7.1. Responsabil de asigurarea regimului de protecție a datelor cu caracter personal în cadrul sistemului de evidență este Administratorul, care dispune de cunoștințe necesare, resurse administrative (timp, resurse umane, echipament și buget) și are acces liber la informația necesară pentru îndeplinirea funcțiilor sale.

7.2. Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

a. informarea și consilierea Operatorului precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în ceea ce privește protecția datelor cu caracter personal

b. monitorizarea respectării dispozițiilor legale referitoare la protecția datelor și a politicilor Operatorului în ceea ce privește protecția datelor cu caracter personal și acordarea de consultanta și recomandări Operatorului și departamentelor interne ale acestuia pentru asigurarea respectării obligațiilor în domeniul protecției datelor

c. asigurarea suportului în elaborarea politicilor și procedurilor interne care sunt necesare pentru reglementarea internă a operațiunilor de prelucrare a datelor cu caracter personal

d. furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia (acorda aviz în cazul operațiunilor de prelucrare de date cu caracter personal supuse evaluării impactului, cu privire la obligația Operatorului de a realiza aceasta analiza, metodologia ce urmează a fi utilizata, existența resurselor necesare, măsurile de securitate, tehnice și organizatorice ce urmează a fi aplicate pentru diminuarea riscurilor asupra drepturilor și libertăților persoanei vizate; emite opinii privind corectitudinea modalității în care s-a realizat analiza de impact și asupra concluziilor acesteia, dând aviz pozitiv sau negativ cu privire la realizarea operațiunii de prelucrare)

e. este persoana de contact a operatorului în domeniul protecției datelor cu caracter personal, fiind menționată în informarea persoanelor vizate

f. este persoana de contact a operatorului în relația cu CNPDCP în cazul controalelor realizate de aceasta, precum și în cazul consultării prealabile a acestuia.

g. cooperarea cu autoritatea de supraveghere

h. asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare

i. participarea la programe de formare profesională pentru cunoașterea legislației și practicii în domeniul protecției datelor

7.3. Operatorul publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

VIII. INCIDENTE DE PROTECȚIE ȘI SECURITATE A DATELOR

8.1. Incidentele sistemelor IT care afectează datele cu caracter personal ale subiecților sau ale altor persoane vizate sunt considerate incidente cu risc ridicat.

8.2. În situația unui incident de securitate a datelor cu caracter personal, se vor avea în vedere și prevederile Politicii privind incidentele de Securitate cu impact asupra protecției datelor cu caracter personal.

8.3. Efectele incidentelor de securitate a datelor personale pentru persoana vizată pot consta în: prejudicii de natură fizică, materială și morală, discriminare, furt sau fraudă a identității, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, sau orice alt dezavantaj semnificativ de natură economică și socială, inclusiv dar fără a se limita la privarea de drepturile sale sau imposibilitatea exercitării controlului asupra datelor sale personale.

8.4. Exemple de incidente de securitate a datelor cu caracter personal:

-furtul sau pierderea unui laptop sau memorii externe care conține date personale ale subiecților;

-datele personale ale subiecților care au utilizat serviciul de înrolare prin aplicație mobilă/website sunt accesate prin exploatarea unei vulnerabilități a aplicației;

-un e-mail cu informații sensibile transmis către un destinatar diferit de cel către care se intenționa transmiterea, etc.

- accesarea neautorizata a rețelei interne a Operatorului;

- transmiterea datelor cu caracter personal pe adrese personale de email

8.5. În situația în care un incident de securitate IT afectează date cu caracter personal, Direcția IT sau angajatul Operatorului care a luat act de un asemenea incident, va informa de îndată Responsabilul pentru protectia datelor pentru analiza măsurilor imediate ce urmează a fi luate de către Operator cum ar fi notificarea CNPDCP cu privire la incident în termen de 72 ore de la data la care angajatul Operatorului a luat cunoștință de aceasta și/sau notificarea persoanelor vizate în cazul existenței unui risc ridicat cu privire la drepturile și libertățile fundamentale ale acesteia.

8.6. Notificarea transmisă CNPDCP de către Responsabilul pentru protectia datelor în cazul apariției unui astfel de incident:

- descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

- comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații

- descrie consecințele probabile ale încălcării securității datelor cu caracter personal

- descrie măsurile luate sau propuse spre a fi luate de Operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

8.7. De asemenea, orice alt tip de incident care ar putea sa afecteze date cu caracter personal prelucrate de către Operator, va fi adus la cunoştinţa Responsabilul cu protecţia datelor pentru analiza în conformitate cu legislaţia privind protecţia datelor cu caracter personal.

8.8. În cazul în care are loc un incident de securitate susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, Operatorului va informa persoana afectată fără întârzieri nejustificate cu privire la acest incident.

8.9. Anual, către 31 ianuarie, deţinătorii de date cu caracter personal prezintă CNPDCP raportul generalizat despre incidentele de securitate a sistemelor informaţionale de date cu caracter personal. În baza acestui raport, Centrul întreprinde măsurile ce se impun de Legea cu privire la protecţia datelor cu caracter personal.

IX. RĂSPUNDEREA PENTRU NERESPECTAREA PREVEDERILOR PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

9.1. Pentru nerespectarea prevederilor prezentului Regulament, persoanele culpabile urmează a fi atrase la răspundere disciplinară, contravenţională, penală sau materială, după caz.

X. DISPOZIŢII FINALE

10.1. Prezentul Regulament este revizuit şi ulterior aprobat de către conducerea Operatorului, periodic, precum şi la necesitate.

10.2. Prezentul Regulament se completează cu prevederile legislaţiei în vigoare.

10.3. Modificarea şi completarea prezentului Regulament se face în modul stabilit pentru aprobarea lui.