De uz intern

APROBAT
Administrator ,,Europarc" SRL

DL. Veaceslav MÎRZA
___ianuarie 2023

_____
l.ș.

POLITICA
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

I. DISPOZIȚII GENERALE

1. Politica privind protecția datelor cu caracter personal în cadrul ,,Europarc" SRL (în continuare ***Politica***) stabilește principiile și cerințele față asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.
2. ,,Europarc" SRL (în continuare EUROPARC) – este o companie care oferă servicii de încredere, IDNO - 1005600004639, cu sediul juridic situat în mun. Chișinău, str. Calea Ieșilor 10 B, Republica Moldova care își desfășoară activitatea în conformitate cu Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere, Legea nr. 133/2011 privind protecția datelor cu caracter personal, dar și alte acte normative din domeniu.
3. ***Politica*** are drept scop stabilirea regulilor tehnice și organizatorice minime de privind asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale de date cu caracter personal și/sau registrelor ținute manual, electronic sau în formă mixtă, conform *Anexei nr. 1*.
4. ***Politica*** este elaborată, în conformitate cu prevederile Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28 ianuarie 1981, publicate în European TreatySeries, nr. 108, ratificată de Republica Moldova prin Hotărârea Parlamentului nr. 483-XIV din 2 iulie 1999, Legii nr. 133/ 2011 privind protecția datelor cu caracter personal, Legii nr. 71/2007 cu privire la registre, dar și ținând cont de Regulamentul general privind protecția datelor nr. 679/2016 (GDPR).
5. În sensul ***Politicii***, se definesc următoarele noțiuni:

   anonimizarea – modificarea datelor personale în așa fel încât să nu poată fi identificate sau să ducă la identificarea subiectului de date, astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile. Datele anonimizate nu reprezintă date cu caracter personal;

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

   autoritate responsabilă - Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova (în continuare – Centrul);

   categorii speciale de date cu caracter personal – datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale;

consimțământul subiectului de date cu caracter personal – manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate;

control de securitate – acțiuni întreprinse de către Europarc sau Centrul în vederea verificării și/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor;

criptarea - tehnici moderne de mascare a informației pentru a preveni accesul nerestricționat la informația protejată;

date cu caracter personal – orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale. **De exemplu:** numele, prenumele, anul nașterii, domiciliul, numărul de identificare de stat (IDNP), imaginile foto și video - reprezintă date cu caracter personal care se referă la o persoană fizică identificată direct;

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

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

informație cu accesibilitate limitată - informație atribuită la secret de stat, secret medical, secret comercial, secret bancar, secret fiscal, secret profesional precum și datele cu caracter personal.

integritate – certitudinea, ne contradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;

mijloace de protecție criptografică a informației care conține date cu caracter personal – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;

operator – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare. **De exemplu**: în toate cazurile când EUROPARC va reglementa printr-un act normativ departamental scopurile și procedurile de colectare, stocare și prelucrare în continuare a cărorva date cu caracter personal în sisteme de evidență automatizate, manuale ori mixte, se va

constitui în calitate de operator al acestor date;

organ de control - orice instituție de stat învestită cu competențe de supraveghere, control și investigare în domeniul său de activitate.

organ de ocrotire a legii:

- autoritate publică sau o subdiviziune a unei astfel de autorități, competentă pentru prevenirea, investigarea, depistarea infracțiunilor, în scopul punerii în aplicare a procedurilor penale, urmăririi penale a infracțiunilor sau executării pedepselor penale, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, cum ar fi, dar nu se limitează la: poliția, organele procuraturii, organele vamale, instituțiile penitenciare, organele pentru prevenirea și combaterea corupției, spălării banilor, finanțării terorismului, recuperării bunurilor infracționale, organele de probațiune, organele securității statului;
- autoritate publică sau o subdiviziune a unei astfel de autorități care acționează în domeniul securității naționale sau securității de stat, care efectuează măsuri speciale de investigații.

perimetru de securitate – zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic și/sau tehnic al accesului;

persoană împuternicită de către operator – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator. **De exemplu:** Companiile care oferă servicii în numele EUROPARC;

persoana responsabilă cu protecția datelor cu caracter personal – persoană fizică (salariat) sau persoană juridică (externalizare) care a fost desemnată de către conducerea EUROPARC cu privire la sarcinile și responsabilitățile prevăzute de art. 25^{1-2} din Legea nr. 133/2011 privind protecția datelor cu caracter personal – în cazul dat, compania „Privacy by Default" SRL, în numele administratorului Dl. Sergiu BOZIANU.

prelucrarea datelor cu caracter personal – orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi:

- ***adaptarea*** - transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate;
- ***alăturarea*** - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;
- ***blocarea*** - întreruperea prelucrării datelor cu caracter personal;

- ***colectarea*** - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace și din orice sursă;
- ***consultarea*** - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operațiuni sau set de operațiuni de prelucrare ulterioară;
- ***combinarea/alinierea*** - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri determinate;
- ***dezvăluirea/divulgarea*** – mijloc de a face disponibile date cu caracter personal către terți prin comunicare, transmitere, diseminare sau punerea la dispoziție în orice alt mod;
- ***distrugerea*** - aducerea la stare de neîntrebuințare, în condițiile legii, definitivă și irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.
- ***extragerea*** - scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială;
- ***înregistrarea*** - consemnarea datelor cu caracter personal într-un sistem de evidență automat (electronic) ori neautomat (manual pe suport de hârtie sau pe orice alt suport), care poate fi registru, fișier electronic, baza de date, cartotecă sau orice formă de evidență organizată, structurată ori ad-hoc sau într-un text, înșiruire de date ori document, indiferent de modalitatea în care se înscriu datele;
- ***modificarea*** - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal;
- ***organizarea*** - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite;
- ***restricționarea*** - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
- ***stocarea*** - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranță;
- ***ștergerea*** - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidențe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistența, inexactitatea;
- ***transformarea*** - operațiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în alte scopuri;

- ***utilizarea*** - folosirea datelor cu caracter personal, în tot sau în parte, de către și în interiorul operatorului, împuterniciților operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;

protecția informației contra acțiunilor neintenționate – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;

prelucrarea transfrontalieră a datelor personale – înseamnă prelucrarea datelor personale cu element de extraneitate la care participă o persoană fizică sau juridică de drept public sau privat aflată în alt stat;

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

pseudonimizarea - prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

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

sesiune de lucru – perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și până la momentul opririi acestora;

sistem informațional de date cu caracter personal:

- totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;
- orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice. În calitate de sistem informațional de date cu caracter personal se constituie inclusiv dar nu se limitează la, bazele de date, sistemele informaționale și informatice în care sunt stocate și prelucrate automatizat sau manual date cu caracter personal. De exemplu: modele clasice ale sistemelor informaționale de date cu caracter personal reprezintă: Registrul de evidență a angajaților EUROPARC sau a

numerelor telefoanelor corporative ale angajaților EUROPARC, Registrul de evidență al vizitatorilor; Registrul de evidență a petițiilor și altor adresări, informațiile personalizate referitoare la instruirea specializată a angajaților EUROPARC ori a altor subiecți implicați în procesul instrucțional, Registrul clienților de servicii etc., alte serii structurate de date cu caracter personal, cum ar fi: imaginile video colectate printr-un sistem de supraveghere video instalat în incinta sau pe perimetrul sediului EUROPARC etc.;

tehnologie informațională (TI) – totalitatea metodelor, procedeelor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;

utilizator – persoana care acționează sub autoritatea operatorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal.

II. ASPECTE GENERALE

6. ***Politica*** reprezintă:
   - actul normativ departamental, cu forță juridică obligatorie, respectarea căreia este asigurată de prevederile actelor normative din domeniul protecției datelor cu caracter personal și este documentul ierarhic superior în nomenclatorul actelor interne cu privire la prelucrarea datelor cu caracter personal;
   - un document unitar, compus din anexe, regulamente, instrucțiuni, note informative, acorduri, clauze contractuale, documente tip, formulare tipizate și/sau alte forme de reglementare internă, elaborate și aprobate de către EUROPARC, care stabilește Cerințele ce necesită a fi asigurate de către orice persoană (angajat, persoană împuternicită etc.) care prelucrează datele cu caracter personal în numele sau pe seama EUROPARC;
7. ***Politica*** are statut de document confidențial, acces la care au doar angajații EUROPARC și alte persoanelor împuternicite de către EUROPARC în măsura în care aceștia prelucrează date cu caracter personal, Centrul și alte organe de control, în măsura în care o astfel de situație este prevăzută de lege. Prin derogare de la această clauză, nu constituie încălcare a regimului de confidențialitate expunerea spre acces nerestricționat a unor pasaje din ***Politică***, pentru informarea vizitatorilor sau altor operatori de date cu caracter personal asupra regimului necesar de a fi respectat.
8. ***Politica*** aplică soluții practice cu un nivel de detaliere și complexitate proporțional, în partea ce ține de identificarea și autentificarea utilizatorilor; de reacționare la incidentele de securitate; de protecție a tehnologiilor informaționale și comunicațiilor; de asigurare a integrității informației care conține date cu caracter personal; de administrare a accesului; de audit și asigurare a evidenței, luând în considerare:

8.1. categoriile datelor cu caracter personal*, conform Anexei nr. 2*;

8.2. operațiunile de prelucrare efectuate datelor cu caracter personal, *conform Anexei nr. 3*;

8.3. dimensiunea EUROPARC, în funcție de numărul angajaților, numărul subdiviziunilor administrative, amplasarea geografică a subdiviziunilor sale teritoriale, inclusiv numărul persoanelor ce pot accesa datele cu caracter personal;

8.4. formele de ținere a registrelor în care sunt prelucrate date cu caracter personal (manuală, electronică sau mixtă);

8.5. complexitatea sistemelor informaționale de date cu caracter personal și programelor de aplicații implicate în procesul de prelucrare a datelor;

8.6. riscurile la care este expus EUROPARC sau persoanele ale căror date cu caracter personal sunt prelucrate, starea de dezvoltare tehnologică în acest domeniu și costul măsurilor de implementare.

9. Documentația referitoare la ***Politică*** este centralizată, completă, actualizată cu regularitate și conține cel puțin următoarele elemente:

9.1. identitatea persoanei responsabile cu protecția datelor cu caracter personal;

9.2. măsurile de securitate;

9.3. mecanismul de punere în aplicare a măsurilor de securitate;

9.4. lista datelor cu caracter personal prelucrate în cadrul EUROPARC*, conform Anexei nr.4*, stabilite de Regulamentul de securitate al fiecărui sistem, care prelucrează date cu caracter personal;

9.5. lista nominală a utilizatorilor, autorizați să acceseze datele cu caracter personal, conform *Anexei nr. 5*;

9.6. descrierea detaliată a criteriilor, în conformitate cu care sunt accesibile datele cu caracter personal prelucrate;

9.7. documentația tehnică cu privire la controalele de securitate;

9.8. orarul controalelor de securitate;

9.9. măsurile de detectare a cazurilor de acces și/sau de prelucrare neautorizată a datelor cu caracter personal;

9.10. rapoarte despre incidentele de securitate.

10. ***Politica*** se elaborează într-un singur exemplar și se completează în mod obligatoriu Fișa de evidență a ***Politicii***, conform *Anexei nr. 6*;

11. Măsurile de securitate emise sunt stabilite conform regulamentelor de securitate ale fiecărui sistem care prelucrează date cu caracter personal.

12. Mecanismul de punere în aplicare a măsurilor de securitate este prevăzut de prezenta ***Politică***;

III. ADUCEREA LA CUNOȘTINȚĂ, ELIBERAREA COPIILOR ȘI MODIFICAREA *POLITICII*

13. ***Politica*** se multiplică și se aduse la cunoștința angajaților EUROPARC, în limitele competențelor funcționale și nivelului de acces acordat la date cu caracter personal.
14. Se eliberează sub semnătură o copie a ***Politicii*** către subiecții vizați în următoarele volume:
    14.1. Conducerii – volumul deplin;
    14.2. Persoanelor cu funcție de conducere – volumul necesar care se apreciază de către conducere;
    14.3. Angajaților – volumul necesar care se apreciază de către superiorii nemijlociți;
    14.4. Persoanelor împuternicite – partea în care sunt vizați la efectuarea anumitor operațiuni de prelucrare a datelor cu caracter personal.
15. La multiplicarea și eliberarea copiilor de pe ***Politică*** se completează în mod obligatoriu fișa de evidență a multiplicării ***Politicii***, conform *Anexei nr. 7*.
16. Semnarea în fișa de evidență a multiplicării ***Politicii*** confirmă aducerea la cunoștință a ***Politicii*** și presupune asumarea responsabilității de către persoana vizată (fizică sau juridică) a Cerințelor care necesită a fi asigurate la prelucrarea datelor cu caracter personal.
17. ***Politica*** în original și ***Politica*** în copie se păstrează în perimetrul de securitate al EUROPARC, fiecare deținător al acesteia fiind responsabil de asigurarea confidențialității acestui act.
18. Se interzice multiplicarea și utilizarea ***Politicii*** în alte situații decât cele prescrise de către aceasta, cu excepția cazului în care există acordul prealabil manifestat explicit de către persoana responsabilă de sistemele informaționale de date cu caracter personal, conform *Anexei nr.8;*
19. În cazul în care în procesul de prelucrare a datelor cu caracter personal se constată necorespunderea unor activități cu cadrul juridic, reglementările ***Politicii*** se revizuiesc imediat și se completează fișa de evidență a modificării și completării ***Politici***, conform *Anexei nr. 9.* În situația în care necorespunderea pretinde a fi una esențială pentru regimul juridic prevăzut de ***Politică***, iar soluțiile pe caz sunt contradictorii, EUROPARC va solicita opinia Centrului.

IV. RESPONSABILITĂȚI ȘI OBLIGAȚIUNI

20. Principala responsabilitate în elaborarea, implementarea și monitorizarea aplicării prevederilor ***Politicii*** revine persoanei responsabile cu protecția datelor cu caracter personal (în continuare Persoana responsabilă cu protecția datelor).
21. EUROPARC a decis asupra necesității desemnării unei companii în calitate de persoană responsabilă

cu protecția datelor cu caracter personal, în conformitate cu art. 25-25/2 din Legea nr. 133/2011 privind protecția datelor cu caracter personal.

22. Persoana responsabilă cu protecția datelor, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor Politicii, se subordonează nemijlocit Directorului EUROPARC sau persoanei care îndeplinește interimatul funcției.
23. Persoana responsabilă cu protecția datelor nu poate fi supus sau subordonat nici unei indicații sau cerințe indiferent de către cine a fost înaintată, în cazul în care această solicitare în mod vădit produce coliziune cu regimul juridic al protecției datelor cu caracter personal.
24. Obligațiile EUROPARC în raport cu Persoana responsabilă cu protecția datelor:
    - 24.1. De a implica Persoana responsabilă cu protecția datelor în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal. Aceste aspecte se referă la modul de prelucrare a datelor și a mijloacelor utilizate în acest sens, transferul transfrontalier și măsurile de conformitate și securitate la prelucrarea datelor cu caracter personal;
    - 24.2. De a oferi suport și de a sprijini Persoana responsabilă cu protecția datelor în îndeplinirea sarcinilor sale, asigurându-i resursele necesare administrative (timp, resurse umane, echipament, soft) și financiare, pentru executarea acestor atribuții;
    - 24.3. De a oferi acces liber la informația necesară pentru îndeplinirea funcțiilor sale, în măsura în care acesta nu operează în afara cadrului ***Politicii;***
    - 24.4. De a oferi accesul la locațiile unde sunt prelucrate datele, inclusiv la datele personale, la regulamente, instrucțiuni, ordine, dispoziții ce se referă la protecția datelor cu caracter personal;
    - 24.5. De a nu sancționa, demite sau restrânge Persoana responsabilă cu protecția datelor prin anumite măsuri administrative pentru îndeplinirea sarcinilor sale în corespundere cu cadrul normativ;
    - 24.6. De a informa Persoana responsabilă de protecția datelor că poartă răspundere în conformitate cu legislația civilă, contravențională și/sau penală, pentru exercitarea cu rea credință a sarcinilor și împuternicirilor de care dispune;
    - 24.7. De a informa Persoana responsabilă de protecția datelor să nu primească indicații sau instrucțiuni care ar putea duce la încălcarea regimului juridic de protecție a datelor cu caracter personal;
    - 24.8. De a informa Persoana responsabilă cu protecția datelor să nu primească indicații sau instrucțiuni care ar putea genera un conflict de interese;
    - 24.9. De a comunica Persoana responsabilă de protecția datelor că este autorizat să efectueze măsuri de instruire, simulare și control a implementării și respectării ***Politicii*** în cadrul EUROPARC;
    - 24.10. De a delega, în caz de necesitate, o parte din responsabilitățile funcționale prevăzute de ***Politică*** către alți angajați printr-un ordin corespunzător.

25. Sarcinile, obligațiile și responsabilitățile Persoanei responsabile de protecția datelor:
    25.1. Informează și oferă consiliere EUROPARC-ului și/sau persoanelor împuternicite de către EUROPARC, precum și angajaților în activități legate de prelucrarea datelor cu caracter personal, respectarea ***Politicii***, cadrul legal din domeniul protecției datelor cu caracter personal;
    25.2. Informează și explică drepturile subiecților de date cu caracter personal;
    25.3. Oferă suport la examinarea cererilor, plângerilor, sesizărilor, reclamațiilor înaintate în contextul domeniului protecției datelor cu caracter personal;
    25.4. Monitorizează respectarea prezentei Politici și a cerințelor din domeniul protecției datelor cu caracter personal;
    25.5. Oferă suport și consiliere la evaluarea impactului asupra protecției datelor cu caracter personal;
    25.6. Reprezintă operatorul pe problemele legate de domeniul protecției datelor cu caracter personal;
    25.7. Informează operatorul, persoanele împuternicite de către operator și angajații acestora despre tendințele și modificările în domeniul protecției datelor cu caracter personal;
    25.8. Cooperează cu Autoritatea de supraveghere, inclusiv ca punct de contact în cazul consultării prealabile cu aceasta;
    25.9. Asigură confidențialitatea și nedivulgarea informațiilor cu care a făcut cunoștință în cadrul realizării sarcinilor și activităților în calitate de responsabil cu protecția datelor cu caracter personal;
    25.10. Dispune de cunoștințe de specialitate în dreptul și practicile din domeniul protecției datelor cu caracter personal și le perfectează sistematic în corespundere cu tendințele din domeniul protecției datelor;
    25.11. Efectuează instruire noilor angajați privitor la principiile de protecție a datelor cu caracter personal;
    25.12. Efectuează cel puțin 1 instruire pe an ale angajaților privitor la principiile de protecție a datelor cu caracter personal;
    25.13. Menține registrul de evidență a persoanelor instruite, conform *Anexei nr. 1*0;
    25.14. Stabilește orarul controalelor de securitate, în conformitate cu regulamentul de securitate al fiecărui Sistem de date cu caracter personal. Controalele de securitate se realizează sistematic (odată în an/jumătate de an). Prin intermediul acestor controale se face o evaluare suplimentară prin care se vede dacă se respectă cerințele de protecție a datelor, de către persoanele responsabile de aceste sisteme;
    25.15. Consiliază privind ținerea registrului controalelor de securitate, conform *Anexei nr.11*.
    25.16. Examinează rapoartele despre incidentele de securitate în registrul de evidență, conform *Anexei nr.12*.

V. CADRUL JURIDIC APLICABIL

26. La prelucrarea datelor cu caracter personal sunt respectate următoarele acte:
    26.1. La nivel internațional/regional:
        26.1.1. Convenția nr. 108 *pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal*;
        26.1.2. Practica Curții Europene a Drepturilor Omului;
        26.1.3. Recomandările Consiliului de Miniștri[1], Autorității Europene de Protecție a Datelor și Comitetului european pentru protecția datelor (CEPD).
    26.2. La nivel național:
        26.2.1. Constituția Republicii Moldova;
        26.2.2. Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;
        26.2.3. Legea nr. 133/2011 privind protecția datelor cu caracter personal;
        26.2.4. Legea 982/2000 privind accesul la informație;
        26.2.5. Alte acte normative naționale care instituie regim special de prelucrare a informațiilor cu accesibilitate limitată potrivit ierarhiei stabilite supra.

VI. MODUL DE APLICARE A CLAUZELOR REGULATORII PREVĂZUTE DE *POLITICĂ*

27. Înaintea punerii în aplicare a noilor procedee și/sau mijloace de prelucrare a datelor cu caracter personal, în mod obligatoriu acestea se vor supune avizării de către Persoana responsabilă cu protecția datelor prin prisma principiului ,,privacy by default" și ,,privacy by design", prevăzut de prezenta ***Politică***.
28. Sub incidența avizării obligatorii a procedeelor și mijloacelor de prelucrare a datelor cu caracter personal cad următoarele activități:
    28.1. Regulamentele, instrucțiunile, contractele, codurile, formularele tipizate, anchetele și orice tip de documente care implică prelucrarea datelor cu caracter personal;
    28.2. Softurile și soluțiile electronice care stabilesc și/sau implică prelucrarea datelor cu caracter personal;
    28.3. Amplasarea mobilierului, posturilor de muncă, computerelor și altor dispozitive;
    28.4. Avizarea procedurilor de acordare și retragere a codurilor de acces, cheilor electronice sau

[1] **Consiliul Uniunii Europene** (uneori denumit și **Consiliul** sau **Consiliul de Miniștri**) este un organism parte a legislativului (UE) reprezentând guvernele statelor membre.

mecanice precum și verificarea respectării acestor proceduri;

28.5. Modalitățile de supraveghere și monitorizare a accesului în perimetrul de securitate;

28.6. Metodele de control și verificare a modului de respectare a sarcinilor și activităților de serviciu;

28.7. Acordarea accesului la datele cu caracter personal către persoanele împuternicite, terți, destinatari precum și entităților care nu sunt considerate ca destinatari (organele de control, organele din sectorul polițienesc);

28.8. Consilierea privind acordarea accesului la date cu caracter personal conform procedurii de solicitare a accesului, conform *Anexei nr.13;*

28.9. Alte activități care implică sau interferează cu domeniul protecției datelor cu caracter personal.

29. Respectarea principiului ,,privacy by design" presupune ca EUROPARC, având în vedere stadiul actual al tehnologiei, costurile implementării, natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, va pune în aplicare măsuri tehnice și organizatorice adecvate (cum ar fi pseudonimizarea, anonimizarea etc.), care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor (precum minimizarea datelor) și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prevăzute de Legea privind protecția datelor cu caracter personal și a proteja drepturile subiectului de date.
30. Respectarea principiului ,,privacy by default" presupune ca, în mod implicit, vor fi prelucrate numai datele personale care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor.
31. Ori de câte ori apar dubii sau neclarități cum ar trebui prelucrate datele cu caracter personal, subiecții vizați au obligația de a informa Persoana responsabilă cu protecția datelor pentru luarea deciziei pe caz.
32. În situația în care într-un caz individual de prelucrare a datelor cu caracter personal se conturează mai multe soluții contradictorii, prelucrarea datelor se va suspenda prin păstrarea acesteia în formă intactă până la luarea unei decizii legale pe caz.
33. Orice dubiu sau interpretare se efectuează în favoarea drepturilor subiectului de date cu caracter personal și asigurarea regimului juridic de confidențialitate prevăzut de Legea privind protecția datelor cu caracter personal.

VII. INTERACȚIUNEA EUROPARC CU CNPDCP ȘI CU ALTE ORGANE DE CONTROL SAU CU ORGANELE DE OCROTIRE A LEGII.

34. În cazul în care în procesul de prelucrare a datelor cu caracter personal sau al asigurării regimului juridic al protecției datelor cu caracter personal se constată anumite acțiuni care excedă regimul juridic al prelucrării datelor cu caracter personal sau în privința cărora există o bănuială rezonabilă de necorespundere, EUROPARC va sesiza imediat CNPDCP, în formă scrisă prin scrisoare oficială sau în formă electronică, telefonic, prin fax sau orice altă modalitate care va permite neîntârziat de a înștiința despre acest fapt, dar nu mai târziu de 72 de ore din momentul cunoașterii despre pretinsul fapt al comiterii și/sau intenționării comiterii unui incident de securitate.
35. EUROPARC poate sesiza sau dezvălui informații cu accesibilitate limitată și altor organe de control sau organe competente prin prisma sarcinilor și atribuțiilor de care dispun acestea cu condiția întrunirii condițiilor de conformitate prevăzute de ***Politică*** și de cadrul normativ în vigoare.
36. La înaintarea unor astfel de sesizări, EUROPARC va reduce la maxim informațiile cu accesibilitate limitată, după caz, oferind indici generali, pentru a aduce în vizorul autorității aspectele necesare legate de fapta sesizată.
37. Centrul în raport cu operațiunile de prelucrare a datelor cu caracter personal efectuate de către EUROPARC sau după caz persoana împuternicită de către EUROPARC, în cadrul unui control înregistrat în modul corespunzător:
    37.1. Dispune de dreptul de acces la informații inclusiv cu accesibilitate limitată care este relevantă situației investigate, indiferent de faptul dacă este prelucrată în format electronic sau manual, prin intermediul soluțiilor software și hardware aflate sub controlul EUROPARC;
    37.2. Restricțiile de confidențialitate prevăzute de Politică nu împiedică CNPDCP de accedere la informația necesară;
    37.3. Poate fi refuzat în acordarea accesului la datele cu caracter personal doar în situația în care solicitarea este una nemotivată.

VIII. PRINCIPIILE GENERALE DE CONFORMITATE LA PRELUCRAREA DATELOR

38. Datele cu caracter personal care fac obiectul unei prelucrări, trebuie să fie prelucrate:
    38.1. *corect și conform prevederilor legale* – orice colectare și ulterior prelucrare de date cu caracter personal urmează să se facă în strictă conformitate cu procedura și cu necesitatea ce rezultă expres din prevederile actelor normative. Aceasta presupune că înainte de a colecta, utiliza și dezvălui datele cu caracter personal, acest fapt trebuie să rezulte expres dintr-un drept sau obligație legală;

38.2. *în scopuri determinate, explicite și legitime, iar ulterior să nu fie prelucrate într-un scop incompatibil* – înainte de a fi colectate și utilizate datele cu caracter personal, acestea urmează a fi raportate exhaustiv la scopul în care sunt colectate acestea, cu stabilirea concretă a sistemului de evidență a datelor cu caracter personal în care se vor prelucra astfel de date, norma legală care oferă un astfel de drept. Datele colectate într-un scop nu pot fi utilizate în oricare alt scop decât cu consimțământul subiectului de date dacă legea nu prevede altfel.

38.3. *adecvat, pertinent și neexcesiv* – atât la colectarea datelor cu caracter personal cât și la stocarea, utilizarea sau prelucrarea în orice alt fel se va efectua raportarea volumului categoriilor de date cu caracter personal prelucrate la necesitatea reală a EUROPARC. În acest sens, se va ține cont de principiul minimizării datelor cu caracter personal colectate și verificării periodice sau la necesitate asupra pertinenței și caracterului neexcesiv al datelor prelucrate.

38.4. *exact și actualizat* – EUROPARC va colecta datele cu caracter personal din actele de identitate din sistemul național de pașapoarte, de la subiectul de date, din sistemele informațional de stat și private, sau alte surse veridice. Actualizarea datelor cu caracter personal se va efectua sistematic.

38.5. *pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sânt colectate și ulterior prelucrate* – datele cu caracter personal se vor stoca doar până la atingerea scopului pentru care datele au fost colectate, conducându-se de legislația în vigoare.

39. În cadrul EUROPARC nu există ierarhie de subordonare sub aspect al prelucrării datelor cu caracter personal. Cerințele de conformitate sunt asumate de către fiecare angajat în parte ținându-se cont de instrucțiunile normative existente la momentul prelucrării.

40. Angajații care efectuează operațiuni de prelucrare a datelor cu caracter personal ce rezultă expres din sarcinile și scopurile stabilite de EUROPARC sunt efectuate de către EUROPARC – persoană juridică, dacă legea nu prevede altfel. În acest context, responsabilitatea juridică și răspunderea față de aceste operațiuni de prelucrare a datelor cu caracter personal ține exclusiv de EUROPARC.

41. În cazul în care informația cu accesibilitate limitată este utilizată de către angajatul EUROPARC în alte scopuri decât cele prestabilite expres de EUROPARC, aceste activități se consideră a fi contrare acestor reglementări, în acest sens, angajatul se va constitui în calitate de operator de date distinct de EUROPARC, responsabilitatea juridică și răspunderea prevăzută de legislația în vigoare se aplică exclusiv în privința acestuia.

42. Persoanele implicate în procesul de prelucrare a datelor cu caracter personal, consultanții național și internaționali, terțe persoane, angajați în cadrul proiectelor de asistență tehnică pentru realizarea sarcinilor, în vederea îndeplinirii de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității

acestora, definesc clar responsabilitățile și procesele de securitate a datelor cu caracter personal, asigură măsuri tehnice și organizaționale necesare organizării procesului de securitatea datelor cu caracter personal.

IX. TEMEIURILE LEGALE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL

43. Datele cu caracter personal pot fi prelucrate în temeiul contractului, a unei obligații legale, a interesului legitim al EUROPARC și/sau în temeiul consimțământului subiectului de date.
44. Consimțământul la prelucrarea datelor cu caracter personal urmează a fi oferit pentru fiecare situație specifică, în cunoștință de cauză, oferirea căruia nu trebuie să influențeze volumul și calitatea raporturilor prestabilite.
45. Consimțământul poate fi obținut în formă olografă, sau electronică potrivit cerințelor documentului electronic.
46. Consimțământul la prelucrarea datelor cu caracter personal va fi colectat pentru fiecare situație specifică care nu este acoperită de raportul contractual sau de lege. Oferirea consimțământului pentru astfel de prelucrări este opțională și nu poate influența volumul și calitatea raporturilor prestabilite inițial. Consimțământul nu poate fi oferit și retras retroactiv.
47. În scopul încheierii contractului de prestare a serviciilor/contractului de muncă/raporturilor de serviciu sau executării acestora, la cererea subiectului de date, în calitate de temei pentru prelucrarea datelor cu caracter personal servește raportul juridic declanșat sau încheiat.
48. Nu se va încheia un consimțământ separat dacă datele sunt colectate direct de la subiectul de date, în cazul:
    48.1. acțiunilor necesare înaintea încheierii contractului;
    48.2. activităților indispensabile executării contractului;
    48.3. îndeplinirea unei obligații care îi revine EUROPARC conform legii;
    48.4. protejarea vieții, integrității fizice sau a sănătății subiectului datelor cu caracter personal;
    48.5. realizarea unui interes legitim al EUROPARC sau al terțului căruia îi sunt dezvăluite datele cu caracter personal, cu condiția ca acest interes să nu prejudicieze interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal;
    48.6. scopuri statistice, de cercetare istorică sau științifică, cu condiția ca datele cu caracter personal să rămână anonime pe toată durata prelucrării.
49. EUROPARC informează că datele cu caracter personal pot fi utilizate și în alte scopuri prevăzute

expres de lege, cum ar fi: la solicitarea organelor de ocrotire a legii, organelor de control - activități pe care EUROPARC nu le poate prestabili însă le ia în calcul atunci când colectează datele cu caracter personal. În cazul unor astfel de situații, EUROPARC va verifica corespunderea solicitării sub aspect de respectare a principiilor de protecție a datelor cu caracter personal și le va executa doar în cazul existenței scopului și temeiului legal.

50. Prelucrarea datelor cu caracter personal se consideră a fi contrară, indiferent de faptul că se face în temeiul consimțământului subiectului de date sau în baza unui raport contractual, atunci când aceasta nu corespunde principiilor de prelucrare a datelor cu caracter personal stabilite de ***Politică***.

X. DREPTURILE SUBIECȚILOR DE DATE CU CARACTER PERSONAL

51. *Dreptul la informare,* constă în dreptul de a fi informat cu privire la identitatea EUROPARC, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, existența drepturilor prevăzute de Legea privind protecția datelor cu caracter personal, precum și condițiile în care pot fi exercitate.
52. *Dreptul de acces la date,* constă în dreptul de a obține de la EUROPARC în temeiul unei cereri, confirmarea/infirmarea faptului dacă datele cu caracter personal care-l vizează au fost sau nu prelucrate precum și a informațiilor ce vizează dreptul la informare.
53. *Dreptul de intervenție* constă în dreptul de a obține în baza unei cereri, rectificarea, actualizarea, blocarea, ștergerea sau transformarea în date anonime a datelor a căror prelucrare nu este conformă cu cerințele Legii privind protecția datelor cu caracter personal, în special a datelor incomplete sau inexacte.
54. *Dreptul de opoziție* constă în dreptul de a se opune în orice moment, din motive întemeiate și legitime legate de situația sa particulară, ca datele care îl vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care există dispoziții legale care prevăd altfel.
55. *Dreptul de a nu fi supus unei decizii individuale,* constă în dreptul de a cere și de a obține retragerea, anularea sau reevaluarea oricărei decizii care produce efecte juridice în privința subiectului de date cu caracter personal, adoptată exclusiv pe baza unei prelucrări automatizate de date, destinată să evalueze unele aspecte ale personalității sale, precum competența profesională, credibilitatea, comportamentul ori alte asemenea aspecte.

XI. CERINȚE GENERALE

56. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemelor informaționale de date cu caracter personal și vor fi efectuate neîntrerupt de către persoanele responsabile angajate la EUROPARC.
57. Configurarea sistemului informațional de date cu caracter personal și a rețelei are loc în conformitate cu cerințele tehnice;
58. Protecția datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.
59. Măsurile de protecție a datelor cu caracter personal prelucrate în sistemele informaționale de date cu caracter personal ale EUROPARC se înfăptuiesc ținându-se cont de necesitatea asigurării confidențialității acestor măsuri.
60. Sunt supuse protecției toate resursele informaționale ale EUROPARC, care conțin date cu caracter personal, inclusiv:
    60.1. suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
    60.2. sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.
61. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal este asigurată în scopul:
    61.1. preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
    61.2. preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
    61.3. respectării cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;
    61.4. asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;
    61.5. păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.
62. Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:
    62.1. preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
    62.2. excluderea accesului neautorizat la datele cu caracter personal prelucrate;

62.3. preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

62.4. preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați ai operatorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.

63. Preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestor informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de regim.

64. Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță.

65. Existența Regulamentelor de securitate pentru fiecare sistem informațional care prelucrează date cu caracter personal trebuie să fie obligatorie.

66. Ordinea de acces la informația care conține date cu caracter personal, prelucrată în cadrul sistemelor informaționale, se stabilește prin Ordin intern sau prin decizia conducerii EUROPARC.

XII. SECURITATEA MEDIULUI FIZIC ȘI A TEHNOLOGIILOR INFORMAȚIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Autorizarea accesului fizic

67. Accesul în sediu ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program, conform listei nominale de acces la sistemul informațional.

68. Accesul în incinta perimetrului de securitate este permis doar personalului autorizat, conform *Anexei nr. 14*. Personalul străin are acces în aceasta încăpere doar sub stricta supraveghere a personalului autorizat.

69. Toate operațiunile de acces la servere sau alte mijloace tehnice sau software se face de către personalul tehnic.

Administrarea și monitorizarea accesului fizic

70. Se efectuează administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.
71. Înainte de acordarea accesului fizic la sistemele informaționale de date cu caracter personal se verifică competențele de acces.

    Persoanele noi angajate, înainte de oferirea drepturilor de acces la sistemele de evidență, sunt instruite în domeniul prelucrării datelor cu caracter personal și semnează declarația de confidențialitate emisă în acest sens.

Securitatea perimetrului EUROPARC și mijloacelor de prelucrare a datelor cu caracter personal

72. EUROPARC are sediul pe teritoriul Republicii Moldova. Perimetrul de securitate al EUROPARC îl reprezintă sediul central, conform *Anexei nr. 15*. Perimetrul sediului și a încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal sunt păstrate integre din punct de vedere fizic, toți pereții sunt întregi, ușile se încuie, iar ferestrele se închid.
73. Pereții exteriori ai încăperilor sunt rezistenți, intrările echipate cu lacăte.
74. Computerele și alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
75. Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc angajații.
76. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
77. 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 EUROPARC.

Controlul vizitatorilor

78. Accesul vizitatorilor se înregistrează în registre, care se păstrează minimum un an. La expirarea termenului de un an, registrele sunt lichidate, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă *(Anexa nr. 19)*.
79. În birourile cu acces interzis aceștia pot intra doar sub supravegherea personalului autorizat.
80. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, aceștia vor fi rugați să părăsească încăperea în mod cât mai urgent.
81. Incidentul va fi adus la cunoștința conducerii EUROPARC.

Securitate electroenergetică

82. Se asigură securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate.
83. În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

Securitatea cablurilor de rețea

84. Cablurile de rețea, prin care se efectuează operațiuni de prelucrare a datelor cu caracter personal, sunt protejate contra conectărilor nesancționate sau deteriorărilor. Cablurile de tensiune sunt separate de cele comunicaționale pentru a exclude bruiajul.
    Personalul tehnic efectuează controale, nu mai rar decât o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de rețea.

Asigurarea securității anti incendiare a sistemelor informaționale de date cu caracter personal

85. EUROPARC dispune de mijloace de asigurare a securității anti incendiare a sediului unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

Controlul instalării și scoaterii componentelor TI

86. Se exercită controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.
87. Informațiile care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standarde de nimicire.

Masurile generale de administrare a securității informaționale

88. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau digitali care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.
89. Computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru.
90. Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.
91. Accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis și controlat.

92. Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni a Conducerii EUROPARC cu excepția situației când astfel de situații rezultă din cerințele funcției de post.

XIII. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAȚIONAL DE DATE CU CARACTER PERSONAL

Identificarea și autentificarea utilizatorului

93. Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.

    Toți utilizatorii (inclusiv personalul care asigură susținerea tehnica, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.

    Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. În cazul în care contractul de munca/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și 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 și autentificare se revocă în mod automat în decursul a două săptămâni de la ultimul acces, sau în mod individual imediat la momentul introducerii modificării în raportul de muncă.

    Se utilizează autentificarea multifactorială, care include parole complexe, cu includerea simbolurilor, literelor, cifrelor în combinație complexă.

    Parola nu va conține inițialele sau date care pot caracteriza o anumită persoană (data de naștere, adresă, poreclă, etc.).

Identificarea și autentificarea echipamentului

94. Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal.

Administrarea identificatorilor utilizatorilor

95. Administrarea identificatorilor utilizatorilor include:
    95.1. identificarea univoca a fiecărui utilizator;
    95.2. verificarea autenticității fiecărui utilizator;

95.3. obținerea autorizației de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declarației de confidențialitate și trecerii procedurii de instruire;

95.4. garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;

95.5. dezactivarea contului de utilizator după o perioadă inactiva, stabilită în timp (2 săptămâni);

95.6. executarea copiilor de arhivă a ID-urilor utilizatorilor.

Asigurarea conexiunii bilaterale în cazul introducerii informației de autentificare a utilizatorilor

96. Se asigură conexiunea bilaterală a EUROPARC cu utilizatorul în momentul procedurilor de autentificare, care nu compromite mecanismul de autentificare.

    După instalarea sistemului, se schimbă informațiile de autentificare a utilizatorilor utilizate standard.

Utilizarea parolelor în procesul asigurării securității informaționale

97. Se respectă regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor care includ:

    97.1. păstrarea confidențialității parolelor;

    97.2. interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;

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

    97.4. alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sunt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere;

    97.5. modificarea parolelor peste intervale de maximum 3 luni;

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

Administrarea parolelor utilizatorilor

98. Se folosesc identificatoare individuale pentru fiecare utilizator și parole individuale ale acestora pentru asigurarea posibilității de stabilire a responsabilității.

    Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora.

    Se asigură blocarea accesului după trei tentative greșite de autentificare.

    Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioadă de un an) și prevenirea folosirii repetate a acestora. La momentul introducerii, parolele nu se reflectă în clar pe monitor.

Parolele se păstrează în forma cifrată, utilizându-se algoritmul criptografic unilateral (funcția hash).

XIV. ADMINISTRAREA ACCESULUI UTILIZATORILOR

Administrarea accesului

99. Se folosesc mecanisme de înregistrare și evidență a persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal și care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

Administrarea conturilor de acces (account-urilor)

100. Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora.
Sunt folosite mijloace automatizate de suport în scopul administrării conturilor de acces.
Se folosesc mijloace automatizate de înregistrare și informare despre crearea, modificarea, dezactivarea și încetarea acțiunii conturilor de acces.

Acordarea accesului

101. Este autorizat accesul la sistemele informaționale de date cu caracter personal în conformitate cu prezenta ***Politică***.

Revizuirea drepturilor de acces ale utilizatorilor

102. Drepturile de acces ale utilizatorilor la sistemele informaționale de date cu caracter personal sunt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate și după oricare schimbare de statut al utilizatorului.

Repartizarea obligațiilor și investirea cu minimul de drepturi și competențe.

103. Repartizarea obligațiilor subiecților care asigură funcționarea sistemelor informaționale de date cu caracter personal este efectuată prin intermediul investirii cu drepturi/competențe corespunzătoare de acces, prin ordin intern întocmit în acest sens.
Utilizatorii sistemelor informaționale de date cu caracter personal se investesc doar cu acele drepturi/competențe, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

Informații de avertizare

104. Înainte de acordarea accesului în sistem, utilizatorii sunt informați despre faptul că folosirea

sistemelor informaționale de date cu caracter personal este controlată și că folosirea neautorizată a acestora se urmărește în conformitate cu legislația.

Blocarea sesiunii de lucru

105. Sesiunea de lucru în sistemul informațional, destinat prelucrării datelor cu caracter personal, se blochează automat, după maxim 5 minute de perioada 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 și autentificare.

Controlul administrării accesului

106. Se efectuează controlul acțiunilor utilizatorului în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

Accesul de la distanță

107. Toate metodele de acces la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sunt documentate, supuse monitorizării și controlului. Lucrul la distanță se efectuează în baza instrucțiuni specifice de reglementare a activității la distanță aprobate prin ordin.

Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal se autorizează de către personalul IT al EUROPARC și este permis doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Limitarea folosirii tehnologiilor fără fir

108. Accesul fără fir la sistemele informaționale de date cu caracter personal este documentat, supus monitorizării și controlului. Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației. Folosirea tehnologiilor fără fir se autorizează de personalul tehnic al EUROPARC.

Administrarea accesului echipamentului portativ și mobil

109. Accesul la sistemele informaționale de date cu caracter personal cu folosirea echipamentului portativ și mobil se documentează, este monitorizat și controlat.

XV. PROTECȚIA SISTEMELOR INFORMAȚIONALE ȘI COMUNICAȚIILOR ÎN CARE SUNT PRELUCRATE DATE CU CARACTER PERSONAL

Divizarea programelor aplicative

110. Se asigură separarea posibilităților funcționale ale utilizatorului de posibilitățile funcționale de gestionare a sistemelor informaționale de date cu caracter personal.

Izolarea funcțiilor de securitate

111. Se asigură izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea sistemelor informaționale de date cu caracter personal.

Informația restantă

112. Sunt preîntâmpinate tentativele dezvăluirii neautorizate sau neintenționate a informației restante care conține date cu caracter personal, prin intermediul resurselor informaționale general accesibile.

Protecția contra refuzului în serviciu

113. Se asigură protecția sistemelor informaționale de date cu caracter personal sau limitate posibilitățile de realizare a atacurilor de diferite tipuri, inclusiv DOS (denial of service) -,,refuz in serviciu".

Prioritățile resurselor

114. Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a prioritarilor, a folosirii resurselor informaționale în care sunt prelucrate date cu caracter personal.

Protecția perimetrului sistemelor informaționale în care sunt prelucrate date cu caracter personal

115. Se efectuează monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaționale.

Amplasarea resurselor general accesibile se asigură în spațiile special destinate a rețelei de calcul cu interfețele fizice de rețea.

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

Asigurarea integrității datelor cu caracter personal transmise

116. Se asigură integritatea datelor cu caracter personal transmise, utilizându-se mijloacele de protecție criptografică.

Asigurarea confidențialității datelor cu caracter personal transmise

117. Se asigură confidențialitatea datelor cu caracter personal transmise, utilizându-se mijloace de protecție criptografică a informației.

XVI. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE DE DATE CU CARACTER PERSONAL

Generarea înregistrărilor de audit în sistemele informaționale de date cu caracter personal

118. Responsabilul fiecărui sistem informațional organizează generarea înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

Lista evenimentelor înregistrate de sistemul de audit al securității în sistemele informaționale de date cu caracter personal

119. Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
    - 119.1. data și timpul tentativei intrării/ieșiri și;
    - 119.2. ID-ul utilizatorului;
    - 119.3. rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.

120. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:
    - 120.1. data și timpul tentativei de pornire;
    - 120.2. denumirea/identificatorul programului aplicativ sau procesului;
    - 120.3. ID-ul utilizatorului;
    - 120.4. rezultatul tentativei de pornire - pozitivă sau negativă.

121. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
    - 121.1. data și timpul tentativei de obținere a accesului (executare a operațiunii);
    - 121.2. denumirea (identificatorul) aplicației sau procesului;
    - 121.3. ID-ul utilizatorului;
    - 121.4. specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
    - 121.5. tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
    - 121.6. rezultatul tentativei de obținere a accesului (executare a operațiunii) - pozitivă sau

negativă.

122. Se efectuează înregistrarea modificărilor drepturilor de acces (competentelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
    122.1. data și timpul modificării competentelor;
    122.2. ID-ul administratorului care a efectuat modificările;
    122.3. ID-ul utilizatorului și competentele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
123. Se efectuează înregistrarea ieșiri din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
    123.1. data și timpul eliberării;
    123.2. denumirea informației și căile de acces la aceasta;
    123.3. specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
    123.4. ID-ul utilizatorului, care a solicitat informația;
    123.5. volumul documentului eliberat (numărul paginilor, a filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

Prelucrarea rezultatelor auditului securității în sistemele informaționale de date cu caracter personal

124. În caz de deranjament al auditului securității în sistemele informaționale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informat Persoana responsabilă cu protecția datelor care întreprinde măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

Monitorizarea, analiza și generarea rapoartelor de audit a securității în sistemele informaționale de date cu caracter personal

125. Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul și întreprinderea acțiunilor prestabilite în ***Politică*** pentru astfel de cazuri.

Protejarea datelor de audit a securității în sistemele informaționale de date cu caracter personal

126. Rezultatele auditului securității în sistemele informaționale de date cu caracter personal, care

reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora.

Păstrarea datelor de audit a securității în sistemele informaționale de date cu caracter personal

127. Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal se justifică în ***Politică***, dar în orice caz acest termen nu este mai mic de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare.

    În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

XVII. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI TEHNOLOGIILOR INFORMAȚIONALE

Înlăturarea deficiențelor de soft destinat prelucrării datelor cu caracter personal

128. Se asigura identificarea, protocolarea și înlăturarea deficientelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestor soft-uri.

Asigurarea protecției contra programelor dăunătoare (virușilor)

129. Se asigură protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsura care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.

Tehnologiile și mijloacele de constatare a intruziunilor

130. Se utilizează tehnologii și mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaționale de date cu caracter personal și constatarea atacurilor, inclusiv care asigura identificarea tentativelor folosirii neautorizate a sistemelor informaționale.

Asigurarea integrității soft-urilor și informației

131. Se asigură protecția și posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal și informației care conține date cu caracter personal.

Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal

132. Se asigură testarea funcționarii corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului și la solicitarea utilizatorului autorizat în acest scop).

XVIII. COPIILE DE REZERVĂ ȘI RESTABILIREA INFORMATIEI CARE CONȚINE DATE CU CARACTER PERSONAL

Copiile de rezervă ale informației care conține date cu caracter personal

133. Copiile de siguranța a informațiilor care conțin date cu caracter personal și a soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate periodic, fiind păstrate cel puțin 1 an în locuri sigure, cu acces limitat.

    Copiile de siguranța se testează în scopul verificării siguranței purtătorilor de informații și integrității informației care conține date cu caracter personal.

    Procedurile de restabilire a copiilor de siguranța se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

XIX. GESȚIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL

Instructajul de reacționare la incidentele de securitate a sistemelor informaționale de date cu caracter personal

134. Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
135. Fiecare incident urmează a fi adus la cunoștința Persoanei responsabile cu protecția datelor în mod de urgență, pentru a putea fi identificată procedura de soluționare a incidentului.

Prelucrarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal

136. În cazul depistării unui incident de securitate, este asigurat mecanismul de informare neîntârziata a conducerii EUROPARC.

137. Prelucrarea incidentelor include în mod obligator depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității inițiale, precum și crearea unei pârghii de evitarea ulterioarelor incidente asemănătoare.

Monitorizarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal

138. Incidentele de securitate a sistemelor informaționale de date cu caracter personal se urmăresc și se documentează în regim permanent.
139. Sunt utilizate mijloace automatizate pentru urmărirea incidentelor de securitate a sistemelor informaționale de date cu caracter personal, colectarea și analiza informației despre aceste incidente.

XX. PROTECȚIA TEHNICĂ A INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL

140. Este asigurată protecția informației care conține date cu caracter personal contra scurgerii prin intermediul rețelei electrice, inclusiv încrucișarea rețelelor electrice ale obiectului cu instalarea filtrelor de protecție care blochează (bruiază) semnalul.

    Se exclude sau se limitează instalarea neautorizată a altor dispozitive electrice, radio sau de alt gen în încăperile unde sunt amplasate mijloacele tehnice de prelucrare a datelor cu caracter personal, în scopul asigurării securității prelucrării datelor cu caracter personal.

    Utilajul, liniile căruia au ieșire în afara perimetrului controlat, este instalat la o distanță de cel puțin 3 metri de la mijloacele TI în care sunt prelucrate date cu caracter personal.

XXI. CONTESTAREA

141. ***Politica*** poate fi contestată în parte sau în totalitate în instanța de judecată doar de către persoanele față de care se aplică prezenta Politică.
142. Persoanele care intenționează să-și realizeze calea de atac în instanța de judecată pot primi extras din ***Politică*** care instituie anumite restricții sau, documentul integral, cu condiția că aceștia, înainte de primire a documentului vor semna clauza de confidențialitate stabilită de ***Politică***.
143. Cerințele de securitate și de conformitate prevăzute de ***Politic***ă se aplică chiar dacă au fost contestate în instanța de judecată, până când clauzele regulatorii ale acesteia nu vor fi suspendate sau încetate prin act judecătoresc definitiv.

XXII. RĂSPUNDEREA

144. EUROPARC, persoana împuternicită de către EUROPARC, persoanele terțe după caz, pentru nerespectarea dispozițiilor ***Politicii*** - poartă răspundere civilă (Codul civil), contravențională (art. 74^1 Cod contravențional) și penală (art. art. 177, 178, 180 Cod penal).

XXIII. DISPOZIȚII FINALE

145. ***Politica*** se revizuiește ca rezultat al modificărilor sau reevaluării componentelor acesteia și se actualizează după caz, dar nu mai puțin de odată în an.

146. ***Politica*** se completează și este dezvoltată prin cerințele contractuale, regulamente, instrucțiuni, indicații orale și scrise.