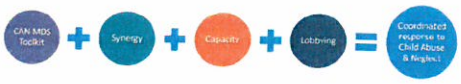


ACT ADITIONAL NR. 1 LA
PROTOCOLUL DE COLABORARE NR.36083
DIN DATA 15.04.2020
PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL în cadrul proiectului „Răspuns coordonat în cazurile de abuz și neglijare a copilului prin intermediul unui set minim de date: de la planificare la aplicare "CAN-SMD II"

Părți:

FEDERAȚIA ORGANIZAȚIILOR NEGUVERNAMENTALE PENTRU COPIL - FONPC, cu sediul social în România, Bucuresti, Strada Matei Basarab, nr. 41, etaj 1, sector 3, 030671, CIF [redacted] având contul IBAN [redacted], deschis la Banca [redacted] în continuare numită FONPC, reprezentata prin Domnul Bogdan SIMION, în calitate de Președinte, denumită în continuare **„Operator"/ `Autoritatea Administrativă Națională CAN-SMD`**

si

DIRECȚIA GENERALĂ DE ASISTENȚĂ SOCIALĂ ȘI PROTECȚIA COPILULUI SECTOR 3, cu sediul în Bucuresti, str. Parfumului nr. 2--4, telefon: 0372.126.100, fax: 0372.126.101, cod de identificare fiscală [redacted] reprezentată legal prin DIRECTOR GENERAL - MIHAELA UNGUREANU

Au convenit încheierea următorului acord:

Termenii utilizați în prezentul Act adițional au sensul expus în Regulamentul UE nr. 679/2016 și în Legea nr. 190/2018.

Având în vedere obligațiile reciproce stabilite în Protocolul de colaborare încheiat în contextul proiectului **„Răspuns coordonat în cazurile de abuz și neglijare a copilului prin intermediul unui set minim de date: de la planificare la aplicare "CAN-SMD II" („Coordinated Response to Child Abuse and Neglect via a Minimum Data Set: from planning to practice 'CAN-MDS II'" (CAN MDS II), co-finanțat de Uniunea Europeană,** părțile convin ca termenii și condițiile enunțate mai jos să se adauge ca act adițional la Protocol.

1. CONTEXTUL PROIECTULUI

Scopul introducerii Setului Minimal de Date privind Copilul Abuzat și Neglijat (CAN SMD) este colectarea de date comparabile și fiabile pe baza unor definiții comune din mai multe sectoare (servicii sociale, judiciare, educaționale, sănătate).

2. OBLIGATIILE OPERATORULUI

2.1. Ținând seama de natura, domeniul de aplicare, contextul si scopurile prelucrării, precum si de riscurile cu grade diferite de probabilitate si gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi in măsura să demonstreze că prelucrarea se efectuează în conformitate cu prevederile Regulamentului (UE) 2016/679. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar. Măsurile mentionate mai jos urmează să fie aplicate de operator pe toată perioada de desfășureare a proiectului. Aceste măsuri vor fi completate în funcție de

necesitățile întâmpinate în practică, dar cu păastrarea principiilor Regulamentului de protecție a datelor si a măsurilor mai jos menționate.

Având în vedere stadiul actual al tehnologiei, costurile implementării, natura, domeniul de aplicare, contextul si scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pe care le prezintă prelucrarea datelor pentru drepturile și libertățile persoanelor fizice, atât in momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate, care sunt destinate să transpună eficient principiile de protecție a datelor, precum:

- reducerea la minimum a datelor incluse în sistem;
- integrarea unor instrumente de verificare a îndeplinirii cerințelor prezentului Regulament;
- protejarea drepturilor persoanelor vizate.

Astfel, operatorul pune in aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai acele date cu caracter personal care sunt absolut necesare pentru îndeplinirea scopurilor specifice ale prelucrării. Obligația de minimalizare se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare si accesibilității lor.

3. OBLIGAȚIILE ȘI ACTIVITĂȚILE OPERATORULUI ASOCIAT

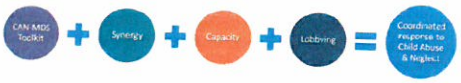
3.1. În cadrul "CAN-SMD II", o*peratorul asociat* prelucrează datele cu caracter personal numai pe baza instrucțiunilor documentate, stabilite împreună cu operatorul, cu respectarea regulilor de securitate și de acces în baza de date a operatorului (user+ parolă, etc), inclusiv în ceea ce privește transferurile de date cu caracter personal către terțe persoane sau instituții sau către o țară terță sau o organizație internațională, cu excepția cazului în care aceasta obligație îi revine instituției/organizației denumită OPERATOR ASOCIAT în temeiul dreptului Uniunii Europene sau al dreptului intern care i se aplică; în acest caz, operatorul asociat notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

OPERATORUL ASOCIAT va prelucra tipurile de date cu caracter personal referitoare la persoanele vizate, în scopurile specificate în prezentul Protocol de colaborare și nu va prelucra, transfera, modifica sau transforma datele cu caracter personal sau nu va dezvălui sau permite divulgarea acestora unei terțe părți decât în conformitate cu instrucțiunile operatorului, cu excepția cazului în care o astfel de prelucrare este impusă de legislația aplicabilă la care operatorul asociat este supus.

3.1. Obiectul si durata prelucrării datelor cu caracter personal sunt stabilite în Protocol, la secțiunea Principalele Responsabilități **ale AUTORITĂȚII ADMINISTRATIVE NAȚIONALE CAN-MDS - Federația Organizațiilor Neguvernamentale pentru Copil – FONPC (*'controlor de date'*)**, punctul F și la secțiunea Principalele Responsabilități **ale PARTENERULUI NAȚIONAL – DIRECȚIA GENERALĂ DE ASISTENȚĂ SOCIALĂ ȘI PROTECȚIA COPILULUI SECTOR 3** punctul C

3.2. Operatorul asociatprelucrează datele cu caracter personal comunicate, pe durata de aplicare a Protocolului și exclusiv in scopul executării obligațiilor asumate prin Protocol;

3.3. Tipurile de date cu caracter personal care urmează să fie prelucrate în baza de date CAN-SMD sunt următoarele informații privind copilul presupusa victimă a abuzului și neglijării: Vârstă, Sex, Data nașterii, Compoziția familiei (Tipul Familiei; Membrii familiei;Numărul membrilor), Îngrijitorii primari, Relația copilului cu îngrijitorul, Sexul îngrijitorului, Data nașterii îngrijitorului, Tipul de incident: maltratare/neglijare. În cele ce urmează (în rândurile de mai jos), ele vor fi denumite Date cu caracter personal;



3.4. Categoriile de persoane la care se referă datele menționate cu caracter personal sunt beneficiarii: copii și adolescenți (cu vârsta cuprinsă între 0 și 18 ani), cât și îngrijitorii acestora pentru care operatorul asociat asigură furnizarea de servicii sociale/educaționale/de sănătate și care sunt suspectați ca fiind victime ale abuzului și neglijării.

Categorii de date- **Axe și elemente de date**

Întrucât CAN-SMD își propune, printre altele, să promoveze descrierea standard a datelor și înțelegerea lor comună, armonizarea și standardizarea datelor în cadrul și între organizațiile care colaborează în cadrul aceluiași sector, sau din diferite sectoare, sunt colectate următoarele tipuri de date:

Informații despre "INCIDENT"
DE_I1: Identificarea / DI-ul incidentului
DE_I2: Data incidentului
DE_I3: Forma/ formele abuzului
DE_I4: Locația incidentului

Informații despre "COPIL"
DE_C1: Identificarea / DI-ul copilului
DE_C2: Sexul copilului
DE_C3: Data nașterii copilului
DE_C4: Cetățenia copilului

Informații despre "FAMILIE"
DE_F1: Compoziția familiei
DE_F2: Relația îngrijitorilor / îngrijitorului principal cu copilul
DE_F3: Sexul îngrijitorilor / îngrijitorului principal
DE_F4: Data nașterii îngrijitorilor / îngrijitorului principal

Informații despre "SERVICII"
DE_S1: Răspunsul instituțiilor
DE_S2: Referire/ referiri către servicii

Informații despre "ÎNREGISTRARE"
DE_R1: Identificarea / DI-ul agenției
DE_R2: Identificarea / DI-ul operatorului
DE_R3: Data înregistrării
DE_R4: Sursa de informare

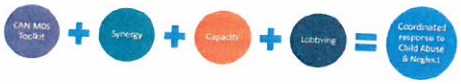
Datele cuprinse în registrul CAN-SMD sunt derivate din 18 elemente de date ordonate (în acord cu logica ISO / IEC 11179) în 5 *axe* (categorii de elemente de date), și anume: "ÎNREGISTRARE", "INCIDENT", "COPIL", "FAMILIE" și "SERVICII".

3.5. Operatorul asociat va lua măsuri rezonabile pentru a asigura conformitatea cu Legislația aplicabilă privind protecția datelor fiecărei persoane vizate (copii și îngrijitori) care poate avea acces la Datele cu caracter personal, asigurându-se în fiecare caz că accesul este strict limitat la persoanele care au atribuții profesionale privind accesarea Datelor cu caracter personal relevante, necesare pentru scopurile stabilite, în contextul obligațiilor acelui individ față de operatorul asociat. Măsurile luate de operatorul asociat privesc:

- informarea tuturor persoanelor care lucrează cu datele proiectului CAN SMD cu privire la obligațiile operatorului asociat în baza acestui Act adițional și a Protocolului de colaborare în ceea ce privește Datele cu caracter personal;

- asigurarea de faptul că respectivii angajați au participat la cursuri de formare adecvate în legătură cu Legislația aplicabila privind protecția Datelor;

- prelucrarea datelor este supusă angajamentelor angajamentelor de confidențialitate sau obligațiilor profesionale sau legale de confidențialitate;



4. **Securitate**

4.1. Având în vedere stadiul actual al dezvoltării, costurile implementării, natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul pentru nerespectarea drepturillor și libertăților persoanelor fizice, operatorul asociat va implementa măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat riscului, (după caz, în funcție de gravitatea riscului se vor putea lua și alte măsuri):

- va asigura pseudonimizarea și criptarea Datelor cu caracter personal – după primirea pseudonimului de la Administratorul Național. Operatorii de date vor folosi pseudonimul primit (sau ID temporar pentru introducerea datelor despre incident/incidentele legate de acel copil)

- va asigura capacitatea de a păstra confidențialitatea, integritatea, disponibilitatea și funcționalitatea continua a sistemelor și serviciilor de prelucrare prin folosirea unor calculatoare sau alte mijloace tehnice securizate prin parole transmise confidențial;

  va asigura capacitatea de a restabili disponibilitatea Datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;

- va dezvolta un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea Prelucrării.

4.2. Fără a se limita la caracterul general al celor de mai sus și în special la obligația sa de a stabili oportunitatea oricăror măsuri tehnice și organizatorice suplimentare, operatorul asociat va implementa și va menține fiecare dintre măsurile tehnice și organizatorice enumerate în Anexa nr. 1 (*Măsuri Tehnice și Organizatorice*).

4.3. La evaluarea nivelului adecvat de securitate, operatorul asociat trebuie să țină seama în special de riscurile implicate de prelucrarea datelor, în special de distrugerea, pierderea, modificarea, dezvăluirea neautorizată sau accesul neautorizat la Datele cu caracter personal transmise, stocate sau altfel prelucrate.

4.4. Nivele de acces ale agențiilor și operatorilor

Responsabilități în gestionarea cazurilor CAN	**Nivel de acces**
Autoritatea Administrativă Națională CAN-SMD prin Administratorul Național	**Acces total (nivel 0)**
Instituții/persoane cu responsabilități de luarea deciziilor prin acțiuni legale: - Scoaterea copilului din familie - Decăderea părinților din drepturi, Suspendarea drepturilor părintești - Stabilirea dacă există suficiente dovezi pentru urmărirea penală (a presupușilor infractori)	**Acces deplin pentru a vedea datele la nivel județean (nivel 1)**

Instituții/persoane responsabile pentru furnizarea de servicii în vederea administrării cazurilor: - Realizarea unor evaluări inițiale pentru cazurile suspectate - Furnizarea de servicii pentru victimele CAN (diagnostic /diagnoză socială / tratament, terapie / consultație /îngrijire) - Furnizarea de servicii pentru familiile victimelor CAN (de sprijin) - Urmărirea cazurilor CAN (follow-up)	**Acces Limitat (nivel 2) pentru a vedea cazurile aflate în propria administrare**
Neimplicarea efectivă în administrarea cazurilor raportate / detectate: - Sesizarea autorităților (opțional) cu privire la cazurile CAN (suspectate) - Raportarea în mod obligatoriu a cazurilor CAN (suspectate) - Aplicarea de screening/ scanarea populației generale a copiilor pentru CAN - Furnizarea măsurilor de protecție de urgență pentru victimele CAN - Furnizarea de consultanță juridică/apărare (advocacy) pentru cazurile CAN	**Acces limitat (nivel 3) pentru a-și vedea propriile informații introduse**

În cazul de față, OPERATORUL ASOCIAT se încadrează la Nivelul de Acces nr. .....

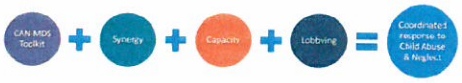
5. Drepturile persoanelor vizate

5.1. Operatorul asociat va prelucra datele personale ale minorilor în baza:

- Legii nr. 272/2004 privind protecția și promovarea drepturilor copilului
- HOTĂRÂRII nr. 49 din 19 ianuarie 2011 pentru aprobarea Metodologiei-cadru privind prevenirea și intervenția în echipă multidisciplinară și în rețea în situațiile de violență asupra copilului și de violență în familie și a Metodologiei de intervenție multidisciplinară și interinstituțională privind copiii exploatați și aflați în situații de risc de exploatare prin muncă, copiii victime ale traficului de persoane, precum și copiii români migranți victime ale altor forme de violență pe teritoriul altor state

5.2. Temeiul prelucrării datelor cu caracter personal este protejarea intereselor vitale ale persoanei vizate sau ale altei persoane fizice (art 6 din Regulamentul (UE) 2016/679, alin 1, litera d), mai precis a minorului care se află în risc de abuz și/sau neglijare.

5.3. Operatorul asociat prin reprezentanții săi (operatorii de date) va notifica prompt Operatorul - Autoritatea Administrativă Națională CAN-SMD, prin Administratorul Național de fiecare dată



când va primi o solicitare de introducere în baza de date a unui caz sau suspiciune de abuz/neglijare, în urma căreia va primi un pseudonim pentru minorul în cauză pentru introducerea în baza de date.

5.4. Operatorul asociat va coopera cu operatorul - Autoritatea Administrativă Națională CAN-SMD , pentru a permite operatorului să respecte orice exercitare a drepturilor de către o Persoană Vizată în temeiul oricărei Legislații aplicabile privind protecția Datelor cu privire la Datele cu caracter personal și să respecte orice evaluare, anchetă, avertizare sau investigație conform Legislației aplicabile privind protecția Datelor a Datelor cu caracter personal sau a acestui act adițional, inclusiv prin:

➢ Furnizarea tuturor Datelor solicitate de operator într-un interval de timp rezonabil specificat de operator în fiecare caz, inclusiv detalii complete și copii ale reclamației, comunicării sau solicitării și orice Date cu caracter personal pe care le deține în legătură cu o Persoană Vizată;

➢ Punerea în aplicare a oricăror măsuri tehnice și organizatorice suplimentare pe care operatorul le-ar putea solicita în mod rezonabil pentru a permite operatorului să răspundă în mod eficient plângerilor, comunicărilor sau solicitărilor relevante.

6. **Încălcarea securității Datelor cu caracter personal**

6.1. Operatorul asociat va notifica operatorul cu promptitudine, dar în orice caz (în maxim 24 ore), după ce va identifica o Încălcarea a securității Datelor cu caracter personal, oferind suficiente informații care să permită operatorului să îndeplinească orice obligație de a raporta o Încălcare a securității Datelor cu caracter personal conform Legislației aplicabile privind protecția Datelor. Această notificare, în măsura în care sunt implicate Datele cu caracter personal , trebuie:

➢ să descrie natura Încălcării securității datelor cu caracter personal, categoriile și numărul de Persoane vizate în cauză, precum și categoriile și numerele înregistrărilor de Date cu caracter personal în cauză;

➢ să includă numele și datele de contact ale responsabilului cu protecția datelor al operatorului asociat sau ale altei persoane de contact relevante, de la care pot fi obținute mai multe informații;

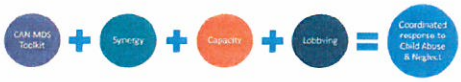
➢ să descrie consecințele probabile ale Încălcării securității datelor cu caracter personal, cât și să descrie măsurile luate sau propuse a fi luate pentru a soluționa Încălcarea securității Datelor cu caracter personal.

6.2. Operatorul asociat va coopera cu operatorul și va întreprinde demersuri rezonabile, în conformitate cu instrucțiunile operatorului, pentru a ajuta la investigarea, atenuarea și remedierea fiecărei Încălcări a securității Datelor cu caracter personal.

7. **Evaluarea impactului privind protecția Datelor și consultarea prealabilă**

7.1. Operatorul asociat va oferi suport rezonabil operatorului cu privire la toate evaluările de impact privind protecția Datelor solicitate în temeiul articolului 35 RGPD și la orice consultări prealabile adresate oricărei autorități de supraveghere a datelor, care sunt solicitate în temeiul articolului 36 RGPD, referitoare la Prelucrarea Datelor cu caracter personal de către operatorul asociat în numele operatorului- Autoritatea Administrativă Națională CAN-SMD și luând în considerare natura prelucrării și a informațiilor disponibile operatorului asociat.

8. **Ștergerea sau returnarea Datelor cu caracter personal.**



8.1. După finalizarea introducerii datelor în sistem, operatorul asociat va șterge prompt și va asigura ștergerea tuturor copiilor/ exemplarelor duplicate, Datelor cu caracter personal prelucrate, în măsura în care nu are obligația legala a păstrării datelor, deci păstrând doar acele date care sunt strict necesare activității lor.

8.2. Operatorul asociat poate păstra Datele cu caracter personal în măsura cerută de legislația aplicabilă și numai în măsura și pentru perioada prevăzută de legislația aplicabilă și întotdeauna cu condiția ca acesta să asigure confidențialitatea tuturor acestor Date cu caracter personal și să se asigure că aceste date cu caracter personal sunt prelucrate numai dacă este necesar pentru scopul (scopurile) specificat(e) în legislația aplicabilă, care impun stocarea acestora și pentru niciun alt scop.

9. **Răspundere**

FEDERAȚIA ORGANIZAȚIILOR NEGUVERNAMENTALE PENTRU COPIL – FONPC, în calitate de Autoritatea Administrativă de Date și Operator nu poate răspunde pentru eventualele situații în care nu au fost respectate regulile privind protecția datelor personale de către operatorii de baze de date, angajați ai Operatorului Asociat.

Autoritatea Administrativă Națională CAN-SMD

Federația Organizațiilor
Neguvernamentale pentru Copil
Președinte
Bogdan SIMION

[redacted]

Direcția Generală de Asistență Socială
și Protecția Copilului Sector 3
Director General
M[redacted]

Direcția Juridică
Director Executiv,
Vasile DOBRANI[redacted]

Consilier Juridic,
[redacted]

ANEXA 1 LA ACTUL ADITIONAL NR...../.....

SECURIZAREA DATELOR

1. Toate datele din sistem vor fi introduse pe platforma **CAN-SMD**. Toate documentele fizice (ciornele cu date) vor fi tocate/distruse în condiții de securitate. Datele la care ne referim sunt: vârstă, sex, data nașterii, compoziția familiei (Tipul Familiei; Membrii familiei;Numărul membrilor) , Îngrijitorii primari, Relația copilului cu îngrijitorul, Sexul îngrijitorului, Data nașterii îngrijitorului, tipul de incident: maltratare/neglijare (conform Art. 3.4 la protocol)

2. Cu ocazia proiectării, întreținerii, actualizării aplicațiilor de gestiune a bazelor de date, se interzice accesul programatorilor/personalului de întreținere a sistemelor informatice la orice fel de date cu caracter personal deținute/ create/ accesate de personalul din structura respectivă. În aceste situații, se pun la dispoziția programatorilor/personalului de întreținere numai date anonime.

CERINȚELE MINIME DE SECURITATE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

3. Prezentele cerințe minime de securitate a prelucrărilor de date cu caracter personal trebuie să stea la baza adoptării și implementării de către operatorii asociați a măsurilor tehnice și organizatorice necesare pentru păstrarea confidențialității și integrității datelor cu caracter personal.

4. ***Identificarea și autentificarea utilizatorului- operator de date***

4.1. Prin **utilizator**- operator de date se înțelege orice persoană care acționează sub autoritatea OPERATORULUI ASOCIAT, cu drept recunoscut de acces la bazele de date cu caracter personal.
4.2. Fiecare reprezentant al operatorului asociat va avea un USER și o PAROLĂ/ Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal, trebuie să se identifice. Identificarea se poate face prin mai multe metode, cum ar fi:
4.2.1. Introducerea codului de identificare de la tastatură (un șir de caractere)- USER,
4.2.2. Introducerea unei parole stabilită personal – PAROLĂ SECURIZATĂ
4.3. Fiecare utilizator are propriul său user
4.4. Orice cont de utilizator este însoțit de o modalitate de autentificare. Autentificarea poate fi făcută prin introducerea unei parole
4.5. Parolele sunt șiruri de caractere. Cu cât șirul de caractere este mai lung, cu atât parola este mai greu de aflat. La introducerea parolelor acestea nu trebuie să fie afișate în clar pe monitor. Parolele trebuie schimbate periodic în funcție de politicile de securitate ale entității (operator sau persoană împuternicită). Schimbarea periodică a parolelor se face numai de către utilizatori autorizați de operator.

4.6. Orice utilizator care primește un cod de identificare și un mijloc de autentificare trebuie să păstreze confidențialitatea acestora și să răspundă în acest sens în fața operatorului.
4.7. Fiecare entitate va stabili o procedură proprie de administrare și gestionare a conturilor de utilizator.
4.8. Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de conducerea entității.

5. Tipul de acces

5.1. Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea pașilor din protocolul de colectare de date. Pentru aceasta, se vor accesa datele în funcție de nivelul de acces din prezentul protocol- Nivel acces nr. .....

5.2. Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. Operatorul va permite accesul programatorilor la datele cu caracter personal după ce acestea au fost transformate în date anonime.

5.3. Operatorul va stabili modalitățile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru această prelucrare de date cu caracter personal trebuie limitată la câțiva utilizatori.

6. Colectarea datelor

6.1. Operatorul asociat desemnează operatori de date, care au participat la programul de formare pentru folosirea sistemului CAN-SMD pentru operațiile de colectare și introducere de date cu caracter personal într-un sistem informațional

6.2. Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizați desemnați de operator.

7. Computerele și terminalele de acces

7.1. Computerele și alte terminale de acces vor fi instalate în încăperi cu acces restricționat.

7.2. Dacă pe ecran apar date cu caracter personal asupra cărora nu se acționează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă automat.

8. Fișierul de acces

8.1. Operatorul- Autoritatea Administrativă Națională CAN-SMD este obligat să ia măsuri ca orice caz introdus în baza de date să fie înregistrat într-un registru pentru prelucrările manuale de date cu caracter personal. Informațiile înregistrate în fișierul de acces sau în registru vor fi:

8.1.1. Codul de identificare (numele operatorului de date din cadrul operatorului asociat);

8.1.2. Numele fișierului accesat (fișei)- pseudonimul minorului;

8.1.3. Numărul înregistrărilor efectuate;

8.1.4. Tipul de access al operatorului de date.

8.1.5. Data accesului (an, lună, zi).

9. Sistemele de telecomunicații

9.1. Partenerii sunt obligați să facă periodic controlul autentificărilor și tipurilor de acces pentru detectarea unor disfuncționalități în ceea ce privește folosirea sistemelor de telecomunicații.

9.2. Partenerii sunt obligați să conceapă sistemul de telecomunicații astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicații nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmisia datelor cu caracter personal.

9.3. Prin sistemele de telecomunicații se vor transmite numai datele cu caracter personal strict necesare.

10. Instruirea personalului

10.1. În cadrul cursurilor de pregătire a operatorilor de date, operatorul este obligat să facă informarea acestora cu privire la prevederile Regulamentului UE 679/2016 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității utilizatorului.

10.2. Operatorii de date care au acces la date cu caracter personal vor fi instruiți de către operator asupra confidențialității acestora și vor fi avertizați prin mesaje care vor apărea pe monitoare în timpul activității. Utilizatorii sunt obligați să își închidă sesiunea de lucru atunci când părăsesc locul de muncă.

11. Folosirea computerelor

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virușilor informatici) operatorul va lua măsuri care vor consta în:

11.1. interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;

11.2. informarea utilizatorilor în privința pericolului privind virușii informatici;

11.3. implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice.

12. Imprimarea datelor

12.1. Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați pentru această operațiune de către operator. Operatorii sunt obligați să aprobe proceduri interne specifice privind folosirea și distrugerea acestor materiale.

Nr. 822 /21.12.2020

ACT ADITIONAL NR. 2 LA
PROTOCOLUL DE COLABORARE
DIN DATA 15.04.2020
„Răspuns coordonat în cazurile de abuz și neglijare a copilului prin intermediul unui set minim de date: de la planificare la aplicare "CAN-MDS II"

Părți:

FEDERAŢIA ORGANIZAŢIILOR NEGUVERNAMENTALE PENTRU COPIL - FONPC, reprezentată prin Domnul Bogdan SIMION, în calitate de Președinte FONPC - denumită în continuare `Autoritatea Administrativă Națională CAN-MDS`
și

Direcția Generală de Asistență Socială și Protecția Copilului Sector 3, reprezentată prin Doamna Mihaela UNGUREANU, în calitate de Director General denumit(ă) în continuare "partener național",

Hotărăsc modificarea punctului 12.3 - Cap. XII Dispoziții finale - adică prelungirea protocolului de colaborare cu încă 7 luni, pentru participarea partenerului național la etapa de pilotare a sistemului CAN-MDS.

În acest sens, durata acordului de parteneriat se prelungește până la 31 Iulie 2021.

Reprezentant FONPC

Bogdan Simion
Președinte

[redacted]

Reprezentant Partener Național

Mihaela Ungureanu
Director Ge

[redacted]

[redacted]