POLITICA DE CONFIDENȚIALITATE CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL DE CĂTRE

CUPRINS:

În conformitate cu prevederile LEGII Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal, SC”Totul pentru copii” SRL S.R.L. prelucrează date cu caracter personal cu respectarea principiilor menționate în continuare, în scopuri legitime.

Prelucrarea datelor cu caracter personal se realizează prin mijloace mixte (manuale și automate), cu respectarea cerințelor legale și în condiții care să asigure securitatea, confidențialitatea și respectarea drepturilor persoanelor vizate.

1. COLECTAREA DATELOR CU CARACTER PERSONAL

Scopul acestei politici de securitate este acela de a asigura nivelul corespunzător al protecţiei datelor cu caracter personal ale persoanelor vizate, prin aplicarea corespunzătoare a legislaţiei naţionale cu referire la protecţia datelor şi confidențialitatea comunicării.

2. PRINCIPII ALE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Notificarea:

Operatorul de date cu caracter personal este notificat la Centrul Național pentru Protecția Datelor cu Caracter Personal al RM;

Legalitatea:

Prelucrarea datelor cu caracter personal este realizată cu bună-credință și se face în temeiul și în conformitate cu prevederile legale;

Scopul bine-determinat:

Orice prelucrare de date cu caracter personal se face în scopuri bine determinate, explicite și legitime, adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate;

Informarea:

Prin prezenta informare persoanele iau cunoștință despre faptul că li se vor prelucra date cu caracter personal;

Stocarea:

Datele cu caracter personal nu se stochează pentru o perioadă mai lunga decât este necesar pentru realizarea scopurilor în care au fost colectate;

Protejarea persoanelor vizate:

Prelucrarea datelor cu caracter personal va fi realizată de persoanele împuternicite din cadrul companiei SC ”Totul pentru copii” SRLsau de către alte persoane împuternicite în condițiile legii.

Securitatea:

Măsurile tehnice și organizatorice de securitate a datelor cu caracter personal sunt stabilite pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat (accesul la bazele de date a utilizatorilor se face pe baza de nume utilizator și parola fiind reglementat prin roluri și drepturi de acces). Posibilitatea de alterare a datelor accesate este protejată prin firewall monitorizat de SC ”Totul pentru copii” SRL, precum și de soluții antivirus actualizat permanent. Transferul între server clienți și administratori sau operatori se face criptat pe baza unui certificat digital, astfel datele nu pot fi interceptate.

3. POLITICA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

În conformitate cu dispozițiile LEGII Nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal, SC ”Totul pentru copii” SRL are obligația de a administra în condiții de siguranță și numai pentru scopurile prezentate mai jos, datele personale care îi sunt furnizate.

SC ”Totul pentru copii” SRL se obligă să păstreze confidențialitatea datelor personale furnizate prin intermediul site-ului www.baby-boom.md , așa cum prevăd dispozițiile LEGII Nr. 133 din 08.07.201 cu modificările ulterioare privind protecția datelor personale.

4. CERINȚELE FAȚĂ DE ASIGURAREA SECURITĂȚII DATELOR CU CARACTER PERSONAL

Prezintă riscuri speciale pentru drepturile şi libertăţile persoanelor următoarele categorii ale operaţiunilor de prelucrare a datelor cu caracter personal:

1) adaptarea, modificarea, dezvăluirea prin transmitere, difuzare sau în orice alt mod, a datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, de apartenenţa la un partid politic sau o organizaţie religioasă, a datelor cu caracter personal privind starea de sănătate sau viaţa intimă, precum şi a datelor cu caracter personal referitoare la condamnările penale, măsurile de constrângere, sancţiunile disciplinare sau contravenţionale;

2) operaţiunile de prelucrare a datelor genetice, biometrice şi a datelor care permit localizarea geografică a persoanelor prin intermediul reţelelor de comunicaţii electronice;

3) operaţiunile de prelucrare a datelor cu caracter personal prin mijloace electronice, având ca scop evaluarea unor aspecte de personalitate, precum competenţa profesională, credibilitatea, comportamentul etc.;

4) operaţiunile de prelucrare a datelor cu caracter personal prin mijloace electronice în cadrul unor sisteme de evidenţă, având ca scop analizarea solvabilităţii, a situaţiei economico-financiare, a faptelor susceptibile de a atrage răspunderea disciplinară, contravenţională sau penală a persoanelor fizice;

5) operaţiunile de prelucrare a datelor cu caracter personal ale minorilor în scopuri comerciale (activităţilor de marketing direct);

6) operaţiunile de prelucrare a datelor cu caracter personal menţionate la subpunctele 1) şi 2) din prezenta anexă, precum şi datele cu caracter personal ale minorilor, colectate prin intermediul Internetului sau mesageriei electronice.

Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (în continuare – Cerinţe) au drept scop stabilirea regulilor minime de implementare de către deţinătorii de date cu caracter personal a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale de date cu caracter personal şi/sau registrelor ţinute manual, în conformitate cu prevederile Legii nr.17-XVI din 15 februarie 2007 cu privire la protecţia datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2007, nr.107-111, art.468) şi ale Legii nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314).

Prezentele Cerinţe creează cadrul necesar aplicării Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28 ianuarie 1981, publicate în European Treaty Series, nr. 108, ratificate de Republica Moldova prin Hotărârea Parlamentului nr. 483-XIV din 2 iulie 1999.

Conform Hotărârii nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemului informaţional de date cu caracter personal şi vor fi efectuate neîntrerupt de către toţi deţinătorii de date cu caracter personal. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale de date cu caracter personal se înfăptuiesc ținându-se cont de necesitatea asigurării confidenţialităţii acestor măsuri. Înfăptuirea oricăror măsuri şi lucrări cu folosirea resurselor informaţionale ale deţinătorului de date cu caracter personal este interzisă în cazurile în care nu sânt adoptate şi implementate măsuri corespunzătoare de protecţie a datelor cu caracter personal.

SC ”Totul pentru copii” SRL certifică faptul că îndeplinește cerințele minime de securitate a datelor cu caracter personal.

SC ”Totul pentru copii” SRL utilizează metode și tehnologii de securitate, împreună cu politici aplicate membrilor și proceduri de lucru, inclusiv de control și audit, pentru a proteja datele cu caracter personal colectate conform prevederilor legale în vigoare. Transferul intre server clienți si administratori sau operatori se face criptat pe baza unui certificat digital, astfel datele nu pot fi interceptate.

Conform Hotărârii nr. 1123 din 14.12.2010 protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată în scopul:

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

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

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

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

5) păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.

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

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

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

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

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

Accesul în sediile/oficiile/birourile ori spaţiile unde sânt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare, cartele cu microprocesoare). Încăperile unde sânt instalate sistemele informaţionale de date cu caracter personal sunt echipate cu sisteme de control al accesului şi supraveghere video în scopul urmăririi accesului persoanelor în aceste spaţii.

În procesul monitorizării se utilizează mijloace de supraveghere şi alarmă în regim real de timp a tuturor cazurilor de acces autorizat şi/sau neautorizat. Sânt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat şi iniţierea acţiunilor de blocare a accesului. Computerele, serverele, alte terminale de acces sunt amplasate în locuri de maxima siguranța cu acces limitat pentru persoane străine.

Se asigură securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, se asigură posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI. Sunt prevăzute surse autonome de alimentare cu energie electrică de scurtă durată, care sânt folosite pentru terminarea

corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică. Se prevăd si mijloace de asigurare a securităţii antiincendiare a sediilor/oficiilor/birourilor unde sânt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal. Se implementează sisteme automatizate de depistare/semnalizare şi stingere a incendiilor în sediile/oficiile/birourile unde sânt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

Computerele, terminalele de acces şi imprimantele sânt deconectate la terminarea sesiunilor de lucru. Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sânt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii deţinătorului de date cu caracter personal.

Scoaterea şi introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează.

Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sânt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.

Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;

2) verificarea autenticităţii fiecărui utilizator;

3) obţinerea autorizaţiei de la persoana responsabilă pentru eliberarea ID-ului utilizatorului;

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

5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (inacţiune în perioada de maximum 2 luni);

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

Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicându-se prescripţii pentru prelucrarea ulterioară şi răspândirea acesteia, inclusiv indicându-se numărul de identificare unic al deţinătorului de date cu caracter personal. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum şi sânt documentate, supuse monitorizării şi controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoanele responsabile ale deţinătorilor de date cu caracter personal şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Accesul fără fir la sistemele informaţionale de date cu caracter personal este documentat, supus monitorizării şi controlului. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale deţinătorului de date cu caracter personal.

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

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

Se asigură confidenţialitatea datelor cu caracter personal transmise, utilizându-se mijloace de protecţie criptografică a informaţiei.

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

Deţinătorii de date cu caracter personal verifică cu regularitate, cel puţin o dată pe an, îndeplinirea măsurilor tehnice şi/sau organizaţionale luate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicaţii şi/sau efectuarea îmbunătăţirilor, în caz de necesitate. Controalele de securitate sânt actualizate de fiecare dată când deţinătorul de date cu caracter personal este reorganizat sau îşi schimbă infrastructura. În scopul verificării nivelului de protecţie a sistemelor informaţionale de date cu caracter personal, precum şi în scopul preîntâmpinării unor eventuale cazuri de acces ilicit sau întâmplător asupra acestor sisteme informaţionale, depistării locurilor slabe în mecanismele de protejare a acestora, Centrul întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaţionale de date cu caracter personal. Rezultatele controalelor efectuate de Centru sânt puse imediat la dispoziţia deţinătorului de date cu caracter personal, nivelul de protecţie a sistemelor informaţionale de date cu caracter personal a căruia a servit obiect al controlului, cu prescrierea, în caz de necesitate, a acţiunilor necesare de a fi întreprinse în vederea asigurării securităţii prelucrării datelor cu caracter personal.

5. DREPTURILE PERSOANEI VIZATE

În conformitate cu prevederile Legii nr. 133 din 08.07.2011, subiectul datelor cu caracter personal are următoarele drepturi:

· Dreptul la informare (art.12): este dreptul persoanei de a obține de la operator, la cerere și în mod gratuit, printr-o solicitare, confirmarea faptului că datele care o privesc sunt sau nu prelucrate de SC ”Totul pentru copii” SRL;

· Dreptul de acces la datele cu caracter personal (art.13): orice subiect al datelor cu caracter personal are dreptul să obţină de la operator, la cerere, fără întârziere şi în mod gratuit orice informație care îl privește despre datele cu caracter personal;

· Dreptul de intervenţie asupra datelor cu caracter personal (art.14): orice subiect al datelor cu caracter personal are dreptul de a obţine de la operator la cerere şi în mod gratuit, rectificarea, actualizarea, blocarea sau ştergerea datelor cu caracter personal a căror prelucrare contravine Legii sus menționate;

· Dreptul de opoziție al subiectului datelor cu caracter personal (art.16): dreptul subiectului de a se opune în orice moment, în mod gratuit, din motive întemeiate şi legitime legate de situaţia sa particulară, ca datele cu caracter personal care îl vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care legea stabileşte altfel. Dacă opoziţia este justificată, prelucrarea efectuată de operator nu mai poate viza aceste date;

· Dreptul de a nu fi supus deciziei individuale (art.17): orice persoană are dreptul de a cere anularea, în totalitate sau parțială, a oricărei decizii individuale care produce efecte juridice asupra drepturilor şi libertăţilor sale, fiind întemeiată exclusiv pe prelucrarea automatizată a datelor cu caracter personal destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul şi altele asemenea;

· Dreptul de a se adresa CNPDCP sau instanței de judecată (art.18): orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal efectuată ilegal sau căreia i-au fost încălcate drepturile şi interesele garantate de prezenta lege are dreptul de a sesiza instanţa de judecată pentru repararea prejudiciilor materiale şi morale.

Orice informație furnizată de către dumneavoastră va fi considerată și va reprezenta consimțământul dumneavoastră expres ca datele dumneavoastră personale să fie folosite de SC”Totul pentru copii” SRL în conformitate cu scopurile menționate mai jos.

Dacă doriți ca datele dumneavoastră personale să fie actualizate sau scoase din baza de date, ori aveți întrebări legate de confidențialitatea datelor, ne puteți contacta/notifica oricând utilizând datele de contact existente pe site.

Dacă nu doriți ca datele dumneavoastră să fie colectate, vă rugăm să nu ni le furnizați.

De asemenea, pentru a reclama nerespectarea drepturilor garantate de Legea nr. 133 din 08.07.2011persoana vizată se poate adresa la Centrului Național pentru Protecția Datelor cu Caracter Personal al RM sau/și instanțelor de judecată.

6. SCOPUL COLECTĂRII DATELOR CU CARACTER PERSONAL

SC ”Totul pentru copii” SRL prelucrează datele cu caracter personal ale clienților săi și altor persoane care au legătură sau iau contact cu acesta, care îi sunt furnizate prin navigarea pe site-ul www.baby-boom.md , în vederea emiterii și livrării mărfii procurate.

Datele cu caracter personal (date de identitate, adresa, cod numeric personal, număr de telefon, vârsta sau orice alte asemenea date care au fost furnizate) pot fi prelucrate și utilizate de către SC ”Totul pentru copii” SRLatât în scopurile emiterii și livrării mărfurilor comandate pe site-ul întreprinderii, cât și în scopul întocmirii unor baze de date și utilizarea acestora în viitoarele demersuri și activități ale operatorului, în conformitate cu prevederile Legii nr. 133 din 08.07.2011 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal.

SC ”Totul pentru copii” SRL nu va dezvălui unei terțe părți niciuna dintre datele dumneavoastră (informații personale sau informații opționale) fără acordul dumneavoastră, cu excepția cazului în care avem convingerea, de bună credință, că legislația ne impune acest lucru sau ca acest lucru este necesar pentru protejarea drepturilor sau a proprietății societății noastre.

7. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE A DATELOR CU CARACTER PERSONAL

SC ”Totul pentru copii” SRL organizează generarea înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal pentru următoarele evenimente:

- Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem (se înregistrează data şi timpul tentativei intrării/ieşirii; ID-ul utilizatorului; rezultatul tentativei de intrare/ieşire – pozitivă sau negativă);

- Se efectuează înregistrarea tentativelor de obţinere a accesului pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal;

- Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces;

- Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului şi statutului obiectelor de acces;

- Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces.

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

Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobişnuite sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul şi întreprinderea acţiunilor prestabilite în politica de securitate pentru astfel de cazuri.

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

Pentru asigurarea integrității informației care conține date cu caracter personal și a tehnologiilor informaționale se asigură identificarea, protocolarea şi înlăturarea deficienţelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri. Se asigură protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus. Se utilizează tehnologii şi mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaţionale de date cu caracter personal şi constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaţionale.

Pentru restabilirea informațiilor care conțin date cu caracter personal (pentru crearea copiilor de rezervă), reieşind din volumul prelucrărilor efectuate, individual SC ”Totul pentru copii” SRL stabileşte intervalul de timp în care se execută copiile de siguranţă a informaţiilor care conţin date cu caracter personal şi soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, ar în orice caz acest termen este mai mic de un an, care se păstrează în locuri protejate, în afara zonei de amplasare a acestei informaţii şi soft-urile de bază. Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

SC ”Totul pentru copii” SRL verifică cu regularitate, cel puţin o dată pe an, îndeplinirea măsurilor tehnice şi/sau organizaţionale luate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicaţii şi/sau efectuarea îmbunătăţirilor, în caz de necesitate. Controalele de securitate urmează a fi actualizate de fiecare dată când deţinătorul este reorganizat sau îşi schimbă infrastructura. În scopul verificării nivelului de protecţie a sistemelor informaţionale de date cu caracter personal, precum şi în scopul preîntâmpinării unor eventuale cazuri de acces ilicit sau întâmplător asupra acestor sisteme informaţionale, depistării locurilor slabe în mecanismele de protejare a acestora, Centrul întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaţionale de date cu caracter personal.

8. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAȚIONALE ȘI PROTECȚIA TEHNICĂ A INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL

Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate. Este asigurat mecanismul de informare neîntârziată a conducerii deţinătorului de date cu caracter personal despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal. Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii. Sunt utilizate mijloace automatizate pentru susţinerea procesului de prelucrare a incidentelor de securitate a sistemelor informaţionale de date cu caracter personal. Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent.

Este exclusă prezenţa necontrolată a persoanelor sau a mijloacelor de transport, precum şi instalarea întâmplătoare a antenelor, într-o zonă de minimum 15 metri de la locul amplasării mijloacelor tehnice principale ale sistemului informaţional de date cu caracter personal, în scopul asigurării securităţii prelucrării datelor cu caracter personal. Încăperile pentru servere se protejează contra scurgerii informaţiei care conţine date cu caracter personal din cauza emisiilor electromagnetice prin ecranarea încăperilor sau instalarea sistemelor de bruiaj electromagnetic, care se proiectează, realizează şi cercetează de întreprinderi specializate în domeniu. Se exclude sau se limitează instalarea neautorizată a altor dispozitive electrice, radio sau de alt gen în încăperile unde sânt amplasate mijloacele tehnice de prelucrare a datelor cu caracter personal, în scopul asigurării securităţii prelucrării datelor cu caracter personal. Utilajul, liniile căruia au ieşire în afara perimetrului controlat, este instalat la o distanţă de cel puţin 3 metri de la mijloacele TI în care sânt prelucrate date cu caracter personal.

SC ”Totul pentru copii” SRL

www.baby-boom.md