SWEDEN

UNDP

Empowered lives.
Resilient nations.

Ghid

privind dezvoltarea practicilor de asigurare a protecției datelor cu caracter personal

Octombrie 2016

Ghidul privind Dezvoltarea practicilor de asigurare a protecţiei datelor cu caracter personal a fost elaborat de Veronica Mocanu, în cadrul Proiectului „Consolidarea guvernării parlamentare în Moldova" finanțat de Guvernul Suediei şi implementat de Programul Națiunilor Unite pentru Dezvoltare (PNUD). Opiniile exprimate în acest document aparţin autoarei şi nu reprezintă neapărat opiniile instituțiilor menționate.

Design: **Bons Offices**

Descrierea CIP a Camerei Naționale a Cărții

Ghid privind dezvoltarea practicilor de asigurare a protectiei datelor cu caracter personal / intocmit de Mocanu Veronica; PNUD Moldova. – Chisinau : S. n., 2016 (Tipogr. "Foxtrot"). – 22 p.
Apare cu suportul financiar al Guvernului Suediei. – 150 ex.

ISBN 978-9975-89-040-3.
342.72/.73(478)
G 49

Cuprins

1. Necesitate

Siguranța în tratamentul datelor cu caracter personal și protecția acestora constituie un subiect de actualitate, fapt datorat conexării acestei tematici la cea privind protecția libertăților și principiilor democratice, pe care se bazează normele juridice europene. Acest interes a crescut considerabil în ultimii zece ani, în context cu progresele tehnologice.

Actualitatea este determinată de contextul global al valorificării protecției datelor cu caracter personal ca un drept fundamental și instituționalizarea reglementărilor legate de protecția datelor cu caracter personal în legislația Republicii Moldova, dar și conștientizarea tot mai frecventă a garanțiilor acordate către populația Republicii Moldova.

Odată cu adoptarea Legii Nr. 133 privind protecția datelor cu caracter personal[1] sunt instituite un șir de obligații pentru persoanele juridice și fizice ce prelucrează date cu caracter personal. Astfel, prezentul document se prezintă drept un scurt îndrumar cu privire la acțiunile ce urmează a fi întreprinse de către deputații din Parlamentul Republicii Moldova, care, în vederea îndeplinirii obligațiilor sale de bază, pot accesa tangențial date cu caracter personal a cetățenilor Republicii Moldova. În același context, prezentul ghid se adresează și personalului auxiliar al Parlamentului Republicii Moldova, avînd drept scop familiarizarea tuturor colaboratorilor instituției cu cerințele legale minime necesare a fi respectate în cazul derulării activităților de prelucrare a datelor cu caracter personal.

Totodată, ghidul atrage atenția reprezentanților instituției legislative supreme, că chiar dacă Parlamentul reprezintă autoritatea legislativă supremă a statului, această instituție și reprezentanții acesteia nu sunt scutiți de obligații de asigurare a protecției asupra datelor cu caracter personal avute în prelucrare.

Astfel, pe parcursul realizării oricărei activități de prelucrare a datelor cu caracter personal, deputații, dar și personalul auxiliar al Parlamentului, ar trebui să se asigure că activitățile de prelucrare sunt realizate în conformitate cu cerințele minime stabilite, corespund unui scop legal determinat, datele cu caracter personal sunt colectate într-o formă neexcesivă și nu aduc atingeri intereselor subiecților vizați, menținîndu-li securitatea și confedențialitatea.

(1) http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=340495

2. Aspecte introductive: Cunoaștem protecția datelor cu caracter personal prin 10 întrebări

1. Ce înțelegem prin noțiunea de date cu caracter personal?

La categoria datelor cu caracter personal urmează a fi atribuită 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.

EXEMPLE:
nume şi prenume
genul
data şi locul naşterii
cetăţenia
IDNP
imaginea
vocea
situaţia familială
situaţia militară
datele de geolocalizare/datele de trafic
porecla/pseudonimul
datele personale ale membrilor de familie
datele din permisul de conducere
datele din certificatul de înmatriculare
situaţia economică şi financiară
datele privind bunurile deţinute
datele bancare
semnătura
datele din actele de stare civilă
numărul dosarului de pensie
codul personal de asigurării sociale (CPAS)
codul asigurării medicale (CPAM)
numărul de telefon/fax
numărul de telefon mobil
adresa (domiciliului/reşedinţei)
adresa de e-mail
datele genetice
datele biometrice şi antropometrice
datele dactiloscopice
profesia şi/sau locul de muncă
formarea profesională – diplome – studii
obişnuinţele/preferinţele/comportamentul
caracteristicile fizice

2. Care sunt datele cu caracter personal speciale și de ce acestora urmează să li se atragă o atenție sporită?

Datele cu caracter personal, în dependență de riscul care-l pot aduce persoanei în caz de prelucrare neadecvată sunt categorizate în două tipuri: **date cu caracter personal obișnuite (N1) și date cu caracter personal speciale (N2)**[2]. În general, prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepția cazurilor reglementate de prevederile art. 6 al Legii privind protecția datelor cu caracter personal. Astfel, deputații și personalul auxiliar al Parlamentului ar trebui să atragă o atenție sporită activităților de prelucrare realizate asupra datelor cu caracter personal speciale, urmînd să respecte rigorile prescrise de prevederile art. 6 al Legii privind protecția datelor cu caracter personal precum și prevederile indicate pentru categoria de date N2 prescrise de Hotărîrea Guvernului 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

(2) Titulatură atribuită de Hotărîrea Guvernului 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal pentru a deosebi masurile de securitate ce urmează a fi împlimentate în caz de prelucrare a datelor cu caracter personal obișnuit N1) și date cu caracter personal speciale (N2)

EXEMPLE:
Datele care dezvăluie originea rasială
Originea etnică a persoanei
Convingerile politice
Convingeri religioase sau filozofice
Apartenenţa socială
Datele privind starea de sănătate sau viaţa sexuală
Datele privind condamnările penale, măsurile procesuale de constrîngere sau sancţiunile contravenţionale

3. Ce reprezintă activitatea de prelucrare a datelor cu caracter personal?

Activitatea de prelucrare a datelor cu caracter personal desemnează orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate.

EXEMPLE:
Colectarea
Înregistrarea
Organizarea
Stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea

4. Cine este operatorul de date?

Operator de date cu caracter personal poate fi orice 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.

EXEMPLU:
Operator: Secretariatul Parlamentului Republicii Moldova Calitatea de operator este înregistrată separat pentru fiecare sistem de evidenţă gestionat.

5. De cînd apare calitatea de operator?

De facto, calitatea de operator de date cu caracter personal apare din momentul inițierii activității de prelucrare iar ne-înregistrarea acestei calități conform prevederilor art. 74[1] alin. 2) Cod Contravențional dă naștere răspunderii contravenționale. Astfel, orice persoană fizică sau juridică ce intenționează să inițieze o activitate de prelucrare a datelor cu caracter personal, urmează inițial să-și înregistreze calitatea de operator notificînd CNPDCP despre activitățile ce intenționează să le realizeze[3], tipurile de date pe care și le propune să le prelucreze, obținînd astfel calitatea de operator de jure înregistrat în Registrul de evidență al operatorilor de date cu caracter personal[4].

6. Cine este persoana împuternicită de către operator?

Persoana împuternicită de către operator este orice persoană fizică sau persoană 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.

EXEMPLUL 1 :
O companie IT care prestează servicii de stocare a datelor și care stochează datele în numele și pentru operator, la indicațiile acestuia, va fi considerată drept persoană împuternicită de operator. În acest caz, pentru operațiunile de stocare a datelor în numele și pentru altă persoană, compania nu va fi considerată operator, ci persoană împuternicită de operator, deoarece prelucrarea de către ea se va limita la aplicarea cunoștințelor tehnice la prelucrarea datelor pe care le stochează. Volumul și categoriile de date stocate, perioada stocării și alte aspecte ale prelucrării datelor transmise acesteia sunt stabilite de operatorul de date.

(3) http://datepersonale.md/md/proc_nof/

(4) https://registru.datepersonale.md/web/guest/cautare-in-baza-de-date-cndpc

EXEMPLUL 2:

Personalul auxiliar al Parlamentului poate avea calitatea de persoană împuternicită într-un raport de prelucrare a datelor în cazul în care în virtutea funcţiei sau ordinului i s-au delegat anumite atribuţii de prelucrare a datelor cu caracter personal.

7. Cine poate fi terț într-un raport de prelucrare a datelor cu caracter personal?

Calitatea de terț într-o activitate complexă de prelucrare a datelor o poate avea orice persoană fizică sau persoană juridică de drept public ori de drept privat, alta decît subiectul datelor cu caracter personal, decît operatorul ori persoana împuternicită de către operator și decît persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite și este autorizată să prelucreze date cu caracter personal.

EXEMPLU:

Deputatul poate avea calitatea de terţ într-un raport de prelucrare a datelor cu caracter personal în situaţia în care către acesta sunt dezvăluite datele personale a unui şir de cetăţeni în contextul unei activităţi de control a executării legilor.

În această situaţie însă, deputatul trebuie să-şi întemeieze demersul în faţa instituţiei de la care urmează să primească informaţia, indicînd scopul colectării datelor şi temeiul legal, fiind obligat totodată să-şi asume responsabilităţi de securitate şi confidenţialitate.

8. De ce este important să deosebim calitățile subiecților implicați în activitățile de prelucrare a datelor cu caracter personal?

Este important să deosebim rolul subiecților implicați într-un proces de colectare în special datorită determinării răspunderii, drepturilor și obligațiilor, precum și în vederea organizării activității de prelucrare a datelor cu caracter personal.

RECOMANDARE:

Deputaţilor le atragem atenţia, că în vederea evitării unor situaţii de conflict cu autorităţile responsabile de prelucrare de date, atunci cînd înaintează demersuri de acces la informaţii cu caracter personal, aceştia sunt obligaţi să indice temeiul legal al unei astfel de solicitări şi să ilustreze legătura cauzală între scop şi demersul înaintat, asumîndu-şi totodată obligaţii corespunzătoare de securitate.

9. Ce rol și ce atribuții poate avea deputatul în cazul în care demarează activități de prelucrare a datelor cu caracter personal în baza funcției deținute?

În temeiul funcției deținute, deputatul Republicii Moldova participă la controlul executării legilor. **El poate lua cunoștință de documentele necesare și participă la exercitarea controlului, în chestiuni ce țin de competența Parlamentului, asupra activității organelor de stat și celor obștești, a unităților**. În realizarea acestor atribuții însă, deputatul urmează să respecte prevederile legislației privind protecția datelor cu caracter personal, în special în ceia ce privește accesul la date, procesul de colectare, respectarea drepturilor subiecților datelor cu caracter personal și menținerea securității.

10. Ce este depersonalizarea datelor?

Depersonalizarea datelor presupune modificarea datelor cu caracter personal astfel încît detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă.

3. Domeniul de aplicare a legislației privind protecția datelor cu caracter personal

În Republica Moldova, **Legea Nr. 133 privind protecția datelor cu caracter personal se aplică prelucrărilor efectuate asupra datelor cu caracter personal realizate**:

- prin intermediul sistemelor de prelucrare automatizată (computer) ce conțin date cu caracter personal;
- pe suport de hârtie sau în orice altă formă de prelucrare neautomatizată dacă fac parte dintr-un sistem informațional;
- printr-un sistem de evidență sau sunt destinate să fie incluse într-un astfel de sistem și conțin date cu caracter personal;
- indiferent de forma acestora: fotografii sau înregistrări video, imagini sau înregistrări ale vocii, date biometrice.

4. Principiile activităţii de prelucrare a datelor cu caracter personal

4.1. Datele urmează a fi prelucrate în mod corect

Corectitudinea în sensul activității de prelucrare urmează a fi înțeleasă drept capacitatea și calitatea operatorului de a fi deschis și transparent cu subiectul datelor, informîndu-l pe cel din urmă despre scopul activității de prelucrare și riscurile care ar putea să apară.

Transparența este întotdeauna importantă, dar mai ales în situațiile în care indivizii au posibilitatea de a alege cu privire la faptul dacă doresc să intre într-o relație cu tine sau nu. În cazul în care persoanele fizice știu de la bun început ce informații vor fi folosite și pentru ce, acestea vor fi în măsură să ia o decizie în cunoștință de cauză cu privire la posibilitatea de a intra într-o relație, sau, poate, pentru a încerca să renegocieze termenii și condițiile contractuale sau să încerce modelarea comportamentului operatorului.

Evaluarea, dacă informațiile sunt procesate corect, ține și de modul în care au fost obținute aceste informații. În special, în cazul în care cineva este înșelat sau indus în eroare când se obține informația, atunci probabilitatea este redusă ca această activitate să fie catalogată drept prelucrare de date corectă

RECOMANDĂRI:

Operatorul ar trebui să dezvolte mecanisme corecte de prelucrare a informaţiei, tinzînd să prefere obţinerea informaţiei de la subiecţii vizaţi sau prin modalităţi expres prevăzute de lege drept posibile.

RECOMANDĂRI:
Pentru implementarea în practică a acestui principiu se recomandă deputaţilor să-şi remodeleze comportamentul cu cetăţenii şi instituţiile publice sau private în maniera în care să ofere suficiente informaţii cu privire la argumentarea comportamentului legal, transparent şi neabuziv.
Astfel, atunci cînd un deputat solicită furnizarea unei informaţii de la o anumită instituţie, întru evitarea situaţiilor de conflict, se recomandă indicarea expresă în demers a temeiului legal ce îi acordă dreptul de acces la o astfel de informaţii şi explicarea scopului solicitării înaintate.

4.2. Datele urmează a fi prelucrate în mod legal

O activitate va fi considerată în conformitate cu legislația, dacă are un temei juridic și este fundamentată pe norme clar definite, care reglementează modul în care va fi desfășurată activitatea în cauză.

Dacă este cazul, respectivele norme ar trebui, de asemenea, să stabilească în mod clar amploarea oricărei puteri discreționare conferite autorității de asigurare a respectării legii și orientării privind modul în care această putere discreționară ar trebui exercitată și să ofere garanții juridice adecvate.

RECOMANDĂRI:
Operatorul ar trebui să evalueze modalităţile de prelucrare, precum şi tipurile de informaţii prelucrate, urmînd să stabilească dacă pentru fiecare tip de informaţie colectată există normă legală ce permite prelucrarea, în caz contrar urmează să obţină consimţămîntul persoanei cu privire la demararea unei astfel de activităţi.
Atunci cînd în exercitarea activităţii de control parlamentar sunt întocmite chestionare, sau înaintate demersuri, acestea întodeauna urmează a fi însoţite de note explicative cu indicarea temeiului legal dar şi cu acordarea de garanţii de securitate.
Se recomandă, deputaţilor şi/sau secţiilor parlamentare să imprime pe actele ce conţin informaţii cu caracter personal text de genul *„Documentul conţine date cu caracter personal”, „Secţia Resurse Umane a Parlamentului Republicii Moldova este înregistrată cu nr.....în Registrul de evidenţă al operatorilor de date cu caracter personal şi autorizată cu drept de prelucrare”.*

4.3. Datele urmează a fi colectate în scopuri determinate, explicite şi legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri

Astfel, în temeiul acestui principiu trebuie să avem în vedere că stocarea de date trebuie să fie valabilă doar pe perioada atingerii scopului propus, iar odată ce scopul este atins datele nu mai urmează să fie stocate, cu excepția situației în care legea expres prevede acest fapt.

RECOMANDĂRI:	
Astfel, în vederea implementării în practică a respectivului principiu, ar fi necesar de revizuit formularele și acțiunile îndreptate spre colectarea de date, urmînd să verificăm dacă procesele de colectare de date au la bază realizarea unor scopuri legale și dacă aceste scopuri sunt sau nu întemeiate.	
În contextul celor sus indicate, întru evitarea practicilor defectuoase, ar fi cazul să ne remodelăm activitatea de prelucrare de date pornind de la următorul algoritm:	1. Stabilirea scopurilor;
	2. Identificarea datelor ce ar contribui la realizarea scopului;
	3. Identificarea temeiului legal pentru activitatea de prelucrare.

4.4. Datele urmează a fi prelucrate adecvat, pertinent şi neexcesiv în ceea ce priveşte scopul pentru care sînt colectate şi/sau prelucrate ulterior

Vor fi prelucrate numai datele care sunt „adecvate, pertinente și neexcesive în raport cu scopurile pentru care sunt colectate și/sau ulterior prelucrate”. Categoriile de date alese pentru prelucrare trebuie să fie necesare pentru a atinge scopul general declarat al operațiunilor de prelucrare, iar un operator ar trebui să limiteze colectarea de date strict la acele informații direct relevante pentru scopul specific urmărit de prelucrare.

RECOMANDĂRI:

Atunci cînd un operator este implicat în activități de colectare de date, obligatoriu trebuie să stabilească cauzalitatea între datele colectate și scopul propus, urmărind totodată să se colecteze doar datele strict necesare pentru realizarea scopului.

Astfel, dacă este necesar să se colecteze o informație doar cu referire la o anumită categorie de subiecți, este important să se urmărească ca acest proces de prelucrare să nu se extindă asupra unui număr mai mare de persoane, care nu au legătură cu scopul prestabilit.

4.5. Datele cu caracter personal, care fac obiectul prelucrării, trebuie să fie exacte şi, dacă este necesar, actualizate

Datele inexacte sau incomplete, din punct de vedere al scopului pentru care sînt colectate și ulterior prelucrate, se șterg sau se rectifică.

Tot în contextul colectării exacte de date apare și întrebarea cu privire la datele greșit înregistrate. Astfel, cu privire la datele greșit înscrise este important să existe un proces de evidență, monitorizare și raportare a erorilor admise.

RECOMANDĂRI:

Operatorul ar trebui să dezvolte un mecanism de actualizare a datelor în cazul în care utilizează sisteme informaţionale automatizate, asigurîndu-şi totodată posibilitatea înscrierii modificărilor realizate, temeiurilor acestora, data şi datele de autentificare a persoanelor responsabile.

Instituirea unor astfel de mecanisme, pe deoparte asigură cetăţeanului dereptul de control asupra procesului de prelucrare a datelor cu caracter personal, iar pe de altă parte acordă posibilitatea monitorizării accesărilor datelor şi instituirea mecanismului de securitate.

4.6. Datele cu caracter personal, care fac obiectul prelucrării trebuie să fie stocate într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sînt colectate și ulterior prelucrate

Stocarea datelor cu caracter personal pe o perioadă mai mare, în scopuri statistice, de cercetare istorică sau științifică, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri

RECOMANDĂRI:

Pentru fiecare categorie de date, operatorul urmează să-şi stabilească un scop, acest scop urmînd a fi prestabilit din timp. Odată cu expirarea termenului prestabilit, sau atingerea scopul, datele urmează a fi radiate sau arhivate în dependenţă de reglementările prestabilite pentru categoria respectivă de date.

Deputaţilor, li se atrage atenţia că ei sunt mandataţi cu drept de prelucrare a datelor cu caracter personal doar pe perioada mandatului, ulterior însă aceştia nu a drept de colectare dar urmează să-şi asume obligaţii de confidenţialitate.

În cazul în care există un act normativ care expres stabileşte termenul de prelucrare a datelor atunci acesta urmează a fi respectat.

5. Asigurarea drepturilor subiectului protecţiei datelor cu caracter personal

5.1. Dreptul de a fi informat despre prelucrarea datelor cu caracter personal

Dreptul de a fi informat despre acțiunile de prelucrare de date ca parte componentă a mecanismului de exercitare a dreptului la protecția datelor cu caracter personal, este instituit pornind de la ideia „transmiterii controlului asupra datelor personale". Individul fiind "proprietar" al datelor ce-l individualizează, este în drept să știe cine, pentru ce și în ce condiții urmează să folosească atributele sale, sau chiar imaginea sa. Mai mult decît atît, pornind de la ideia „proprietății" asupra propriei persoane și atributelor de individualizare, legislatorul a prevăzut expres că în spatele dreptului de a fi informat al persoanei vizate, trebuie să existe obligația expresă a operatorului de a informa subiectul de date despre o eventuală prelucrare de date.

Operatorul este obligat să ofere subiectului datelor cu caracter personal, la cerere, fără întîrziere și în mod gratuit, ***orice informație legată de***:

- confirmarea faptului, că datele care îl privesc sînt sau nu sînt prelucrate de acesta, de asemenea, informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sînt dezvăluite datele;
- comunicarea, într-o formă inteligibilă și într-un mod care nu necesită un echipament suplimentar, a datelor cu caracter personal, care fac obiectul prelucrării, precum și a oricărei informații disponibile privind originea acestor date;
- informații privind principiile de funcționare a mecanismului prin care se efectuează prelucrarea automatizată a datelor, care vizează subiectul datelor cu caracter personal;
- informații cu privire la consecințele juridice generate de prelucrarea datelor cu caracter personal pentru subiectul acestor date;
- informații privind modul de exercitare a dreptului de intervenție asupra datelor cu caracter personal.

În cazul în care datele cu caracter personal privind starea de sănătate sînt prelucrate în scop de cercetare științifică, dacă nu există riscul de a se aduce atingere drepturilor subiectului datelor cu caracter personal și dacă datele nu sînt utilizate pentru a lua decizii sau măsuri față de o anumită persoană, comunicarea informațiilor sus indicate se poate face într-un termen mai mare decît cel stabilit de Legea privind accesul la informație, în măsura în care aceasta ar putea afecta cercetarea sau rezultatul acesteia, dar nu mai tîrziu de momentul în care cercetarea este încheiată. Subiectul datelor cu caracter personal trebuie să își dea consimțămîntul ca datele privind starea de sănătate să fie prelucrate în scop de cercetare științifică, precum și asupra posibilei amînări din acest motiv a comunicării informațiilor prevăzute de cadrul legal in vigoare drept obligatoriu a fi adus la cunoștință.

5.2 Dreptul de acces la datele cu caracter personal prelucrate

În vederea asigurării continuității exercitării dreptului la protecția datelor cu caracter personal, este instituit dreptul de acces la datele personale ce se prezintă drept un instrument de control asupra îndeplinirii de către operator a obligației de a informa subiectul de date despre acțiunile de prelucrare ce le realizează sau urmează să le realizeze. În contextul dreptului de acces la datele personale, orice subiect al datelor cu caracter personal are dreptul să obțină de la operator, la cerere, fără întîrziere și în mod gratuit confirmarea faptului că datele care îl privesc, sunt sau nu sunt prelucrate de acesta, de asemenea informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele.

Orice subiect al datelor cu caracter personal are dreptul să obțină de la operator, la cerere, fără întîrziere și în mod gratuit:

- confirmarea faptului că datele care îl privesc sînt sau nu sînt prelucrate de acesta, de asemenea informații referitoare la scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sînt dezvăluite datele;
- comunicarea, într-o formă inteligibilă și într-un mod care nu necesită un echipament suplimentar, a datelor cu caracter personal care fac obiectul prelucrării, precum și a oricărei informații disponibile privind originea acestor date;
- informații privind principiile de funcționare a mecanismului prin care se efectuează prelucrarea automatizată a datelor care vizează subiectul datelor cu caracter personal;
- informații cu privire la consecințele juridice generate de prelucrarea datelor cu caracter personal pentru subiectul acestor date;
- informații privind modul de exercitare a dreptului de intervenție asupra datelor cu caracter personal.

5.3 Dreptul de intervenţie asupra datelor cu caracter personal

În sensul dreptului privind protecția datelor cu caracter personal, subiectul de date dispune nu doar de prerogativa de a solicita informații despre acțiunile de prelucrare ce sunt realizate, dar și de prerogativa de a interveni asupra activităților de prelucrare, prin înaintarea demersurilor legate de rectificarea, actualizarea, blocarea sau ștergerea datelor cu caracter personal a căror prelucrare contravine reglementărilor privind protecția datelor, în special datorită caracterului incomplet sau inexact al datelor.

Orice subiect al datelor cu caracter personal are dreptul de a obține de la operator sau persoana împuternicită de către acesta, la cerere și în mod gratuit:

- rectificarea, actualizarea, blocarea sau ștergerea datelor cu caracter personal a căror prelucrare contravine prezentei legi, în special datorită caracterului incomplet sau inexact al datelor;
- notificarea terților cărora le-au fost dezvăluite datele cu caracter personal despre operațiunile efectuate conform lit. a), exceptînd cazurile cînd această notificare se dovedește a fi imposibilă sau presupune un efort disproporționat față de interesul legitim care ar putea fi lezat.

5.4 Dreptul de opoziţie al subiectului datelor cu caracter personal

Tot în contextul dispunerii de dreptul la protecția datelor, individului i s-a atribuit în temeiul prevederilor art. 16 a Legii privind protecția datelor și prerogativa de a se opune activităților de prelucrare.

Subiectul datelor cu caracter personal are dreptul:

- de a se opune în orice moment, în mod gratuit, din motive întemeiate și legitime legate de situația sa particulară, ca datele cu caracter personal care îl vizează să facă obiectul unei prelucrări, cu excepția cazurilor în care legea stabilește altfel. Dacă opoziția este justificată, prelucrarea efectuată de operator nu mai poate viza aceste date.
- de a se opune în orice moment, în mod gratuit și fără nici o justificare, ca datele care îl vizează să fie prelucrate pentru prospectare comercială. Operatorul sau persoana împuternicită de către operator este obligată să informeze subiectul despre dreptul de a se opune unei astfel de lucrări înaintea dezvăluirii către terți a datelor sale cu caracter personal.

6. Acţiuni ce urmează a fi întreprinse în vederea asigurării implementării prevederilor Legii Nr. 133 privind protecția datelor cu caracter personal

Desemnarea persoanei responsabile pentru asigurarea protecției datelor cu caracter personal pe instituție.

Identificarea tuturor sistemelor informaționale prin intermediul cărora sunt prelucrate date cu caracter personal.

Elaborarea politicii de securitate pe instituție și a regulamentului de prelucrare a datelor cu caracter personal.

Aducerea la cunoștință tuturor subiecților implicați în procesul de colectare a datelor a textului politicii de securitate pe instituție și a regulamentului de prelucrare a datelor cu caracter personal contra semnătură.

Notificarea Centrului Național pentru Protecția Datelor cu Caracter Personal cu privire la sistemele informaționale utilizate și categoriile de date cu caracter personal prelucrate.

Afișarea numărului de operator întregistrat în Registrul de evidență a operatorilor de date cu caracter personal și **afișarea politicii de securitate** a instituției pe site-ul acesteia în vederea asigurării transparenței și famialirizării subiecților protecției cu drepturile pe care le dețin.

7. Măsuri organizatorice şi tehnice pentru asigurarea protecţiei datelor cu caracter personal

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 urmează a fi dezvoltate și implimentate neîntrerupt de către toți deținătorii de date cu caracter personal.

Operatorul este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

Aceste măsuri trebuie să asigure, potrivit stadiului tehnicii utilizate în procesul de prelucrare și de costuri, un nivel de securitate adecvat în ceea ce privește riscurile pe care le reprezintă prelucrarea, precum și în ceea ce privește natura datelor care trebuie protejate.

Astfel, în vederea conformării cu cadrul legal din domeniul protecției datelor cu caracter personal, fiind operator de facto, Parlamentul abordat drept instituție juridico-statală separată este obligat să-și remodeleze funcționalitatea și să realizeze acțiuni îndreptate spre implimentarea cerințelor minime de securitate în contextul activității exercitate.

Asigurarea protecției datelor cu caracter personal se impune a fi drept o activitate partajată, instituită și controlată de Președintele Paralamentului împreună cu responsabilul de protecția datelor pe instituție, realizată și implimentată la nivel individual de fiecare angajat al instanței.

Activitatea de protecție a datelor cu caracter personal este o activitate complexă și eforturile celor implicați în activitatea de securizare urmează a fi direcționate cel puțin pe două niveluri:

- Control administrativ,
- Securitatea mediului fizic și resurselor informaționale.

Controlul administrativ al protecției datelor cu caracter personal este o activitate ce urmează a fi dezvoltată și implimentată **atît la nivel central cît și individual.** La nivel central activitatea de asigurare a protecției datelor cu caracter personal urmează a fi realizată de Președintele Parlamentului, Vice-președintele Parlamentului pe perioada de lipsă sau vacanță a primului.

În contextul asigurării controlului pe instituție asupra procesului de prelucrare de date, Președintele urmează să **numească o persoană responsabilă de asigurarea protecției datelor cu caracter personal în cadrul instituției.** În sarcina respectivei persoane va fi pusă și activitatea legată de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, și aceasta va fi subordonată nemijlocit conducătorului instituției și nu va avea alte responsabilități incompatibile cu sarcinile funcției de implementare a politicii.

Persoana desemnată responsabilă de asigurarea protecției datelor cu caracter personal urmează să administreze pe instituție procesul de prelucrare de date, să delimiteze atribuțiile în conformitate cu cadrul legal în vigoare, să dispună eliberarea/suspendarea/sau încetarea operațiunilor de prelucrare, să monitorizeze incidentele de securitate și să elaboreze mecanisme de prevenire și remediere a situațiilor de fraudare a datelor cu caracter personal.

În vederea delimitării atribuțiilor și reglementării raporturilor de prelucrare de date **Persoana responsabilă din cadrul instituției împreună cu alți colaboratori urmează să elaboreze documentația** referitoare la politica de securitate a datelor cu caracter personal pe instituție și aceasta urmînd să conțină cel puțin următoarele documente:

1.	Regulamentul privind activitatea de prelucrare și asigurare a protecției datelor cu caracter personal (Regulamentul trebuie să delimiteze atribuțiile subiecților implicați în activitatea de prelucrare și urmează a fi adus la cunoștința angajaților contra semnătură);
2.	Nomenclatorul datelor cu caracter personal prelucrate, a localizării acestora şi a operaţiunilor efectuate asupra lor;
3.	Lista nominală a utilizatorilor, autorizaţi să acceseze datele cu caracter personal;
4.	Măsurile de securitate elaborate pe instituție;
5.	Mecanismul de punere în aplicare a măsurilor de securitate;
6.	Descrierea configuraţiei sistemului informaţional de date cu caracter personal şi a reţelei;
6.	Descrierea detaliată a criteriilor, în conformitate cu care sînt accesibile datele cu caracter personal prelucrate în registrul ţinut manual;
8.	Documentaţia tehnică cu privire la controalele de securitate;
9.	Orarul controalelor de securitate;
10.	Măsurile de detectare a cazurilor de acces şi/sau de prelucrare neautorizată a datelor cu caracter personal;
11.	Rapoarte despre incidentele de securitate.

Tot în contextul realizării controlului administrativ al activității de prelucrare de date, ***persoana responsabilă urmează*** să administreze procesul de acces la sistemele informaționale, accesul în afara împuternicirilor urmînd să fie considerat drept acces neautorizat. Înainte de acordarea accesului în sistem, utilizatorii urmează a fi 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.

Persoana responsabilă avînd atribuții de administrare, urmează să elaboreze și să implementeze un mecanism practic de control al acțiunilor angajaților instanței în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

La nivel individual fiecare angajat al instituției urmează să identifice personal datele ce urmează să le prelucreze în contextul activității realizate și acțiunile ce-i sunt puse în sarcină spre realizare, urmînd totodată să reevalueze scopul și să dezvolte mecanisme de administrare corecte și legale.

În vederea conformării față de prevederile cadrului legal privind necesitatea implimentării mecanismelor minime de protecție a datelor cu caracter personal, ar fi cazul să ne începem activitatea cu o analiză a activității de prelucrare a datelor cu caracter personal. Astfel, **în contextul procesului de evaluare, în dependență de atribuțiile exercitate trebuie să identificăm**:

- Ce atribuții de prelucrare de date ne sunt atribuite de lege prin funcția exercitată și cum realizăm respectivele acțiuni în corabore cu pevederile legislației privind protecția datelor cu caracter personal?
- Ce date cu caracter personal prelucrăm, nu sunt acestea excesive?
- Care este sursa datelor parvenite spre prelucrare, sunt acestea veridice?
- Care sunt formele de prelucrare?
- Prin intermediul căror resurse/sisteme informaționale prelucrăm datele cu caracter personal?
- Ce riscuri pot afecta procesele de prelucrare de date, cum le putem preveni?

8. Sugestii pentru dezvoltarea modalităţilor corecte de prelucrare a datelor cu caracter personal

În acest subcapitol sunt sugerate cele mai bune practici care pot fi aplicate de către membrii Parlamentului și funcționarii acestuia în vederea dezvoltării practicilor de asigurare a protecției datelor cu caracter personal.

8.1. Măsuri organizatorice

8.1.1. Identificarea tipurilor de date cu caracter personal care sunt prelucrate în cadrul unității, sau de către deputat, sau de către un funcționar anume.

8.1.2. Stabilirea tipului de date în dependență de categorie, date obișnuite sau date speciale.

8.1.3. Identificarea scopurilor pentru care sunt prelucrate datele cu caracter personal, verificînd dacă există temei legal pentru inițierea unui astfel de mecanism de prelucrare.

8.1.4. Evaluarea modalităților de prelucrare a datelor cu caracter personal, cu identificarea riscurilor ce ar putea aduce atingeri activităților de prelucrare.

8.1.5. Stabilirea termenului de stocarea a datelor cu caracter personal prelucrate.

8.1.6. Dezvoltarea mecanismelor de prevenire sau înlăturare promtă a riscurilor ce ar putea să afecteze procesul de prelucrare a datelor cu caracter personal.

8.1.7. Dezvoltarea mecanismului de acces la datele cu caracter personal, avînd în vedere că acestea pot fi dezvăluite doar cu consimțămîntul subiectului de date sau în limita prevederilor indicate în art. 6-9 a Legii privind protecția datelor cu caracter personal.

8.1.8. Dezvoltarea mecanismelor proprii de asigurare a drepturilor subiecților la protecția datelor cu caracter personal și anume a mecanismelor legate de asigurarea dreptului de informare despre prelucrare, acces asupra datelor prelucrate, intervenție asupra datelor prelucrate, opoziție, anulare sau radiere a datelor prelucrate prin mijloace exclusiv automatizate, acces în justiție.

8.2. Delimitarea responsabilităţilor şi formare

8.2.1. Toți subiecții, care în virtutea funcției, sunt implicați în activități de prelucrare a datelor cu caracter personal sunt obligați să-și asume responsabilități de asigurare a confidențialității consemnate prin acord și semnătură. Pentru personal, acestea pot fi prestabilite în contractul de angajare. Pentru voluntari, stagiari, consultanți acestea pot fi definite printr-un acord de confidențialitate.

8.2.2. Elaborarea și aducerea la cunoștința întregului personal a normelor de protecție a datelor cu caracter personal.

8.2.3. Desemnarea persoanei responsabile pentru protecția datelor cu caracter personal responsabilă pe instituție și persoanei responsabile pentru protecția datelor cu caracter personal responsabilă pe secție, în cazul secțiilor cu prelucrări masive de date cu caracter personal.

8.3. Securitatea informației

8.3.1. Securitatea mediului fizic

- A încuia oficiul de fiecare dată când acesta nu funcționează;
- A nu lăsa niciodată vizitatorii nesupravegheați;
- A se asigura ca ecranul calculatorului nu poate fi văzut de terți;

- Personalul de formare trebuie să cunoască când pot transmite informația altor persoane și să se consulte cu persoanele responsabile de protecția datelor atunci când acest lucru este neclar;

8.3.2. Protecția informației deținute la nivel electronic:

- Aplicarea controlului de acces pentru a restricționa accesul la informație;
- Utilizarea parolei pentru protejarea fișierelor salvate pe dispozitive de stocare portabile;
- Criptarea laptop-urilor și stick-urilor de memorie;
- Păstrarea informațiilor minime pe dispozitivele de stocare portabile;
- Asigurarea confidențialității parolelor;
- Copierea de rezervă a documentelor în mod regulat;
- Curățirea calculatoarelor și altor dispozitive electronice de stocare atunci când acestea nu mai sunt necesare;

8.3.3. Protecția înregistrărilor pe hârtie:

- Blocarea fișierele de hârtie atunci când acestea nu sunt în uz;
- Nimicirea prin mărunțire a deșeurilor cu conținut confidențial;
- A nu lăsa în jur sacii de gunoi cu deșeuri cu conținut confidențial;
- A transporta numai informații minime din birou;

8.3.4. Protecția informației deținute de către furnizori ai părților terțe prin:

- Obligarea lor să îndeplinească cerințele de protecție a datelor referitoare la securitatea contractelor lor;
- Crearea măsurilor de verificare dacă furnizorii de terțe părți respectă cerințele de securitate.

8.4. Informarea persoanelor

8.4.1 E necesar ca colaboratorii Parlamentului să fie deschiși și expliciți cu privire la acțiunile realizate asupra informația personale pe care o colectează.

8.4.2 Publicarea unei înștiințări de confidențialitate clare și informative pe site-ul instituției va ajuta oamenii să înțeleagă ce urmează să se întâmple cu datele lor personale. Dacă colectați date statistice în activitatea site-ului folosind cookie-uri (fișiere text care adună informații standarte de logare pe internet și de comportament al vizitatorilor), atunci trebuie să Vă referiți la acest lucru în notificarea dvs. de confidențialitate.

8.5. Listele de adrese, de marketing și lista electorală

8.5.1 Nu colectați date de contact ale alegătorilor din surse conexe, cu excepția cazului cînd sunteți sigur că ei doresc să faceți acest lucru.

8.5.2 Oricînd veți transmite materiale de marketing direct la alegători, trebuie să includeți detalii cu privire la modul în care aceștia pot refuza primirea unor astfel de materiale.

8.5.3 Veți avea grijă dacă veți considera să utilizați listele electorale pentru a contacta alegătorii. Lista electorală completă, care poate fi accesată de un membru al Parlamentului numai în scopuri legate de activitatea de deputat sau pentru scopuri electorale. Este o încălcare de a folosi lista electorală completă pentru orice alte scopuri.

8.6. Solicitări prin telefon

8.6.1 Fiți atent cînd cineva solicită informații personale prin telefon și nu distribuiți date personale, decât dacă sunteți sigur de persoana cu care vorbiți. Puteți verifica identitatea cuiva cerându-le să răspundă la o întrebare despre ceva din informația pe care o dețineți deja. Sau ați putea să cereți ca ei să aducă dovada identității lor la birou.

8.6.2 Puteți lua în calcul cererile primite prin telefon, dar este important să dezvoltați și mecanisme de identificare și securizare în acest sens. Este o bună practică de a lua notițe și a le trata la fel de atent ca pe alte documente din dosare cu regim confidențial.

8.7. Corespondența cu electoratul

8.7.1 În cazul în care cetățenii Vă contactează și nu este clar ce acțiune ei doresc să fie întreprinsă în urma contactării, verificați cu ei, astfel ca să devină clar. Nu folosiți datele personale pentru orice alt scop.

8.7.2 Asigurați-Vă că informațiile primite de la sau despre cetățeni să fie tratate în mod confidențial, dacă nu este indicat altfel.

8.7.3 Atunci când răspundeți prima dată unui cetățean care a cerut asistență, adăugați un paragraf standard, care dovedește că veți trata datele personale primite după cum este necesar pentru rezolvarea problemei lui, și că veți trata informația primită în conformitate cu rigorile legislative în vigoare.