MINISTERUL ENERGIEI
C.N.M.A.G.
CENTRUL NATIONAL
DE MANAGEMENT AL APEI GRELE

romania2019.eu
Romanian Presidency of the Council of the European Union

Sat Răscolești, comuna Izvorul Bârzii,
Calea Târgu Jiului, km 7, județul Mehedinți
C.I.F 38530608
Tel: 0252-707007
email cnmag.office@gmail.com

REGULAMENT

PRIVIND

PROTECŢIA DATELOR CU CARACTER PERSONAL

CAP. 1 DISPOZIŢII GENERALE

1.1.Obiect şi obiective

(1) Prezentul regulament stabileşte normele referitoare la protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestora, asigurând in acelasi timp protecţia drepturilor şi libertăţilor fundamentale ale persoanelor fizice şi în special a dreptului acestora la protecţia datelor cu caracter personal;

(2) Exercitarea drepturilor prevăzute în prezentul regulament nu poate fi restrânsă decât în cazurile expres şi limitativ prevăzute de lege.

(3) Libera circulaţie a datelor cu caracter personal în interiorul Uniunii Europene nu poate fi restricţionată sau interzisă din motive legate de protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

1.2.Domeniu de aplicare

(1) Prezentul regulament se aplica tuturor angajaţilor Centrului Național de Management al Apei Grele cu atribuţii de prelucrare a datelor cu caracter personal şi/sau, după caz, persoanelor împuternicite ale Centrului Național de Management al Apei Grele.

(2) Prezentul regulament se aplica prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

1.3.Termeni şi definiţii

1.În sensul prezentului regulament:

"Date cu caracter personal" înseamnă orice informaţii privind o persoană fizică identificată sau identificabilă ("Persoana vizata"). O persoana fizica identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

2."Prelucrare" înseamnă orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi:

- colectarea - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;
- înregistrarea - consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori neautomat, care poate fi registru, fişier automat, baza de date sau orice formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;
- organizarea - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul eficientizării/optimizării activităţilor de prelucrare a acestora;
- stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranţă;

- adaptarea - transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;

- modificarea - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;

- extragerea - scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;

- consultarea - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;

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

- dezvăluirea/divulgarea - a face disponibile date cu caracter personal către terţi prin comunicare, transmitere, diseminare sau punerea la dispoziţie în orice alt mod;

- alăturarea - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;

- combinarea/alinierea - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

- blocarea - întreruperea prelucrării datelor cu caracter personal;
restricţionarea - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

- ştergerea - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;

- transformarea - operaţiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;

- distrugerea - aducerea la stare de neîntrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

3."Creare de profiluri" înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoana fizică, în special pentru a analiza sau prevedea aspecte privind performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se afla persoana fizică respectivă sau deplasările acesteia;

4."Pseudonimizare/date anonime" înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor masuri tehnice şi organizatorice care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

5."Sistem de evidenta a datelor" înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice;

6."Operator" înseamnă persoana fizică sau juridică, autoritatea publica, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; dacă scopul şi mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ. În sensul prezentului regulament au calitatea de Operator, Centrul Național de Management al Apei Grele, cu toate entităţile funcţionale/structurile organizatorice – departamente, servicii, birouri, compartimente, comisii, comitete, etc., dacă stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal.

7."Persoana împuternicită de operator/procesator" înseamnă persoana fizică sau juridică, autoritatea publica, agenţia sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

8."Destinatar" înseamnă persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terţă. Cu toate acestea, autorităţile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autorităţile publice respective respectă normele aplicabile în materie de protecţie a datelor, în conformitate cu scopurile prelucrării;

9."Parte terţă" înseamnă o persoană fizică sau juridică, autoritate publică, agenţie sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

10."Consimţământ" al persoanei vizate înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta accepta, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

11."Încălcarea securităţii datelor cu caracter personal" înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

12."Date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezulta în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

13."Date biometrice" înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirma identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

14."Date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

15."Întreprindere" înseamnă o persoana fizică sau juridică ce desfăşoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociaţii care desfăşoară în mod regulat o activitate economică;

16."Grup de întreprinderi" înseamnă o întreprindere care exercită controlul şi întreprinderile controlate de aceasta;

17."Reguli corporatiste obligatorii" înseamnă politicile în materie de protecţie a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce priveşte transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoana împuternicită de operator în una sau mai multe ţări terţe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

18."Autoritate de supraveghere/ANSPDCP" înseamnă Autoritatea Naţională de Supraveghere a Datelor cu Caracter Personal;

19. „Codul numeric personal (C.N.P.)"înseamnă un număr semnificativ care individualizează în mod unic o persoana fizică, constituind un instrument de verificare a stării civile a acesteia şi de identificare în anumite sisteme informatice de către persoanele autorizate;

20. „Date cu caracter personal cu funcţie de identificare de aplicabilitate generală (date cu caracter special)"înseamnă numere prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care au aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul paşaportului, al permisului de conducere, numărul de asigurare sociala sau de sănătate;

21. „Utilizator" înseamnă orice persoană care acţionează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal; are calitatea de utilizator al datelor cu caracter personal, personalul Operatorului – Centrul Naţional de Management al Apei Grele sau al împuternicitului acestuia ale cărei atribuţii de serviciu presupun operaţiuni de prelucrare a datelor cu caracter personal.

22.„Responsabilul de protecţia datelor" înseamnă persoana din cadrul Centrului Naţional de Management al Apei Grele cu sarcini/responsabilităţi specifice privind funcţionarea corespunzătoare a sistemului de protecţie a datelor cu caracter personal, în conformitate cu prevederile GDPR precum şi elaborarea, implementarea şi monitorizarea respectării prevederilor prezentului Regulament.

CAP.2 PRINCIPII LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL

2.1.Legalitate, echitate şi transparenţă– un principiu esenţial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate „în mod legal, echitabil şi transparent faţă de persoana vizată.";

Principiul transparenţei prevede că orice informaţii şi comunicări referitoare la prelucrarea respectivelor date cu caracter personal trebuie să fie uşor accesibile şi uşor de înţeles şi ca trebuie să se utilizeze un limbaj simplu şi clar; acest principiu se referă în special la informarea persoanei vizate privind identitatea operatorului şi scopurile prelucrării, precum şi la oferirea de informaţii suplimentare, pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoanele fizice vizate şi dreptul acestora de a li se confirma şi comunica datele cu caracter personal care sunt prelucrate;

Persoanele fizice trebuie informate cu privire la riscurile, normele, garanţiile şi drepturile în materie de prelucrare a datelor cu caracter personal şi cu privire la modul în care să îşi exercite drepturile în legătură cu prelucrarea;

Scopurile specifice în care datele cu caracter personal sunt prelucrate trebuie să fie explicite şi legitime şi să fie determinate la momentul colectării datelor respective;

Datele cu caracter personal trebuie să fie adecvate, relevante şi limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesita, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum;

Datele cu caracter personal ar trebui prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace;

Operatorul trebuie să stabilească termene pentru ştergere sau revizuirea periodică.

Operatorul trebuie să ia toate masurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau şterse;

Datele personale trebuie prelucrate într-un mod care să asigure în mod adecvat securitatea şi confidenţialitatea, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal şi a echipamentului utilizat pentru prelucrare.

2.2.Limitări legate de scop– datele personale trebuie să fie colectate în scopuri bine determinate, explicite şi legitime, iar prelucrările ulterioare nu trebuie să se abată de la aceste scopuri. Prelucrarea ulterioara în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică/ istorică ori în scopuri statistice nu se consideră incompatibilă de la scopurile iniţiale;

2.3.Minimizarea/Reducerea la minimum a datelor– orice colectare de date personale trebuie foarte bine analizată înainte de obţinerea efectivă a datelor, care trebuie să fie cele mai adecvate, relevante și strict limitate la ceea ce este absolut necesar pentru scopurile în care sunt prelucrate;

2.4.Exactitatea informaţiilor– datele cu caracter personal trebuie să fie exacte, şi, în cazul în care este necesar, trebuie sa fie actualizate; operatorii trebuie să ia toate măsurile pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere;

2.5.Limitarea stocării – datele trebuie păstrate fix atât timp cat sunt necesare pentru prelucrarea asumată. Perioadele mai lungi de stocare sunt excepţii asociate cu activităţi de prelucrare în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, sub rezerva punerii în aplicare a măsurilor tehnice şi organizatorice adecvate prevăzute de GDPR în vederea garantării drepturilor şi libertăţilor persoanei vizate;

2.6.Integritate şi confidenţialitate – prelucrarea datelor personale trebuie făcută în cele mai adecvate condiţii de siguranţă, care să includă „protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare”.

Nerespectarea acestui principiu expune direct la breşe de securitate şi confidenţialitate şi, implicit, la penalităţile extrem de severe prevăzute de GDPR;

2.7.Responsabilitate – Operatorul este responsabil de respectarea principiilor GDPR şi de a demonstra această respectare. GDPR impune nu numai respectarea principiilor GDPR – de exemplu, prin documentarea deciziilor luate cu privire la o activitate de procesare, ci şi să se demonstreze oricând aceasta respectare (responsabilitate).

În consecinţă, orice prelucrare de date cu caracter personal trebuie să fie legală şi echitabilă;

CAP. 3 LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Prelucrarea este legală numai dacă şi în măsura în care se aplică cel puţin una dintre următoarele condiţii:

- persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului;
- prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este investit operatorul;
- prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizata este un copil.

CAP. 4 CONSIMŢĂMÂNTUL PERSOANEI VIZATE ŞI CONDIŢIILE PRIVIND CONSIMŢĂMÂNTUL

4.1.În cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul expres, neechivoc, liber şi informat pentru prelucrarea datelor sale cu caracter personal.

4.2.În cazul în care consimţământul persoanei vizate este dat în contextul unei declaraţii scrise care se refera şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentata într-o forma care o diferenţiază în mod clar de celelalte aspecte, într-o forma inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu.

4.3.Persoana vizata are dreptul să îşi retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, persoana vizata este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia.

4.4.Atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cat mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionata sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

4.5.La nivelul Centrul Național de Management al Apei Grele, ca Operator de date cu caracter personal, consimţământul persoanelor vizate este acordat:

- în cadrul procesului de recrutare/selecţie de personal;
- în cadrul procedurilor de achiziții;
- în situaţia încheierii unor contracte cu terții, exclusiv în situaţia în care prelucrarea datelor personale se face în scop de marketing direct (furnizarea de informaţii despre serviciile, evenimentele şi manifestările CNMAG;

4.6.În cadrul procesului de recrutare/selecţie de personal, Specialistul de Resurse Umane din cadrul Centrul Național de Management al Apei Grele va solicita acordarea consimţământului de către potenţialul angajat prin semnarea de către acesta a unei Declarații de consimțământ prin care își declară acordul cu privire la utilizarea şi prelucrarea datelor cu caracter personal și faptul că a fost informat în legătură cu prelucrarea datelor cu caracter personal la nivelul institutiei, precum şi în legătură cu drepturile de care beneficiază, potrivit legislaţiei specifice. Declarațiile de consimțământ se vor păstra în evidentele Specialistului de Resurse Umane.

4.7.Daca prelucrarea datelor personale se bazează pe consimţământ, prelucrarea datelor unui copil este legală daca acesta are cel puţin vârsta de 16 ani. Daca copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă şi în măsura în care consimţământul respectiv este acordat sau autorizat de titularul răspunderii părinteşti asupra copilului. Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri dacă titularul răspunderii părinteşti a acordat sau a autorizat consimţământul, ţinând seama de tehnologiile disponibile. Aceste dispoziţii nu afectează dreptul general al contractelor aplicabil în statele membre UE, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

CAP. 5 REGULI SPECIALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

5.1.Prelucrarea unor categorii speciale de date cu caracter personal

5.1.1.Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viata sexuală sau orientarea sexuală ale unei persoane fizice.

5.1.2.Prevederile anterioare nu se aplica în următoarele situaţii:

- când persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepţia cazului în care dreptul Uniunii sau dreptul intern prevede că interdicţia prevăzută anterior să nu poată fi ridicată prin consimţământul persoanei vizate;
- când prelucrarea este necesara în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă

şi al securităţii sociale şi protecţiei sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanţii adecvate pentru drepturile fundamentale şi interesele persoanei vizate;

- când prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizata se afla in incapacitate fizica sau juridica de a-şi da consimţământul;
- când prelucrarea este efectuată în cadrul activităţilor lor legitime şi cu garanţii adecvate de către o fundaţie, o asociaţie sau orice alt organism fără scop lucrativ şi cu specific politic, filozofic, religios sau sindical, cu condiţia ca prelucrarea să se refere numai la membrii sau la foştii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale şi că datele cu caracter personal sa nu fie comunicate terţilor fără consimţământul persoanelor vizate;
- când prelucrarea se refera la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare;
- când prelucrarea este necesara din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate;
- când prelucrarea este necesară în scopuri legate de medicina preventiva sau a muncii, de evaluarea capacitaţii de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării condiţiilor şi garanţiilor prevăzute de lege; datele cu caracter personal pot fi prelucrate în scopurile menţionate anterior în cazul în care datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.
- când prelucrarea este necesară din motive de interes public în domeniul sănătăţii publice, cum ar fi protecţia împotriva ameninţărilor transfrontaliere grave la adresa sănătăţii sau asigurarea de standarde ridicate de calitate şi siguranţă a asistenţei medicale şi a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, în special a secretului profesional; sau
- când prelucrarea este necesara în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor

şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate.

5.2.Prelucrarea datelor cu caracter personal cu funcţie de identificare generală

5.2.1.Datele cu caracter personal cu funcţie de identificare generală (Codul numeric personal - CNP, seria şi numărul actului de identitate/paşaportului etc.) vor fi prelucrate, exclusiv în situaţiile în care este necesară stabilirea identităţii persoanelor vizate şi prelucrarea este prevăzută în mod expres de o dispoziţie legală.

5.2.2.Prin legislaţia naţională se pot detalia condiţiile specifice de prelucrare a unui număr de identificare naţional sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare naţional sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanţii corespunzătoare pentru drepturile şi libertăţile persoanei vizate.

5.3.Prelucrarea datelor cu caracter personal referitoare la condamnări penale şi infracţiuni

Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni sau la masuri de securitate conexe se efectuează numai sub controlul unei autorităţi de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de legislaţia naţională care prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se tine numai sub controlul unei autorităţi de stat.

5.4.Prelucrarea care nu necesită identificarea

5.4.1.În cazul în care scopurile pentru care Centrul Național de Management al Apei Grele (operatorul) prelucrează date cu caracter personal nu mai necesită sau nu necesită identificarea unei persoane vizate de către operator, operatorul nu are obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica persoana vizata în scopul unic al respectării legislaţiei specifice.

5.4.2.Daca, în cazurile menţionate anterior, operatorul poate demonstra ca nu este în măsura să identifice persoana vizata, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, prevederile legale privind dreptul de acces, de rectificare, de ştergere, la restricţionarea prelucrării, dreptul la portabilitatea datelor nu se aplica, cu excepţia cazului în care persoana vizată, în scopul exercitării drepturilor sale menţionate anterior, oferă informaţii suplimentare care permit identificarea sa.

5.5. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video

5.5.1. Utilizarea sistemului video este necesară pentru buna administrare şi funcţionare a Centrului Național de Management al Apei Grele, în special în vederea controlului de securitate şi pază. De asemenea, sistemul video este necesar pentru a sprijini politicile de securitate mai cuprinzătoare instituite de actele normative care reglementează protecţia informaţiilor clasificate şi contribuie la îndeplinirea atribuţiilor structurii de securitate, astfel cum este prevăzut în HG nr. 585 din 13 iunie 2002 pentru aprobarea Standardelor naţionale de protecţie a informaţiilor clasificate în România.

5.5.2. Auditare internă: Sistemul video existent a fost instalat în urma unor analize de risc, anexate planurilor de protecţie şi pază.

5.5.3. Revizuiri periodice: O revizuire periodică va fi întreprinsă, conform HG nr.301/2012 de către structurile responsabile cu asigurarea securităţii şi va reanaliza:

- necesitatea menţinerii în uz a sistemului

- îndeplinirea scopului declarat
- posibile alternative adecvate la sistem
- prezenta politică respectă legislatia in vigoare.

5.5.4. Zonele supravegheate: Sistemul de supraveghere prin mijloace video, cuprinde sediul Centrul Național de Management al Apei Grele. Amplasarea camerelor a fost atent analizată pentru a asigura limitarea pe cât posibil a monitorizării zonelor care nu prezintă interes pentru scopul urmărit. Dispozitivele de înregistrare sunt amplasate în spaţii bine protejate, neexistând posibilitatea sustragerii suportului de stocare sau a dispozitivului, în special în timpul producerii unui eveniment. Nu sunt monitorizate zonele în care există un nivel ridicat al aşteptărilor privind viaţa privată, precum birourile, toaletele şi alte locaţii similare. În mod excepţional, în cazul unor necesităţi în materie de securitate justificate în mod corespunzător, se pot instala camere în astfel de locuri, însă numai după efectuarea unei evaluări de impact şi după informarea responsabilului cu protecţia datelor personale. În astfel de cazuri, trebuie amplasat un anunţ specific şi vizibil în locurile respective.

5.5.5. Datele cu caracter personal colectate prin intermediul supravegherii video

5.5.5.1.Scopul supravegherii prin mijloace video: Centrul Național de Management al Apei Grele utilizează sistemul de supraveghere video doar în scop de securitate şi control acces. Cu ajutorul acestui sistem se controlează accesul în incinta unităţii, se asigură securitatea bunurilor şi siguranţa persoanelor - angajaţi ai instituţiei sau vizitatori, precum şi a proprietăţilor şi informaţiilor deţinute. Sistemul de supraveghere video completează celelalte măsuri fizice de securitate, cum ar fi sistemul de control acces, făcând parte din măsurile întreprinse pe baza politicii de securitate, elaborată la nivelul instituţiei, şi ajută la prevenirea, combaterea şi, dacă e cazul, cercetarea accesului fizic neautorizat, inclusiv a accesului neautorizat la spaţiile securizate şi la încăperile protejate, accesul neautorizat la infrastructura informatică sau la informaţiile operaţionale. În plus, sistemul de supraveghere video ajută la prevenirea, detectarea şi investigarea furturilor de echipament sau de bunuri deţinute de instituţie sau la prevenirea, detectarea şi investigarea riscurilor şi ameninţărilor la adresa personalului angajat care îşi desfăşoară activitatea la locaţia supravegheată.

5.5.5.2. Limitarea scopului: Sistemul de supraveghere video nu este utilizat în alt scop decât cel notificat, nu foloseşte la monitorizarea activităţii angajaţilor sau la pontaj. De asemenea, sistemul nu este mijloc de investigare sau de obţinere a unor informaţii pentru anchetele interne sau procedurile disciplinare, cu excepţia situaţiilor în care se produce un incident de securitate fizică sau se observă un comportament infracţional (în circumstanţe excepţionale imaginile pot fi transferate organelor de cercetare în cadrul unei investigaţii disciplinare sau penale).

5.5.5.3. Categorii speciale de date: Sistemul video al Centrului Național de Management al Apei Grele nu are ca scop captarea (de exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (de exemplu, indexare, creare de profiluri) care dezvăluie „categorii speciale de date”, iar instituţia nu intenţionează să utilizeze sistemul de supraveghere şi în mod ad-hoc, respectiv cu caracter temporar, de circumstanţă.

5.5.5.4. Descrierea şi specificaţiile tehnice ale sistemului: În mod convenţional sistemul de supraveghere video este un sistem static. Are ca funcţie înregistrarea imaginilor şi este echipat cu senzori de mişcare. Sistemul poate înregistra orice mişcare detectată de camerele instalate în zona supravegheată, alături de dată, oră şi locaţie. Toate camerele sunt funcţionale 24 de ore, 7 zile pe săptămână. Atunci când este necesar, calitatea imaginilor permite recunoaşterea celor care trec prin zona de acţiune a camerelor. Pentru o mai mare siguranţă a prelucrării datelor care pot fi obţinute în urma supravegherii video, camerele sunt, astfel utilizatorul nu poate modifica perimetrul/scopul supravegherii.). Operatorii special instruiţi trebuie să respecte setările de confidenţialitate şi drepturile de acces. Nu există interconexiune cu alte sisteme şi nu se înregistrează sunetul.

5.5.5.5.Accesul este strict limitat la angajaţii autorizaţi în camerele de control unde se află sistemul de supraveghere video.

5.5.6. Accesul la datele personale si dezvaluirea acestora

Drepturi de acces: Accesul la imaginile stocate şi/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane ce au cu conturi limitate. În special, instituţia noastră impune limite în privinţa persoanelor care au dreptul:

- să vizioneze materialul filmat în timp real - imaginile care se derulează în timp real sunt accesibile angajatilor desemnaţi;
- să vizioneze înregistrarea materialului filmat - vizionarea prin derulare a imaginilor înregistrate se va face în cazuri justificate, cum ar fi cazurile prevăzute expres de lege şi incidentele de securitate, de către persoanele special desemnate.

5.5.7. Dezvăluirea datelor cu caracter personal: Centrul Național de Management al Apei Grele are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvârşirea unor fapte de încălcare a legii. Sistemul de supraveghere video nu este utilizat pentru verificarea prezenţei la program sau evaluarea performanţei la locul de muncă. În cazuri excepţionale, dar cu respectarea garanţiilor descrise anterior, se poate acorda acces Comisiei Disciplinare, în cadrul unei anchete disciplinare, cu condiţia ca informaţiile să ajute la investigarea unei infracţiuni sau a unei abateri disciplinare de natură să prejudicieze drepturile şi libertăţile unei persoane. Orice încălcare a securităţii în ceea ce priveşte camerele video este indicată în registrul de investigaţii, iar responsabilul cu protecţia datelor personale este informat în legătură cu acest lucru cât mai repede posibil.

5.5.8. Durata de stocare: Durata de stocare a datelor obţinute prin intermediul sistemului de supraveghere video este proporţională cu scopul pentru care se prelucrează datele, astfel că imaginile sunt stocate pentru o perioadă de aproximativ 20 de zile în funcţie de capacitatea de stocare, după care se şterg prin procedură automată în ordinea în care au fost înregistrate. În cazul producerii unui incident de securitate, durata de păstrare a materialului filmat relevant poate depăşi limitele normale în funcţie de timpul necesar investigării suplimentare a incidentului de securitate. Păstrarea este documentată riguros, iar necesitatea păstrării este revizuită periodic.

5.5.9. Drepturile persoanei vizate: Centrul Național de Management al Apei Grele garantează că asigură respectarea drepturilor ce revin persoanelor vizate, conform legii. Toate persoanele implicate în activitatea de supraveghere video şi cele responsabile de administrarea imaginilor filmate, vor respecta politica de securitate în vigoare.

5.5.10. Informarea persoanelor vizate: Informarea primară a persoanelor vizate se realizează în mod clar şi permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă şi localizat în zona supravegheată, astfel încât să semnaleze existenţa camerelor de supraveghere, dar şi pentru a comunica informaţiile esenţiale privind prelucrarea datelor personale – conform Anexei. Persoanele vizate sunt atenţionate asupra existenţei sistemului de supraveghere video şi a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării şi identifică Centrul Național de Management al Apei Grele ca operator al datelor colectate prin intermediul supravegherii video.

5.5.11. Exercitarea drepturilor de acces, intervenţie şi opoziţie: Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care le privesc deţinute de Centrul Național de Management al Apei Grele, de a solicita intervenţia (ştergere/actualizare/rectificare/anonimizare) sau de a se opune prelucrărilor, conform legii. Orice cerere de a accesa, rectifica, bloca şi/sau şterge date cu caracter personal ca urmare a utilizării camerelor video ar trebui să fie adresată Centrul Național de Management al Apei Grele - Responsabilul cu Protecţia Datelor Personale. În cazul în care persoana vizată are alte întrebări privind prelucrarea de către Centrul Național de Management al Apei Grele a datelor personale care o privesc, se poate adresa Responsabilului cu Protecţia Datelor Personale. Răspunsul la solicitarea de acces, intervenţie sau opoziţie se dă în termen de 15 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amânare a răspunsului, de asemenea i se va comunica şi procedura care va urma pentru soluţionarea cererii.

5.5.12.Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate care o privesc. Imaginile furnizate vor fi clare, în măsura posibilităţii, cu condiţia de a nu prejudicia drepturile terţilor (persoana vizată va putea vizualiza doar propria imagine, imaginile altor persoanelor care pot apărea în înregistrare vor fi editate astfel încât să nu fie posibilă recunoaşterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată este obligată să se identifice dincolo de orice suspiciune (să prezinte actul de identitate când participă la vizionare), să menţioneze data, ora, locaţia şi împrejurările în care a fost înregistrată de camerele de supraveghere. De asemenea, persoana vizată va prezenta şi o fotografie recentă astfel încât utilizatorii desemnaţi să o poată identifica mai uşor în imaginile filmate.

5.5.13.Există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune şi în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor terţe persoane, de exemplu dacă în imagini apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

CAP.6 DREPTURILE PERSOANEI VIZATE ÎN CONTEXTUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

6.1. Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate: Centrul Național de Management al Apei Grele – in calitate de operator date cu caracter personal, ia măsuri adecvate pentru a furniza persoanei vizate informaţiile legale solicitate, precum şi orice notificări şi comunicări referitoare la prelucrare, într-o forma concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informaţiile pot fi furnizate verbal, cu condiţia ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

6.1.1.În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

- fie să perceapă o taxa rezonabilă ţinând cont de costurile administrative pentru furnizarea informaţiilor sau a comunicării sau pentru luarea măsurilor solicitate;

- fie să refuze să dea curs cererii. În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

6.2. Dreptul la informare

6.2.1. Informaţii care se furnizează în cazul în care datele cu caracter personal sunt colectate direct de la persoana vizată.

6.2.1.1. În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, Centrul Național de Management al Apei Grele, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate următoarele informaţii:

- identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;

- datele de contact ale responsabilului cu protecţia datelor, după caz;

scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

- interesele legitime urmărite de operator sau de o parte terţă, după caz;

- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

6.2.1.2. În plus, faţă de informaţiile menţionate anterior, în momentul în care datele cu caracter personal sunt obţinute, operatorul furnizează persoanei vizate următoarele informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă:

- perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

- existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;

- atunci când prelucrarea se bazează pe consimţământul persoanei vizate, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;

- dreptul de a depune o plângere în fata unei autorităţi de supraveghere;

- dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;

- existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.2.1.3. În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de aceasta prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante;

6.2.1.4. Prevederile precedente nu se aplică dacă şi în măsura în care persoana vizată deţine deja informaţiile respective.

6.2.2. Informaţii care se furnizează în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată

6.2.2.1 În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, Centrul Național de Management al Apei Grele furnizează persoanei vizate următoarele informaţii:

- identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
- datele de contact ale responsabilului cu protecţia datelor, după caz;

scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;

- categoriile de date cu caracter personal vizate;

6.2.2.2. Pe lângă informaţiile menţionate anterior, operatorul furnizează persoanei vizate următoarele informaţii necesare pentru a asigura o prelucrare echitabilă şi transparentă în ceea ce priveşte persoana vizată:

- perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- interesele legitime urmărite de operator sau de o parte terţă, după caz;
- existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării şi a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;
- atunci când prelucrarea se bazează pe consimţământul persoanei vizate, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
- dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
- sursa din care provin datele cu caracter personal şi, dacă este cazul, dacă acestea provin din surse disponibile public;
- existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.2.2.3. Operatorul furnizează informaţiile menţionate anterior:

- într-un termen rezonabil după obţinerea datelor cu caracter personal, dar nu mai mare de o lună, ţinându-se seama de circumstanţele specifice în care sunt prelucrate datele cu caracter personal;
- dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă; sau

dacă se intenţionează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

6.2.2.4. În cazul în care operatorul intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obţinute, operatorul furnizează persoanei vizate, înainte de aceasta prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante.

6.2.2.5 Prevederile precedente nu se aplică dacă şi în măsura în care:

- persoana vizată deţine deja informaţiile;

- furnizarea acestor informaţii se dovedeşte a fi imposibilă sau ar implica eforturi disproporţionate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, sub rezerva condiţiilor şi a garanţiilor prevăzute de lege, sau în măsura în care obligaţia furnizării informaţiilor este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia masuri adecvate pentru a proteja drepturile, libertăţile şi interesele legitime ale persoanei vizate, inclusiv punerea informaţiilor la dispoziţia publicului;

- obţinerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii Europene sau de dreptul intern sub incidenţa căruia intra operatorul şi care prevede masuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

- în cazul în care datele cu caracter personal trebuie să rămână confidenţiale în temeiul unei obligaţii statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligaţii legale de a păstra secretul.

6.2.3. Informarea persoanelor vizate în contextul activităţilor specifice Centrului Național de Management al Apei Grele: În contextul realizării atribuţiilor stabilite de lege şi desfăşurării activităţii curente a Centrului Național de Management al Apei Grele, inclusiv derulării raporturilor de muncă, activităţii contractuale şi /sau participării la evenimente specializate organizate în incinta Centrului Național de Management al Apei Grele, precum şi în contextul îndeplinirii obligaţiilor legale, informarea persoanelor vizate se poate realiza, după cum urmează :

(1) În cadrul procesului de recrutare/selecţie de personal, Specialistul de Resurse Umane va pune la dispoziţia potenţialului angajat o Notă de Informare și o Declarație de consimțământ candidat, pe care acesta / aceasta le va citi şi semna. Prin aceste documente, candidatul este informat/a și își exprimă acordul în legătură cu prelucrarea datelor cu caracter personal la nivelul Centrului Național de Management al Apei Grele precum şi în legătură cu drepturile de care beneficiază, potrivit legislaţiei specifice. Nota de Informare și Declarația de consimțământ candidat se vor păstra distinct în evidenţele Specialistului de Resurse Umane. Modelul Notei de Informare și a Declarației de consimțământ candidat este prevăzut în **Anexa nr.1 și Anexa nr.2; la prezentul Regulament;**

(2) În contextul derulării raporturilor de muncă, Specialistul de Resurse Umane va pune la dispoziţia fiecărui angajat din cadrul Centrului Național de Management al Apei Grele o Notă de Informare și o Declarație de consimțământ angajat, pe care acesta / aceasta le va citi şi semna. Prin aceste documente, angajatul este informat/a și își exprimă acordul în legătură cu prelucrarea datelor cu caracter personal la nivelul Centrului Național de Management al Apei Grele precum şi în legătură cu drepturile de care beneficiază, potrivit legislaţiei specifice. Nota de Informare și Declarația de consimțământ angajat se vor păstra distinct în evidenţele Specialistului de Resurse Umane. Modelul Notei de Informare și a Declarației de consimțământ angajat este prevăzut în **Anexa nr.3 și Anexa nr.4, la prezentul Regulament;**

(3) Persoanele vizate, respectiv angajaţii, clienţii/potenţialii clienţi, vizitatorii şi alte persoane care intră în sediul Centrului Național de Management al Apei Grele, ale căror date sunt prelucrate prin intermediul sistemelor de supraveghere video sunt informate în acest sens prin intermediul unor Note de Informare. Modelul Notei de Informare cu privire la prelucrarea datelor prin sistemele de supraveghere video este prevăzut în **Anexa nr.6, la prezentul Regulament.**

Informările în cauza, precum şi indicatoarele de marcare a existentei sistemului de supraveghere video vor fi aplicate în locurile unde sunt amplasate camere de supraveghere video.

6.3. Dreptul de acces al persoanei vizate: Persoana vizată are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc şi, în caz afirmativ, acces la datele respective şi la următoarele informaţii:

- scopurile prelucrării;

- categoriile de date cu caracter personal vizate;

destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţari terţe sau organizaţii internaţionale;

- acolo unde este posibil, perioada pentru care se preconizează ca vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioadă;

- existenţa dreptului de a solicita operatorului rectificarea sau ştergerea datelor cu caracter personal ori restricţionarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

- dreptul de a depune o plângere în fata unei autorităţi de supraveghere;

- în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;

- existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizata şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.3.1.În cazul în care datele cu caracter personal sunt transferate către o ţară terţă sau o organizaţie internaţională, persoana vizată are dreptul să fie informată cu privire la garanţiile adecvate, prevăzute de lege referitoare la transfer. Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării.

6.3.2.Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxa rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic şi cu excepţia cazului în care persoana vizată solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent.

6.3.3.Dreptul de a obţine o copie menţionată anterior nu aduce atingere drepturilor şi libertăţilor altora.

6.4. Dreptul la rectificare: Persoana vizata are dreptul de a obţine de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ţinându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obţine completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declaraţii suplimentare.

6.5. Dreptul la ştergerea datelor ("dreptul de a fi uitat"): Persoana vizată are dreptul de a obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplica unul dintre următoarele motive:

- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- persoana vizata îşi retrage consimţământul pe baza căruia are loc prelucrarea, şi nu exista niciun alt temei juridic pentru prelucrarea;
- persoana vizată se opune prelucrării şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării, în cazul prelucrării în scop de marketing direct;
- datele cu caracter personal au fost prelucrate ilegal;
- datele cu caracter personal trebuie şterse pentru respectarea unei obligaţii legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidenţa căruia se afla operatorul;

Alineatele anterioare nu se aplică în măsura în care prelucrarea este necesară:
pentru exercitarea dreptului la liberă exprimare şi la informare;

- pentru respectarea unei obligaţii legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este investit operatorul;
- din motive de interes public în domeniul sănătăţii publice;
- în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorica ori în scopuri statistice, în măsura în care dreptul la ştergere este susceptibil să facă imposibilă sau sa afecteze în mod grav realizarea obiectivelor prelucrării respective; sau
- pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

6.6.Dreptul la restricţionarea prelucrării: Persoana vizată are dreptul de a obţine din partea operatorului restricţionarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

- persoana vizată contestă exactitatea datelor, pentru o perioada care îi permite operatorului să verifice exactitatea datelor;
- prelucrarea este ilegala, iar persoana vizată se opune ştergerii datelor cu caracter personal, solicitând în schimb restricţionarea utilizării lor;
- operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanţă; sau
- persoana vizată s-a opus prelucrării, pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

În cazul în care prelucrarea a fost restricţionată conform prevederilor anterioare, astfel de date cu caracter personal pot, cu excepţia stocării, să fie prelucrate numai cu consimţământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau pentru protecţia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru. O persoană vizată care a obţinut restricţionarea prelucrării este informată de către operator înainte de ridicarea restricţiei de prelucrare.

6.7. Obligaţia de notificare cu privire la rectificarea, ştergerea datelor cu caracter personal sau restricţionarea prelucrării: Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ştergere a datelor cu caracter personal sau restricţionare a prelucrării, cu excepţia cazului în care acest lucru se dovedeşte imposibil sau presupune eforturi disproporţionate. De asemenea, operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

6.8. Dreptul la portabilitatea datelor: Persoana vizata are dreptul de a primi datele cu caracter personal care o privesc şi pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

- prelucrarea se bazează pe consimţământ sau pe un contract; şi
- prelucrarea este efectuată prin mijloace automate.

În exercitarea dreptului său la portabilitatea datelor, persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic. Exercitarea dreptului la portabilitatea datelor nu aduce atingere dreptului la ştergerea datelor. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este investit operatorul.

Dreptul la portabilitatea datelor nu aduce atingere drepturilor şi libertăţilor altora.

6.9. Dreptul la opoziţie şi procesul decizional individual automatizat

6.9.1. Dreptul la opoziţie

6.9.1.1. În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situaţia particulară în care se afla, prelucrării datelor cu caracter personal care o privesc, inclusiv creării de profiluri. Operatorul nu mai prelucrează datele cu caracter personal, cu excepţia cazului în care operatorul demonstrează ca are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra intereselor, drepturilor şi libertăţilor persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţă.

6.9.1.2. Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

6.9.1.3 În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

6.9.1.4.Cel târziu în momentul primei comunicări cu persoana vizată, dreptul la opoziţie menţionat este adus în mod explicit în atenţia persoanei vizate şi este prezentat în mod clar şi separat de orice alte informaţii.

6.9.1.5. În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice, persoana vizată, din motive legate de situaţia sa particulară, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepţia cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

6.9.2. Procesul decizional automatizat, crearea de profiluri

6.9.2.1. Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

6.9.2.2. Prevederile anterioare nu se aplică în cazul în care decizia:
este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date;

- este autorizată prin dreptul Uniunii sau dreptul intern care se aplica operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate; sau
- are la baza consimţământul explicit al persoanei vizate.

6.9.2.3. În cazurile în care decizia este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date sau are la bază consimţământul explicit al persoanei vizate, operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate, cel puţin dreptul acesteia de a obţine intervenţie umană din partea operatorului, de a-şi exprima punctul de vedere şi de a contesta decizia.

6.9.2.4. Deciziile menţionate anterior nu au la baza categoriile speciale de date cu caracter personal, cu excepţiile prevăzute de lege (ex: persoana vizată şi-a dat consimţământul explicit) şi în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

CAP. 7 RESTRICȚII

7.1.Prin legislaţia specifică care se aplică operatorului de date sau persoanei împuternicite de operator se poate restricţiona domeniul de aplicare al obligaţiilor şi al drepturilor prevăzute în actuala legislaţie în măsura în care dispoziţiile acesteia corespund drepturilor şi obligaţiilor menţionate anterior, atunci când o astfel de restricţie respectă esenţa drepturilor şi libertăţilor fundamentale şi constituie o măsură necesară şi proporţională într-o societate democratică, pentru a asigura:

- securitatea naţională;
- apărarea;
- securitatea publică;
- prevenirea, investigarea, depistarea sau urmărirea penală sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa securităţii publice şi prevenirea acestora;
- alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;
- protejarea independenţei judiciare şi a procedurilor judiciare;
- prevenirea, investigarea, depistarea şi urmărirea penală a încălcării eticii în cazul profesiilor reglementate;

- funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii oficiale;

- protecţia persoanei vizate sau a drepturilor şi libertăţilor altora;

punerea în aplicare a pretenţiilor de drept civil.

CAP. 8 OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

8.1. Responsabilitatea Operatorului: In vederea asigurării unui nivel adecvat de protecţie/securitate a datelor cu caracter personal, la nivelul Centrului Național de Management al Apei Grele se adoptă/stabilesc măsuri organizatorice şi reguli, precum:

- Instalarea de sisteme de supraveghere video şi sisteme antiefracţie;
- Monitorizarea şi intervenţia în caz de alarmă asigurată în permanenţă de personal specializat/autorizat;
- Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transport, distrugere şi arhivare stabilite prin Legea Arhivelor Naţionale, legislaţia internă şi internaţională privind protecţia datelor cu caracter personal, şi prin proceduri interne;

(1) Personalul Centrului Național de Management al Apei Grele este instruit în legătură cu aspectele legale privind protecţia datelor personale şi cu privire la riscurile pe care le comportă prelucrarea datelor personale. Astfel, conducerea unitatii, prin specialistul IT, stabileşte fiecărui utilizator tipurile de acces şi operaţiunile permise acestuia, strict necesare pentru îndeplinirea atribuţiilor de serviciu. Utilizatorul/angajatul Centrului Național de Management al Apei Grele poate prelucra date cu caracter personal doar pe perioada în care ocupa funcţia respectivă. Extinderea sau restrângerea atribuţiilor de prelucrare a datelor cu caracter personal se dispune de unitate atunci când utilizatorul/angajatul se afla în una dintre următoarele situaţii:

- la modificarea raporturilor de muncă;
- la modificarea atribuţiilor privind prelucrarea datelor cu caracter personal, prevăzute în fişa postului.

(2) Dreptul de acces al utilizatorului la sistemul de evidenţă a datelor cu caracter personal se suspendă pe perioada în care acesta se afla în una dintre următoarele situaţii:

- se află în concediu fără plată, concediu medical, concediu pentru creşterea sau îngrijirea copilului minor, pentru o perioada mai mare de 3 luni;
- se afla în concediu de maternitate sau concediu pentru incapacitate temporară de muncă;
- urmează un curs sau o specializare cu scoatere din program, pentru o perioada mai mare de 3 luni;
- pe perioada cercetării disciplinare, în situaţia în care faţă de utilizator se efectuează cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispoziţiilor legale;

alte cazuri prevăzute de lege.

(3) Cu ocazia proiectării, întreţinerii, actualizării aplicaţiilor de gestiune a bazelor de date, se interzice accesul providerilor/programatorilor/personalului de întreţinere a sistemelor informatice la orice fel de date cu caracter personal deţinute/create/accesate de personalul din

structura respectiva a institutiei. În aceste situaţii, se pun la dispoziţia providerilor / programatorilor/personalului de întreţinere numai date anonime/pseudonimizate;

(4) Pentru cazuri excepţionale, numai pe durata intervenţiei şi circumstanţiat limitativ la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezenţa unui utilizator desemnat de operator, în această situaţie, răspunderea pentru păstrarea confidenţialităţii datelor aparţine persoanelor în cauză, sens în care trebuie să semneze un Angajament de confidenţialitate;

(5) Operaţiunile de colectare, introducere, modificare şi actualizare a datelor cu caracter personal se realizează numai de personalul anume desemnat de către conducătorii operatorului, conform actelor de reglementare internă;

(6) Centrului Național de Management al Apei Grele dispune masurile tehnice necesare care să permită identificarea utilizatorului care a introdus, modificat sau actualizat datele cu caracter personal;

(7) Bazele de date cu caracter personal deţinute/create şi programele folosite de operatori/utilizatori sunt salvate, prin copii de siguranţă, la un interval de timp stabilit de conducerea unitatii, în funcţie de mărimea, volumul şi importanţa acestor baze de date;

(8) Centrului Național de Management al Apei Grele desemnează/stabileşte utilizatori care să aibă atribuţii de serviciu şi executarea copiilor de siguranţă ale bazelor de date deţinute/create şi ale programelor folosite. Accesul în încăperile în care se află documente ce conţin date cu caracter personal şi/sau terminale de acces/echipamente care prelucrează date cu caracter personal este limitat la utilizatorii stabiliţi de conducătorii operatorului şi numai pentru îndeplinirea atribuţiilor de serviciu (acces restricţionat/controlat);

(9) Documentele, terminalele de acces/echipamentele care conţin date cu caracter personal vor fi ţinute/păstrate în fişete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare şi/sau în încăperi/spaţii care se pot încuia. Documentele care conţin date cu caracter personal, folosite pentru realizarea anumitor operaţiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora. Terminalele de acces/echipamentele se securizează cu parolă;

(10) Aplicaţiile informatice care gestionează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acţionează asupra datelor afişate pe ecran pe o perioadă de timp stabilită, prin proceduri de lucru/diagrame flux, în funcţie de operaţiunile care trebuie executate.

(11) Terminalele de acces trebuie să aibă setate funcţia de închidere automată a ecranului şi funcţia „lock screen - screen saver" la o temporizare prestabilită, prin proceduri de lucru/diagrame flux, iar dacă acest lucru nu este posibil din punct de vedere tehnic, după trecerea intervalului de timp stabilit, datele afişate trebuie ascunse sau sesiunea de lucru va fi închisă. Terminalele de acces folosite în relaţia cu publicul se poziţionează astfel încât datele afişate să fie vizualizate numai de către utilizatori;

(12) Accesul utilizatorilor/angajaţilor Centrului Național de Management al Apei Grele la datele cu caracter personal care se regăsesc în Reţeaua Centrului Național de Management al Apei Grele – serverele şi staţiile de lucru, se face controlat/restricţionat pe bază de user şi parolă, setate exclusiv de specialistul IT, utilizatorii având drept de acces limitat, onform procedurilor interne (ex: read only, write, execute, modify, full control etc.);

(13) Nu este permisă scoaterea din organizaţie a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD etc.) care conţin date cu caracter personal, decât cu aprobarea prealabilă a conducerii unitatii;

(14) Se interzice utilizarea serviciului de e-mail în orice mod ce ar avea drept consecinţa transmiterea, distribuirea şi livrarea de mesaje nesolicitate de poştă electronică în volum mare sau de mesaje comerciale nesolicitate ("Spam"). Prin spam înţelegem trimiterea de mesaje (comerciale) nesolicitate în urma cărora se primesc plângeri din partea celor care le primesc, folosirea sau distribuirea de liste de e-mail-uri care aparţin unor persoane care nu şi-au exprimat consimţământul anterior.

(15) Utilizatorii/angajaţii nu vor deschide email-uri de tip SPAM/Malware şi/sau orice alte comunicaţii electronice care nu au legătură cu activitatea desfăşurată în calitate de angajat. Totodată, angajaţii unitatii nu au voie să găzduiască sau să permită găzduirea site-urilor sau informaţiilor a căror publicitate este făcuta prin emailuri SPAM. Nerespectarea politicii anti-spam constituie abatere disciplinară şi se sancţionează potrivit Regulamentului Intern.

(16) Utilizatorii/angajaţii unitatii care prelucrează date cu caracter personal sunt obligaţi să îşi închidă sesiunea de lucru, să blocheze ecranul terminalelor de acces atunci când părăsesc locul de muncă, iar la sfârşitul programului de lucru să închidă terminalele de acces;

(17) Listarea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizaţi, şi, acolo unde echipamentul de imprimare permite, aceasta operaţiune se va realiza controlat, pe bază de parolă.

8.2. Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit

(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare (mijloace manuale şi/sau automate - ex: sisteme de operare, servere, staţii de lucru, soluţii de securitate, de backup, de stocare, programe/soluţii software/aplicaţii IT achiziţionate sau dezvoltate in-house etc.), cât şi în cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate (ex: pseudonimizarea), care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor, precum reducerea la minimum a datelor, şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentului regulament şi a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligaţie se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare şi accesibilităţii lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenţia persoanei, de un număr nelimitat de persoane.

(3) Un mecanism de certificare aprobat menţionat de legislaţia specifică poate fi utilizat drept element care să demonstreze îndeplinirea cerinţelor prevăzute anterior.

8.3. Persoana împuternicită de Operator: În cazul în care prelucrarea urmează să fie realizată în numele operatorului, acesta contractează exclusiv persoane împuternicite care oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerinţele prevăzute în prezentul regulament şi să asigure protecţia drepturilor persoanei vizate.

(1) Persoana împuternicită de operator nu recrutează o alta persoana împuternicită fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizaţii generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecţii fătă de aceste modificări.

(2) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date cu caracter personal şi categoriile de persoane vizate şi obligaţiile şi drepturile operatorului.

(3) Respectivul contract sau act juridic prevede în special ca persoana împuternicită de operator:

- prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţara terţă sau o organizaţie internaţională, cu excepţia cazului în care aceasta obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

- se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutara adecvata de confidenţialitate;

adoptă toate masurile tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate a datelor personale corespunzător, în conformitate cu cerinţele legislaţiei specifice;

respecta condiţiile menţionate privind recrutarea unei alte persoane împuternicite de operator;

ţinând seama de natura prelucrării, oferă asistenţa operatorului prin masuri tehnice şi organizatorice adecvate, în măsură în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute de legislaţia specifică;

- ajută operatorul să asigure respectarea obligaţiilor privind securitatea prelucrării, notificarea Autorităţii/informarea persoanei vizate în cazul încălcării securităţii datelor, evaluarea impactului asupra protecţiei datelor, consultarea prealabilă, ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;

la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

(4) Persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucţiune încalcă prezentul regulament sau alte dispoziţii din dreptul intern sau din dreptul Uniunii referitoare la protecţia datelor.

(5) În cazul în care o persoana împuternicită de un operator recrutează o alta persoana împuternicită pentru efectuarea de activităţi de prelucrare specifice în numele operatorului, aceleaşi obligaţii privind protecţia datelor prevăzute în contractul sau în alt act juridic încheiat între operator şi persoana împuternicită de operator, astfel cum sunt prevăzute anterior, revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanţii suficiente pentru punerea în aplicare a unor masuri tehnice şi organizatorice adecvate.

(6) În cazul în care aceasta a doua persoana împuternicită nu îşi respecta obligaţiile privind protecţia datelor, persoana împuternicită iniţială rămâne pe deplin răspunzătoare faţă de operator în ceea ce priveşte îndeplinirea obligaţiilor persoanei împuternicite subsecvent.

(7) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, sau la un mecanism de certificare aprobat, menţionate de legislaţia specifică, poate fi utilizată ca element prin care să se demonstreze existenta garanţiilor suficiente menţionate anterior.

(8) Fără a aduce atingere unui contract individual încheiat între operator şi persoana împuternicită de operator, contractul sau celalalt act juridic încheiat între persoana împuternicită de operator ţi o alta persoană împuternicită, se poate baza, integral sau parţial, pe clauze contractuale standard prevăzute/adoptate de Comisia Europeană/ de o autoritate de supraveghere, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul legislaţiei specifice;

(9) Contractul sau celalalt act juridic menţionat anterior se formulează în scris, inclusiv în format electronic.

(10) În cazul în care o persoana împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor şi mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce priveşte prelucrarea respectivă.

(11) În situaţiile în care sunt prelucrate date cu caracter personal în numele Centrului Național de Management al Apei Grele, de către persoane împuternicite (procesatori de date - ex: instituţii de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariaţi, companii de curierat etc.) derulatorii de contract ai Centrului Național de Management al Apei Grele vor avea responsabilitatea/obligativitatea de încheia cu fiecare dintre aceste persoane împuternicite acorduri de prelucrare a datelor cu caracter personal, care vor avea în conţinut elementele prevăzute în prezentul Regulament şi legislaţia specifică, stabilite în prealabil de Responsabilul cu protecţia datelor şi aprobate de conducerea unitatii.

8.4.Desfăşurarea activităţii de prelucrare sub autoritatea Operatorului sau a Persoanei Împuternicite de Operator

(1) Persoana împuternicită de operator şi orice persoana care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

8.5. Evidentele activităţilor de prelucrare

8.5.1. Organizaţiile care au mai puţin de 250 de angajaţi nu au obligaţia de a ţine evidenţa prelucrării de date cu caracter personal, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, sau date cu caracter personal referitoare la condamnări penale şi infracţiuni, astfel cum sunt prevăzute în legislaţia specifică.

8.5.2. În situaţia în care, operatorul va intra sub incidenţa prevederilor anterior menţionate, acesta păstrează o evidenţă a activităţilor de prelucrare desfăşurate sub responsabilitatea lor. Respectiva evidenţă cuprinde următoarele informaţii:
numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;

- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţara terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi documentaţia care dovedeşte existenta unor garanţii adecvate;
- acolo unde este posibil, termenele-limita preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a masurilor tehnice şi organizatorice de securitate adecvate;

8.5.3. Fiecare operator şi, după caz, persoana împuternicită de operator păstrează o evidenţă a tuturor categoriilor de activităţi de prelucrare desfăşurate în numele operatorului, care cuprind:

- numele şi datele de contact ale persoanei sau persoanelor împuternicite de operator şi ale fiecărui operator în numele căruia acţionează aceasta persoana (aceste persoane), precum şi ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;
- categoriile de activităţi de prelucrare desfăşurate în numele fiecărui operator;
- dacă este cazul, transferurile de date cu caracter personal către o ţara terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, o descriere generală a masurilor tehnice şi organizatorice de securitate adecvate.

8.5.4. Evidenţele menţionate anterior se formulează în scris, inclusiv în format electronic.

8.5.5. Operatorul sau persoana împuternicită de acesta, precum şi, sau al persoanei împuternicite de operator pun evidentele la dispoziţia autorităţii de supraveghere, la cererea acesteia, cu notificarea prealabila a Operatorului;

8.6. Cooperarea cu Autoritatea de supraveghere: Centrului Naţional de Management al Apei Grele în calitate de Operator şi persoana împuternicită de operator şi, după caz, reprezentantul acestora, cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor.

8.7. Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- pseudonimizarea şi criptarea datelor cu caracter personal;
- capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continuă ale sistemelor şi serviciilor de prelucrare precum si capacitatea de a restabili disponibilitatea datelor cu caracter personal si accesul la acestea in timp util in cazul in care are loc un incident de natura fizica sau tehnica ;
- un proces pentru testarea, evaluarea şi aprecierea periodică a eficacităţii masurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

8.8. La evaluarea nivelului adecvat de securitate, se tine seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

8.9. Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat, menţionate în legislaţia specifică, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerinţelor prevăzute anterior.

8.10. Operatorul şi persoana împuternicită de acesta iau masuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care aceasta obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern.

CAP.9 EVALUAREA IMPACTULUI ASUPRA PROTECŢIEI DATELOR ŞI CONSULTAREA PREALABILĂ

9.1.Responsabilul cu protecția datelor cu caracter personal elaborează, la solicitarea operatorului, în colaborare cu angajaţii Centrului Național de Management al Apei Grele, evaluarea impactului asupra unui anumit tip de prelucrare de date cu caracter personal.

9.2. Evaluarea impactului asupra protecției datelor se impune mai ales în cazul:

- unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
- prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale şi infracţiuni menţionate în legislaţia specifica; sau

unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

9.3.Autoritatea de supraveghere întocmeşte şi publică o lista a tipurilor de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor.

9.4. Autoritatea de supraveghere poate, de asemenea, sa stabilească şi sa pună la dispoziţia publicului o lista a tipurilor de operaţiuni de prelucrare pentru care nu este necesara o evaluare a impactului asupra protecţiei datelor.

9.5. Evaluarea conţine cel puţin:

- o descriere sistematica a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

- o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;

- o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate; şi masurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal şi să demonstreze conformitatea cu dispoziţiile prezentului regulament, luând în considerare drepturile şi interesele legitime ale persoanelor vizate şi ale altor persoane interesate.

9.6. La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menţionate în legislaţia specifică, în special în vederea unei evaluări a impactului asupra protecţiei datelor.

9.7. Operatorul, prin Responsabilul de protecţia datelor, solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanţilor acestora privind prelucrarea prevăzută, fără a aduce atingere protecţiei intereselor comerciale sau publice ori securităţii operaţiunilor de prelucrare.

9.8. Atunci când prelucrarea are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidenţa căruia intră operatorul, iar dreptul respectiv reglementează operaţiunea de prelucrare specifică sau setul de operaţiuni specifice în cauză şi deja s-a efectuat o evaluare a impactului asupra protecţiei datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, prevederile anterioare nu se aplică, cu excepţia cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităţilor de prelucrare.

9.9. Acolo unde este necesar, operatorul, prin Responsabilul de protecţia datelor, efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecţiei datelor, cel puţin atunci când are loc o modificare a riscului reprezentat de operaţiunile de prelucrare.

9.10. Consultarea prealabila a Autorităţii de Supraveghere:

(1) Operatorul, prin Responsabilul de protecţia datelor, consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecţiei datelor indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor masuri luate de operator pentru atenuarea riscului.Atunci când consultă autoritatea de supraveghere, operatorul, prin Responsabilul de protecţia datelor, îi furnizează acesteia:

- dacă este cazul, responsabilităţile respective ale operatorului, ale operatorilor asociaţi şi ale persoanelor împuternicite de operator implicate în activităţile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

- scopurile şi mijloacele prelucrării preconizate;

- masurile şi garanţiile prevăzute pentru protecţia drepturilor şi libertăţilor persoanelor vizate, în conformitate cu prezentul regulament;

- datele de contact ale specialistului de date personale ;

- evaluarea impactului asupra protecţiei datelor; şi

orice alte informaţii solicitate de autoritatea de supraveghere.

(2) Dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere şi sa obţină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecţia sociala şi sănătatea publică.

CAP.10 RESPONSABILUL DE PROTECŢIA DATELOR CU CARACTER PERSONAL

10.1. Alocarea responsabilităţilor/sarcinilor aferente Responsabilului de protecţia datelor

(1) La nivelul Centrului Național de Management al Apei Grele sarcinile/responsabilităţile Responsabilului cu protecţia datelor au fost alocate unui responsabil cu protecţia datelor.

(2) Responsabilităţile alocate/stabilite prin Fisa de post sunt următoarele:

- participă la procesul de tranziţie către conformitatea cu Regulamentul privind Protecţia Datelor cu Caracter Personal (GDPR);

- informează şi consiliază Centrul Național de Management al Apei Grele, sau persoana împuternicită de Centrul Național de Management al Apei Grele, precum şi angajaţii organizaţiei care se ocupă de prelucrare datelor cu caracter personal privind obligaţiile (naţionale şi europene) referitoare la prelucrarea datelor cu caracter personal, precum şi cu privire la orice aspect legat de protecţia datelor cu caracter personal;

- acordă consiliere şi se implica în mod direct în efectuarea evaluărilor de impact asupra protecţiei datelor, monitorizează funcţionarea acestora, inclusiv privind consultarea prealabilă a autorităţii de supraveghere, dacă este cazul;

- monitorizează respectarea prevederilor legale (naţionale şi europene) şi ale reglementărilor interne referitoare la protecţia datelor personale la nivelul Centrului Național de Management al Apei Grele;

- monitorizează alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

- participă la instruirea angajaţilor implicaţi în operaţiunile de prelucrare a datelor personale;

- participă la activitatea de actualizare a evidenţei operaţiunilor de prelucrare a datelor personale şi monitorizează corectitudinea acesteia;

- redactează şi negociază clauze contractuale privind prelucrarea datelor cu caracter personal;

- monitorizează, utilizând metoda eşantionului, modul în care persoanele ale căror date cu caracter personal se procesează, au fost informate de drepturile pe care le au;

- asigură asistenţa privind gestionarea prelucrării de date cu caracter personal, menţinerea registrului de prelucrări a datelor personale precum şi registrul privind incidentele de securitate şi efectuează notificările privind încălcarea securităţii datelor personale;

- persoanele vizate pot contacta şi solicită asistenţa de specialitate din partea Responsabilului cu protecţia datelor cu privire la toate aspectele legate de prelucrarea datelor si de exercitarea drepturilor lor;

- cooperează cu autoritatea de supraveghere (ANSPDCP) si acţionează ca punct de contact în relaţia cu autoritatea de supraveghere, persoanele vizate, precum şi în cadrul unitatii în legătură cu aspecte de prelucrare;

10.2. Responsabilităţile Centrului Național de Management al Apei Grele faţă de Responsabilul de protecţia datelor

(1) Conducerea Centrului Național de Management al Apei Grele şi conducătorii entităţilor funcţionale din cadrul intituției se vor asigură că Responsabilul cu protecţia datelor este implicat corespunzător şi în timp util în toate aspectele legate de protecţia datelor cu caracter personal;

(2) Conducerea Centrului Național de Management al Apei Grele şi conducătorii entităţilor funcţionale din cadrul instituției vor acorda întregul sprijin Responsabilului de date personale, asigurându-i resursele necesare pentru executarea atribuţiilor sale, precum şi pentru accesarea datelor cu caracter personal şi a operaţiunilor de prelucrare şi pentru menţinerea cunoştinţelor sale de specialitate;

(3) În desfăşurarea activităţii, Responsabilul de protecţia datelor nu va primi niciun fel de instrucţiuni în ceea ce priveşte îndeplinirea atribuţiilor sale în legătură cu GDPR.

(4) Conducerea Centrului Național de Management al Apei Grele şi responsabilul cu protecţia datelor se vor asigura ca niciuna din sarcinile celui din urma nu generează un conflict de interese.

CAP.11 TRANSFERURILE DE DATE CU CARACTER PERSONAL CATRE ŢĂRI TERŢE SAU ORGANIZAŢII INTERNAŢIONALE

11.1. Orice decizie de a transfera date în afara spaţiului Uniunii Europene şi al Zonei Economice-Europene va fi supusă, anterior transferului şi în timp util, analizei Responsabilului de protecţia datelor.

(1) Transferurile de date în afara spaţiului Uniunii Europene şi al Zonei Economice-Europene se pot face:

- in temeiul unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecţie;

- in baza unor garanţii adecvate oferite de unitate sau persoana împuternicită a unitatii.

Garanţiile adecvate pot fi furnizate prin:

- un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice;

- reguli corporatiste obligatorii;

- clauze standard de protecţie a datelor adoptate de Comisia Europeană;

- clauze standard de protecţie a datelor adoptate de o autoritate de supraveghere şi aprobate de Comisia Europeană;

- un cod de conduita aprobat, însoţit de un angajament obligatoriu şi executoriu din partea Centrului Național de Management al Apei Grele sau a persoanei împuternicite de Centrul

Național de Management al Apei Grele din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

- un mecanism de certificare aprobat, însoţit de un angajament obligatoriu şi executoriu din partea Centrului Național de Management al Apei Grele sau a persoanei împuternicite de Centrul Național de Management al Apei Grele din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

11.2. Sub rezerva autorizării din partea autorităţii de supraveghere, garanţiile adecvate pot fi furnizate, în special, prin:

- clauze contractuale între Centrului Național de Management al Apei Grele, persoana împuternicită de Centrul Național de Management al Apei Grele şi operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din ţara terţă sau organizaţia internaţională; sau
- dispoziţii care urmează să fie incluse în acordurile administrative dintre autorităţile sau organismele publice, care includ drepturi opozabile şi efective pentru persoanele vizate.

11.3.În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie sau a unor garanţii adecvate, un transfer de date către o ţara terţă sau o organizaţie internaţională poate avea loc numai în una dintre condiţiile următoare:

- persoana vizată şi-a exprimat în mod explicit acordul cu privire la transfer, după ce a fost informată asupra posibilelor riscuri pe care transferurile le pot implica pentru persoana vizată;
- transferul este necesar pentru executarea unui contract între persoana vizată şi Centrul Național de Management al Apei Grele sau pentru aplicarea unor masuri precontractuale adoptate la cererea persoanei vizate;
- transferul este necesar pentru încheierea sau pentru executarea unui contract încheiat în interesul persoanei vizate între Centrului Național de Management al Apei Grele şi o alta persoană fizică sau juridică;
- transferul este necesar din considerente importante de interes public;
- transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanţă;
- transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizata nu are capacitatea fizica sau juridica de a-şi exprima acordul;
- transferul se realizează dintr-un registru care, potrivit dreptului UE sau al dreptului intern, are scopul de a furniza informaţii publicului şi care poate fi consultat de public în general, sau de orice persoană care poate face dovada unui interes legitim.

11.4. In lipsa unei decizii a Comisiei, a unor garanţii adecvate dar şi în lipsa condiţiilor precizate anterior, un transfer către o ţara terţă sau o organizaţie internaţională poate avea loc numai în cazul în care:

- transferul nu este repetitiv;
- se referă doar la un număr limitat de persoane vizate;
- este necesar în scopul realizării intereselor legitime majore urmărite de operator – Centrul Național de Management al Apei Grele.

CAP.12 CĂI DE ATAC, RĂSPUNDERI, MĂSURI ŞI SANCŢIUNI SPECIFICE

12.1.Fără a aduce atingere oricăror alte cai de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere, în special în statul membru în care îşi are reşedinţa obişnuită, în care se află locul sau de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încălca prezentul regulament.

12.2.Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluţia şi rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul legislaţiei specifice.

12.3.Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercită o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorităţi de supraveghere care o vizează.

12.4. Fără a aduce atingere oricăror alte cai de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercită o cale de atac judiciară eficientă în cazul în care autoritatea de supraveghere competentă nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluţionarea plângerii depuse.

12.5.Acţiunile introduse împotriva unei autorităţi de supraveghere sunt aduse în faţa instanţelor din statul membru în care este stabilită autoritatea de supraveghere.

12.6. În cazul în care acţiunile sunt introduse împotriva unei decizii a unei autorităţi de supraveghere care a fost precedata de un aviz sau o decizie a Comitetului european pentru protecţia datelor în cadrul mecanismului pentru asigurarea coerenţei, autoritatea de supraveghere transmite curţii avizul respectiv sau decizia respectivă.

12.7. Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere la o autoritate de supraveghere, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul legii au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prevederile legale specifice.

12.8. Acţiunile introduse împotriva unui operator sau unei persoane împuternicite de operator sunt prezentate în fata instanţelor din statul membru unde operatorul sau persoana împuternicită de operator îşi are un sediu. Alternativ, o astfel de acţiune poate fi prezentată în faţa instanţelor din statul membru în care persoana vizată îşi are reşedinţa obişnuita, cu excepţia cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acţionează în exercitarea competentelor sale publice.

12.9. Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a legislaţiei specifice are dreptul să obţină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit. Orice operator implicat în operaţiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operaţiunile sale de prelucrare care încalcă prevederile legislaţiei specifice. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligaţiile din legislaţia specifică care revin în mod specific persoanelor împuternicite de operator sau a acţionat în afara sau în contradicţie cu instrucţiunile legale/contractuale ale operatorului. Operatorul sau persoana împuternicită de operator este exonerat(ă) de răspundere dacă dovedeşte că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.

12.10. Autoritatea de supraveghere asigură faptul că impunerea unor amenzi administrative pentru încălcările prevederilor legislaţiei specifice este, în fiecare caz, eficace, proporţională şi disuasiva. În funcţie de circumstanţele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menţionate de legislaţia specifică.

Autoritatea poate:

- să emită avertizări;
- să emită mustrări;
- să dea dispoziţii;
- să oblige operatorul să informeze persoana vizată cu privire la o încălcare a protecţiei datelor;
- să limiteze sau să interzică prelucrarea;
- sa dispună rectificarea sau ştergerea datelor sau restricţionarea prelucrării.

(1) În cazul în care operatorul va fi sancţionat administrativ pentru nerespectarea legislaţiei privind protecţia datelor cu caracter personal, Responsabilul de protecţia datelor va analiza oportunitatea contestării sancţiunii administrative şi va formula propuneri în legătură cu în legătură promovarea căii de atac, precum şi, dacă este cazul, va elabora contestaţia, urmând să analizeze cel puţin următoarelor aspecte:

- natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauza, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;
- dacă încălcarea a fost comisă intenţionat sau din neglijenţă;

orice acţiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;

- gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia;
- eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
- gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea şi a atenua posibilele efecte negative ale încălcării;
- categoriile de date cu caracter personal afectate de încălcare;
- modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, în special dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
- în cazul în care măsurile menţionate de legislaţia specifică au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauza cu privire la acelaşi obiect, respectarea respectivelor masuri;
- aderarea la coduri de conduită sau la mecanisme de certificare aprobate; şi

orice alt factor agravant sau atenuant aplicabil circumstanţelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(2) Responsabilul de date personale va reprezenta operatorul în cadrul procedurii administrative în fata autorităţii cât şi în situaţia în care se va contesta decizia autorităţii în fata instanţelor judecătoreşti.

CAP.13 RESPONSABILITĂŢI ÎN CADRUL CENTRULUI NAȚIONAL DE MANAGEMENT AL APEI GRELE

13.1. Cunoaşterea şi aplicarea corespunzătoare a prezentului Regulament reprezintă obligaţia întregului personal angajat al Centrului Național de Management al Apei Grele potrivit limitelor de autoritate aprobate;

13.2. Responsabilităţile privind protecţia datelor cu caracter personal revin gradual întregului personal al Centrului Național de Management al Apei Grele;

13.3. Responsabilităţile în ceea ce priveşte elaborarea, avizarea, aprobarea, implementarea, supravegherea şi evaluarea aplicabilităţii prezentului Regulament, precum şi dispunerea masurilor care se impun revin, după cum urmează:

- Centrului Național de Management al Apei Grele (cu toate structurile organizatorice), în calitate de Operator:

- asigură implementarea legislaţiei comunitare-UE şi naţionale privind protecţia datelor cu caracter personal la nivelul Centrului Național de Management al Apei Grele, prin prezentul regulament sau alte acte interne ;

- asigură conformarea tuturor activităților de prelucrare cu prevederile legislaţiei comunitare-UE şi naţionale privind protecţia datelor cu caracter personal;

- asigură informarea persoanelor vizate şi respectă drepturile acestora;

- ia măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal; asigură respectarea prezentului regulament privind masurile de protecţie a persoanelor cu privire la prelucrarea datelor cu caracter personal.

13.4. Organele de Conducere ale Centrului Național de Management al Apei Grele, conducătorii structurilor sale organizatorice (secţii, servicii, birouri, compartimente etc.) sunt responsabili cu protecţia datelor cu caracter personal pentru activităţile coordonate şi au în acest sens următoarele responsabilităţi specifice:

- stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare în contextul derulării activităţii comerciale/contractuale şi/sau participării la evenimentele specializate organizate de unitate şi/sau în incinta unităţii, inclusiv desfăşurării activităţii curente, precum şi în contextul îndeplinirii obligaţiilor legale;

- asigură implementarea şi monitorizează respectarea actelor de reglementare internă şi a legislaţiei specifice, în materia prelucrării datelor cu caracter personal de către utilizatorii (angajaţii) din subordine;

- coordonează şi monitorizează activitatea personalului pe linia protecţiei datelor cu caracter personal la nivelul operatorului;

- asigura desfăşurarea pregătirii de specialitate şi instruirea utilizatorilor în acest domeniu;

- dispun masuri de completare sau, după caz, de modificare a fişei posturilor utilizatorilor;

- analizează şi dispun în ceea ce priveşte suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidenţă a datelor cu caracter personal, în condiţiile legii;

- dispun masuri organizatorice pentru exercitarea drepturilor de către persoana vizată;

- coordonează procesul de furnizare a datelor şi informaţiilor necesare în vederea soluţionării cererilor persoanelor vizate;

- ţin evidenţa cererilor persoanelor vizate care au legătură cu activităţile coordonate ce implica prelucrarea datelor cu caracter personal;

- analizează periodic activitatea utilizatorilor;

- informează operativ Responsabilul de protecţia datelor despre vulnerabilităţile şi riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii şi propune masuri pentru înlăturarea acestora;

- informează operativ Responsabilul cu protecţia datelor în legătură cu orice încălcare a normelor de protecţie a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate, cu privire la masurile dispuse pentru identificarea persoanei responsabile şi limitarea efectelor unei diseminări neautorizate a datelor, precum şi cu privire la situaţiile în care au fost emise recomandări sau aplicate sancţiuni de către Autoritatea naţionala de supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigaţii.

13.5.Utilizatorii, respectiv angajaţii Centrului Național de Management al Apei Grele care prelucrează date cu caracter personal au următoarele responsabilităţi specifice:

- să cunoască şi să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum şi ale prezentului regulament;

- să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condiţiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute şi consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de lege, condiţiile în care pot fi exercitate aceste drepturi etc.;

- să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin şefilor ierarhici, organelor de conducere ale Centrului Național de Management al Apei Grele, pentru realizarea activităţilor specifice ale acestora;

- să păstreze confidenţialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;

- să respecte masurile de securitate, precum şi celelalte reguli stabilite la nivelul Centrului Național de Management al Apei Grele;

- să informeze de îndată seful ierarhic şi Responsabilul de protecţia datelor personale despre împrejurări de natura a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situaţie în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă.

13.6. Derulatorii de contracte din cadrul Centrului Național de Management al Apei Grele au responsabilitatea / obligativitatea inserării în contractele încheiate şi gestionate de către aceştia a clauzelor specifice, cu privire la protecţia datelor cu caracter personal şi/sau cu privire la respectarea Condiţiilor Generale, Tehnice şi de Participare. In situaţiile în care sunt prelucrate date cu caracter personal în numele Centrului Național de Management al Apei Grele de către persoane împuternicite (procesatori de date-ex: instituţii de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariaţi, companii de curierat etc.), derulatorii de contract vor avea responsabilitatea/obligativitatea de încheia cu fiecare dintre aceste persoane împuternicite acorduri de prelucrare a datelor cu caracter personal, care vor avea în conţinut elementele prevăzute în prezentul Regulament şi legislaţia specifică, stabilite în prealabil de Responsabilul de protecţia datelor şi aprobate de conducerea Centrului Național de Management al Apei Grele.

13.7. Specialistul Resurse Umane: asigură informarea potenţialilor angajaţi şi a angajaţilor Centrului Național de Management al Apei Grele cu privire la prelucrarea datelor cu caracter personal şi la drepturile de care beneficiază potrivit legii, participă la organizarea şi administrarea programelor de pregătire continuă a angajaţilor în domeniul protecţiei datelor personale, pune la dispozitia salariatilor, la angajare, în vederea informării şi luării la cunoştinţă cu privire la prevederile prezentului Regulament şi se asigură de semnarea de către salariaţi a Angajamentului de Conformare conform **Anexei nr. 5,**

13.8. Specialistul IT – responsabil cu: luarea măsurilor tehnice şi organizatorice, specifice zonei IT, prevăzute de prezentul Regulament: elaborarea/ implementarea/ monitorizarea permanentă a politicilor/procedurilor specifice de protecţie/securitate a datelor cu caracter personal la nivelul Centrului Național de Management al Apei Grele, precum si instruirea utilizatorilor/angajaţilor cu privire la politicile/procedurilor specifice de protecţie/securitate a datelor cu caracter personal la nivelul Centrului Național de Management al Apei Grele

13.9. Serviciul Administrativ – responsabil cu suportul tehnic, respectiv cu afişarea Notelor de Informare privind protecţia datelor şi aplicarea indicatoarelor de marcare a existenţei sistemului de supraveghere video, în locurile unde sunt amplasate camere de supraveghere video-CCTV, va verifica periodic starea fizică a informărilor şi a indicatoarelor anterior menţionate şi va răspunde de siguranţa şi confidenţialitatea datelor personale stocate în sistemul de supraveghere/monitorizare video.

CAP.14 ANGAJAMENTUL DE CONFORMARE A ANGAJAŢILOR FAŢĂ DE LEGISLAŢIA SPECIFICĂ ŞI REGULAMENTUL PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL

14.1. La angajare, înainte de începerea activităţilor de prelucrare a datelor cu caracter personal, dar şi ulterior, cu ocazia derulării raporturilor de muncă, organizării de instruiri profesionale specifice, toţi angajaţii care prelucrează date cu caracter personal trebuie să semneze un Angajament individual de conformare faţă de legislaţia specifică şi a prezentului Regulament. Modelul de Angajament de conformare utilizat este prevăzut în **Anexa nr. 5.**

14.2. Confirmarea scrisă reprezintă asumarea individuală a angajamentului de respectare a legislaţiei specifice şi a prezentului regulament privind protecţia datelor cu caracter personal, în scopul protejării reputaţiei unităţii şi aplicării standardelor de etica în afaceri.

14.3. Semnătura de confirmare înseamnă :

- că angajatul a luat cunoştinţă despre prevederile prezentului regulament privind protecţia datelor cu caracter personal;
- că angajatul a participat la programele de pregătire şi a fost instruit conform prevederilor prezentului regulament adoptat în acest domeniu;
- că angajatul înţelege importanţa respectării în totalitate a cerinţelor cuprinse în legislaţia specifică şi în prezentul regulament privind protecţia datelor cu caracter personal;
- că angajatul îşi asumă necondiţionat responsabilitatea în ceea ce priveşte conformarea cu cerinţele cuprinse în legislaţia specifică şi în prezentul regulament privind protecţia datelor cu caracter personal;

- că angajatul înţelege că, în situaţia nerespectării principiilor şi cerinţelor cuprinse în prezentul regulament privind protecţia datelor cu caracter personal, se face direct răspunzător pentru încălcarea angajamentului individual şi pentru consecinţele ce decurg din acesta.

14.4. Refuzul de a semna confirmarea angajamentului individual înseamnă că este necesară identificarea motivelor reale care au condus la refuz, că este necesara instruirea suplimentară, dacă motivul real este neînţelegerea mesajului sau informaţiilor transmise, precum si că este necesară, de asemenea, examinarea atenta a angajatului respectiv, urmată de luarea unor masuri adecvate, mai ales în situaţia în care acesta ocupă o funcţie care prezintă un risc sensibil la adresa unitatii, dacă refuzul de a semna confirmarea nu are o motivaţie reală.

14.5. Angajamentele de Conformare semnate de salariaţi se vor păstra în evidentele Specialistului de Resurse Umane.

CAP.15 DISPOZIŢII FINALE

Prezentul Regulament are caracter „Uz intern”, difuzarea acestuia neautorizată de către salariaţi către terţe persoane intră sub incidenţa Angajamentului de conformare şi se sancţionează conform legislaţiei în vigoare iar nerespectarea lui atrage sancţiuni din partea organelor de reglementare/supraveghere competente, în condiţiile legii.

Aplicarea sancţiunilor administrative nu înlătură răspunderea penală, civilă, materială sau contravenţională, după caz, a persoanelor vinovate.

Prezentul regulament completează: regulamentele, procedurile interne, precum şi orice alte acte de reglementare internă.

Dacă ulterior datei intrării în vigoare a prezentei reglementari, o prevedere legală modifică, completează sau abrogă prevederi ale prezentului regulament, se vor aplica de drept prevederile legale în vigoare.