AGENŢIA ROMÂNĂ DE SALVARE A VIEŢII OMENEŞTI PE MARE CONSTANŢA
Nr. 10.565
din 21.09.2021

AGENŢIA ROMÂNĂ DE SALVARE A VIEŢII OMENEŞTI PE MARE

Adresa: Incintă Port Constanta, Dana 78, 900900, Constanţa, România
Tel./Fax: +40 241 616111; +40 241 488226; +40 241 488227
E-mail: arsvom@intersat-telecom.ro; Web: www.arsvom.ro; CUI: 16330145

APROB
DIRECTOR GENERAL
Lt. Col. Dr. Ing. VOICU IONUȚ

Ministerul Transporturilor și Infrastructurii
Agenția Română de Salvare a Vieții Omenești pe Mare Constanța
ROMÂNIA
21.09.2021

NORME INTERNE

referitoare la respectarea regulamentului general privind protecția datelor cu caracter personal (RGPD)

CUPRINS

CAP. 1 DISPOZIȚII GENERALE 5

1.1. Obiect și obiective 5

1.2. Domeniu de aplicare 5

1.3. Termeni și definiții: 5

1.4. Documente de referință (Acte normative în domeniul GDPR): 10

CAP. 2 PRINCIPII LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL 10

2.1. Legalitate, echitate și transparență 10

2.2. Limitări legate de scop 10

2.3. Minimizarea/Reducerea la minimum a datelor 10

2.4. Exactitatea informațiilor 10

2.5. Limitarea stocării 11

2.6. Integritate și confidențialitate 11

2.7. Responsabilitate 11

CAP. 3 LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL 12

CAP. 4 CONSIMȚĂMÂNTUL PERSOANEI VIZATE ȘI CONDIȚIILE PRIVIND CONSIMȚĂMÂNTUL 13

CAP. 5 REGULI SPECIALE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL 15

5.1. Prelucrarea unor categorii speciale de date cu caracter personal 15

5.2. Prelucrarea datelor cu caracter personal speciale cu funcție de identificare generală. 17

5.3. Prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni. 17

5.4. Prelucrarea care nu necesită identificarea 17

5.5. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video. 18

5.6. Prelucrarea în contextul ocupării unui loc de muncă 18

5.7. Prelucrarea datelor cu caracter personal în scop promoțional (marketing) 19

CAP.6 DREPTURILE PERSOANEI VIZATE ÎN CONTEXTUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL 20

6.1. Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate 20
6.2. Dreptul la informare 21
6.3. Dreptul de acces al persoanei vizate 26
6.4. Dreptul la rectificare 27
6.5. Dreptul la ștergerea datelor ("dreptul de a fi uitat") 27
6.6. Dreptul la restricționarea prelucrării 28
6.7. Obligația de notificare cu privire la rectificarea, ștergerea datelor cu caracter personal sau restricționarea prelucrării. 28
6.8. Dreptul la portabilitatea datelor 29
6.9. Dreptul la opoziție și procesul decizional individual automatizat 29

CAP. 7 RESTRICȚII 31

CAP. 8 OPERATORUL (ARSVOM Constanța) ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR 31

8.1. Responsabilitatea Operatorului 31
8.2. Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit.. 35
8.3. Persoana împuternicită de Operator 36
8.4. Desfășurarea activității de prelucrare sub autoritatea Operatorului sau a persoanei împuternicite de operator. 39
8.5. Evidențele activităților de prelucrare 39
8.6. Cooperarea cu Autoritatea de supraveghere 40
8.7. Masuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal 41
8.8. Notificarea Autorității de Supraveghere în cazul încălcării securității datelor cu caracter personal 45
8.9. Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal 46

CAP. 9 EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR ȘI CONSULTAREA PREALABILĂ (DACĂ ESTE CAZUL) 47

9.1. Evaluarea impactului asupra protecției datelor 47
9.2. Consultarea prealabilă a Autorității de Supraveghere 49

CAP.10 RESPONSABILUL DE PROTECȚIA DATELOR (DPO) 49

10.1. Alocarea responsabilităților/sarcinilor aferente DPO 49
10.2. Responsabilitățile operatorului față de DPO 50

CAP.11 TRANSFERURILE DE DATE CU CARACTER PERSONAL CATRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE(DACĂ ESTE CAZUL) **51**

CAP.12 CĂI DE ATAC, RĂSPUNDERI, MĂSURI ȘI SANCȚIUNI SPECIFICE **53**

12.1. Dreptul de a depune o plângere la o autoritate de supraveghere 53

12.2. Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere 53

12.3. Dreptul la o cale de atacă eficientă împotriva unui operator sau a unei persoane împuternicite de operator 54

12.4. Dreptul la despăgubiri și răspunderea operatorului sau a persoanei împuternicite de operator (dacă este cazul) 54

12.5. Condiții generale pentru impunerea amenzilor administrative 55

CAP.13 RESPONSABILITĂȚI ÎN CADRUL ARSVOM Constanța **56**

CAP.14 ANGAJAMENTUL DE CONFORMARE A ANGAJAȚILOR FAȚĂ DE LEGISLAȚIA SPECIFICĂ ÎN DOMENIUL PROTECȚIEI DATELOR CU CARACTER PERSONAL **60**

CAP. 15 PREGĂTIREA ȘI INSTRUIREA PERSONALULUI ABILITAT SĂ ACCESEZE ASTFEL DE INFORMAȚII **61**

CAP. 16 DISPOZIȚII FINALE **62**

ANEXE **64**

CAP. 1 DISPOZIȚII GENERALE

1.1. Obiect și obiective

1.1.1. Prezentele norme asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora în ceea ce privește protecția datelor cu caracter personal;

1.1.2. Exercitarea drepturilor prevăzute în prezentele norme nu poate fi restrânsă decât în cazurile expres și limitativ prevăzute de lege.

1.1.3. Libera circulație a datelor cu caracter personal în interiorul Uniunii Europene nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

1.2. Domeniu de aplicare

1.2.1. Prezentele norme se aplică tuturor angajaților instituției cu atribuții de prelucrare a datelor cu caracter personal și/sau după caz persoanelor împuternicite ale acesteia.

1.2.2. Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuat total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor.

1.3. Termeni și definiții:

1. "*Date cu caracter personal*", acronim DCP , înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("Persoană vizată"). O persoană fizică 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 on-line, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

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

- colectarea, strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale și din orice sursă;
- înregistrarea - consemnarea datelor cu caracter personal într-un sistem de evidență automată ori neautomată, care poate fi registru, fișier automat, bază

de date sau orice formă de evidență organizată, structurată ori ad-hoc sau întrun text, înșiruire 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 atribuțiilor legale ale operatorului, în scopul eficientizării/optimizării activităților de prelucrare a acestora;
- stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranță;
- adaptarea - transformarea datelor cu caracter personal colectate inițial, conform criteriilor prestabilite și scopurilor pentru care au fost colectate;
- modificarea - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menținerii caracteristicilor de exactitate, realitate, actualitate;
- extragerea - scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială;
- consultarea - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operațiuni sau set de operațiuni de prelucrare ulterioare;
- utilizarea - folosirea datelor cu caracter personal, în tot sau în parte, de către și în interiorul operatorului, împuterniciților operatorului ori destinatarului, dup caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;
- dezvăluirea/divulgarea - a face disponibile date cu caracter personal către terți prin comunicare, transmitere, diseminare sau punerea la dispoziție 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 inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;
- blocarea - întreruperea prelucrării datelor cu caracter personal;
- restricționarea - marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

- ștergerea - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidențe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistența, inexactitatea;
- transformarea - operațiunea efectuat asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;
- distrugerea - aducerea la stare de neîntrebuințare, în condițiile legii, definitiv și irecuperabil, prin mijloace mecanice sau termice, a suportului fizică 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 persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se afla persoana fizică respectiv 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 informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri tehnice și organizatorice care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

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

6. *"Operator"* înseamnă persoană fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoană fizică sau juridică, de drept public ori de drept privat, care este desemnat ca operator prin acel act normativ sau în baza acelui act normativ. În sensul prezentului regulament ARSVOM are calitatea de operator, cu toate entitățile funcționale/structurile organizatorice – departamente, servicii, birouri, compartimente, etc., dacă stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal.

7.*"Persoană împuternicită de operator/procesator"* înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
8. *"Destinatar"* înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile 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 autoritățile publice respective respect normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;
9.*"Parte terță"* înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoană împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
10.*"Consimțmânt"* al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o „Declarație„ sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
11.*"Încălcarea securității datelor cu caracter personal"* înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizat 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 moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezulta în special în urma unei analize a unei mostre de material biologică recoltate de la persoană în cauză;
13.*"Date biometrie"* 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 confirmă 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 asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

15. *"Întreprindere"* înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;
16. *"Grup de întreprinderi"* înseamnă o întreprindere care exercit controlul și întreprinderile controlate de aceasta;
17. *"Reguli corporatiste obligatorii"* înseamnă politicile în materie de protecție 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 privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe 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 Națională de Supraveghere a Datelor cu Caracter Personal;
19. *„Codul numeric personal (CNP)"* înseamnă un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a stării civile a acesteia și de identificare în anumite sisteme informatice de către persoanele autorizate;
20. *„Date cu caracter personal cu funcție de identificare de aplicabilitate generală (date cu caracter special)"* înseamnă numere prin care se identifică o persoană fizică în anumite sisteme de evidență și care au aplicabilitate generală, cum ar fi: codul numerică personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate;
21. *„Utilizator"* înseamnă orice persoană care acționează 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, respectiv al primăriei sau al împuternicitului acestuia ale cărei atribuții de serviciu presupun operațiuni de prelucrare a datelor cu caracter personal.
22. *„Responsabilul de protecția datelor"*, cu acronim DPO, înseamnă persoană din cadrul ARSVOM Constanța cu sarcini/responsabilități specifice privind funcționarea corespunzătoare a sistemului de protecție a datelor cu caracter personal, în conformitate cu prevederile RGPD precum și elaborarea,

implementarea și monitorizarea respectării prevederilor Regulamentului UE nr. 679/2016.

1.4. Documente de referință (Acte normative în domeniul GDPR):

- Regulamentul (UE) 679/2016 al Parlamentului European si al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (RGPD);
- Legea nr. 190/2018 referitoare la protecția datelor cu caracter personal în România;
- Ghiduri explicitate ale Grupului de Lucru Art. 29 al Uniunii Europene (Comitetul European pentru protectia datelor - CEPD);
- Regulamente și proceduri interne ;

CAP. 2 PRINCIPII LEGATE DE PRELUCRAREA DATELOR CU CARACTER PERSONAL

2.1. Legalitate, echitate și transparență

Un principiu esențial, strâns asociat cu drepturile fundamentale ale omului. Datele cu caracter personal trebuie să fie prelucrate „în mod legal, echitabil și transparent față de persoana vizată.";

2.2. Limitări legate de scop

Datele personale trebuie să fie colectate în scopuri bine determinate, explicite și legitime, iar prelucrările ulterioare nu trebuie să se abat de la aceste scopuri. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică/ istorică ori în scopuri statistice nu se consideră incompatibilă de la scopurile inițiale;

2.3. Minimizarea/Reducerea la minimum a datelor

Orice colectare de date personale trebuie foarte bine analizată înainte de obținerea 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 informațiilor

Datele cu caracter personal trebuie să fie exacte, și 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 șterse sau rectificate fără întârziere;

2.5. Limitarea stocării

Datele trebuie păstrate fix atât timp cât sunt necesare pentru prelucrarea asumată. Perioadele mai lungi de stocare sunt excepții asociate cu activități de prelucrare în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, conform art. 89, alin.1 din RGPD, sub rezerva punerii în aplicare a măsurilor tehnice și organizatorice adecvate prevăzute de RGPD în vederea garantării drepturilor și libertăților persoanei vizate;

2.6. Integritate și confidențialitate

Prelucrarea datelor personale trebuie făcută în cele mai adecvate Condiții de siguranță, care să includă „protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare". Nerespectarea acestui principiu expune direct la breșe de securitate și confidențialitate și implicit, la penalitățile extrem de severe prevăzute de RGPD;

2.7. Responsabilitate

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

În consecință:

- Orice prelucrare de date cu caracter personală trebuie să fie legală și echitabilă;
- Ar trebui să fie transparentă pentru persoanele fizice vizate că sunt colectate, utilizate, consultate sau prelucrate datele cu caracter personal care le privește și în ce măsură datele sunt sau vor fi prelucrate;
- Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal trebuie să fie ușor accesibile și ușor de înțeles și ca trebuie să se utilizeze un limbaj simplu și clar;
- Persoanele fizice trebuie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea;
- Scopurile specifice în care datele cu caracter personal sunt prelucrate trebuie să fie explicite și legitime și să fie determinate la momentul colectării datelor respective;

- Datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, 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 îndeplinită în mod rezonabil prin alte mijloace;
- Operatorul trebuie să stabilească termene pentru ștergere 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 șterse;
- Datele personale trebuie prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizat a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

CAP. 3 LEGALITATEA PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

a) **persoana vizată și-a dat consimțământul** pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

b) **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;

c) **prelucrarea este necesară în vederea îndeplinirii unei obligații legale** care îi revine operatorului;

d) **prelucrarea este necesară pentru a proteja interesele vitale** ale persoanei vizate sau ale altei persoane fizice;

e) **prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public** sau care rezultă din exercitarea autorității publice cu care este investit operatorul;

f) **prelucrarea este necesară în scopul intereselor legitime** urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile

și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când menționată este un copil. „Interesele legitime ale unui operator", inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se afla în serviciul acestuia. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor poate constitui un interes legitim al operatorului de date în cauză.

CAP. 4 CONSIMȚĂMÂNTUL PERSOANEI VIZATE ȘI CONDIȚIILE PRIVIND CONSIMȚĂMÂNTUL

4.1. În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat **consimțământul expres, neechivoc, liber și informat** pentru prelucrarea datelor sale cu caracter personal.
4.2. În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentat într-o formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.
4.3. Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia.
4.4. Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționat sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesar pentru executarea acestui contract.

4.5. **La nivelul instituției, în calitate de Operator de date personale, consimțământul persoanelor vizate este acordat**:
- în cadrul procesului de recrutare/selecție de personal;
- în situația încheierii unor contracte cu partenerii colaboratori, exclusiv în situația în care prelucrarea datelor personale se face în scop de marketing direct (furnizarea de informații despre serviciile, evenimentele și manifestările expoziționale ale instituției);
- în situația abonării la newsletter (furnizarea de informații despre serviciile, evenimentele și manifestările expoziționale ale instituțiilor statului);
- în situația înregistrării unui cont pe website-uri, pentru evenimente (în scop de marketing direct).

4.6. În cadrul procesului de recrutare/selecție de personal, biroul de Resurse Umane va solicita acordarea consimțământului de către potențialul angajat prin semnarea de către acesta a unei Note de Informare prin care declară că a fost informată în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției, precum și în legătură cu drepturile de care beneficiază, potrivit legislației specifice. Notele de Informare se vor păstra distinct în evidentele biroului de Resurse Umane.

4.7. În situația în care conducătorul instituției decide prelucrarea în scop de marketing direct, respectiv furnizarea către partenerii contractuali a unor informații despre serviciile, evenimentele și manifestările expoziționale ale ARSVOM etc., entitățile funcționale/persoanele derulatoare/responsabile de contract vor avea în vedere în mod obligatoriu exprimarea consimțământului în scopul menționat anterior de către persoana vizată, prin bifarea unei căsuțe dedicate din contract. Lipsa consimțământului conduce la imposibilitatea prelucrării în scop de marketing direct.

4.8. În cazul abonării la newsletter, consimțământul persoanei vizate este dat prin bifarea unei căsuțe dedicate din secțiunea website-ului, persoana fiind informată cu privire la aspectele privind protecția datelor cu caracter personal.

4.9. În cazul înregistrării unui cont pe website-uri pentru achiziția de servicii/achitarea tarifelor online, accesarea unor servicii specifice, precum și în cazul invitaților online adresate vizitatorilor specialiști în vederea participării acestora la evenimente etc., consimțământul persoanei vizate este dat prin bifarea unor căsuțe dedicate din secțiunea website-ului, persoana fiind informată cu privire la aspectele privind protecția datelor cu caracter personal.

4.10. Entitățile funcționale/persoanele derulatoare/responsabile de contract, precum și cele responsabile de operațiunile de marketing direct (inclusiv serviciile aferente IT) vor avea în vedere în mod obligatoriu consimțământul exprimat în acest sens de către persoana vizată, pentru evitarea unor situații de neconformare față de prevederile legale privind protecția datelor personale.
4.11. Daca prelucrarea datelor personale se bazează pe consimțământ, prelucrarea datelor este legală daca persoana fizică are cel puțin vârsta de 16 ani.

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 apartenența la sindicate și prelucrarea de date genetice, de date biometrie pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.
5.1.2. Prevederile anterioare nu se aplica în următoarele situații:
a) când persoană vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede că interdicția prevăzut anterior să nu fi ridicat prin consimțământul persoanei vizate;
b) când prelucrarea este necesara în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției 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 garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;
c) când prelucrarea este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se afla in incapacitate fizică sau juridica de a-și da consimțământul;
d) când prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și

cu specifică politic, filozofic, religioasă sau sindicală, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și că datele cu caracter personal sa nu fie comunicate terților fără consimțământul persoanelor vizate;

e) când prelucrarea se refera la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

f) când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

g) când prelucrarea este necesara din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

h) când prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistenta socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute de lege, datele cu caracter personal pot fi prelucrate în scopurile menționate anterior în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate.

i) când prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional; sau

j) 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 speciale cu funcţie de identificare generală.

Datele cu caracter personal speciale 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 prevăzut în mod expresă de o dispoziţie legală. Prin legislaţia naţională se pot detalia condiţiile specifice de prelucrare a unui număr de identificare naţional sau a oricărui alt identificator cu aplicabilitate general. În acest caz, numărul de identificare naţională sau orice alt identificator cu aplicabilitate general 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 măsuri 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 instituţia în calitate de operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica persoana vizată în scopul unic al respectării legislaţiei specifice.

5.4.2. Daca, în cazurile menţionate anterior, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează 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 aplică, cu excepţia cazului în care persoană

vizată, în scopul exercitării drepturilor sale menționate anterior, oferă informații suplimentare care permit identificarea sa.

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

ARSVOM, prin intermediul sistemelor de supraveghere video, prelucrează datele cu caracter personal, respectiv imaginea și alte informații ce permit identificarea persoanelor vizate. Imaginile referitoare la persoane identificate sau identificabile, prelucrate prin mijloace de supraveghere video, constituie date cu caracter personal:

a) chiar dacă nu sunt asociate cu datele de identificare ale persoanei sau

b) chiar daca nu conțin imaginea persoanei filmate, ci alte informații de natură să conducă la identificarea acesteia (ex: numărul de înmatriculare al vehiculului). Scopul prelucrării datelor personale constă în respectarea prevederilor Legii nr. 333/2003, rsepectiv: monitorizarea/securitatea persoanelor, spațiilor și/sau bunurilor private, prevenirea și combaterea infracțiunilor, îndeplinirea obligațiilor legale și realizarea intereselor legitime. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se realizează numai de către persoane autorizate de operatorul de date. Informațiile înregistrate pot fi comunicate numai următorilor destinatari: persoana vizată, reprezentanții legali/împuterniciții persoanei vizate, reprezentanții autorizați a instituției, organele de urmărire/cercetare penală, instanțe judecătorești, în conformitate cu prevederile legislației interne și comunitare aplicabile activității desfășurate de instituție. Durata de stocare a datelor obținute prin intermediul sistemului de supraveghere video este de până la 30 de zile, cu excepția situațiilor exprese reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului înregistrările se distrug sau se șterg. Informarea video în cauză, precum și indicatoarele de marcare a existentei sistemului de supraveghere video vor fi aplicate în locurile unde sunt amplasate camerele de supraveghere video.

5.6. Prelucrarea în contextul ocupării unui loc de muncă

5.6.1. Prin lege sau prin acorduri colective, se pot prevedea norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de

muncă, al asigurării sănătății și securității la locul de muncă, al protejării proprietății angajatorului sau a clientului, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă.

5.6.2. Aceste norme includ măsuri corespunzătoare și specifice pentru garantarea demnității umane, a intereselor legitime și a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce privește transparența prelucrării, transferul de date cu caracter personal în cadrul unui grup de operatori de date personale sau al unui grup de operatori implicați într-o activitate economică comună și sistemele de monitorizare la locul de muncă.

5.7. Prelucrarea datelor cu caracter personal în scop promoțional (marketing)

Datele cu caracter personal furnizate de persoanele vizate (cum ar fi: nume și prenume, adresa de e-mail, nr. fax, nr. telefon mobil/fix) vor putea fi prelucrate doar cu consimțământul persoanelor vizate expres, neechivoc, liber, informat și anterior exprimat în anumite cazuri, cu respectarea drepturilor acestora, în special a dreptului de informare și opoziție, în următoarele scopuri: marketing (inclusiv marketing direct), concursuri, efectuarea de comunicări comerciale pentru serviciile instituției, inclusiv cele dezvoltate împreună cu un partener, prin orice mijloc de comunicare, inclusiv prin intermediul serviciilor de comunicații electronice. Datele cu caracter personal furnizate de persoanele vizate vor putea fi folosite în scop promoțional (marketing) și pentru produsele sau serviciile altor parteneri ai ARSVOM, cu respectarea drepturilor persoanelor vizate. Persoanele vizate își pot exercita dreptul de prevenire a unei asemenea prelucrări prin selectarea casetelor adecvate din formularele/documentele utilizate pentru colectarea datelor cu caracter personal. Indiferent de situație, în cazul în care menționată va dori ca datele cu caracter personal să nu mai fie prelucrate de operator, poate solicita în mod expres încetarea oricărei prelucrări de date din partea acesteia. Totodată, atunci când persoana vizată dorește să nu mai primească newsletter sau materiale informative din partea operatorului, se poate dezabona folosind butonul "Dezabonare" sau „Unsubscribe".

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

6.1. Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate

6.1.1. Instituția ia măsuri adecvate pentru a furniza persoanei vizate informațiile legale solicitate, precum și orice notificări și comunicări (în situația exercitării drepturilor de care beneficiază potrivit legii) referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

6.1.2. Instituția facilitează exercitarea drepturilor persoanei vizate.

6.1.3. Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri prin care își exercită drepturile de care beneficiază în baza legii, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două săptămâni atunci când este necesar.

6.1.4. ARSVOM informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

6.1.5. Daca nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoană vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciar.

6.1.6. Informațiile furnizate în temeiul legislației specifice și orice comunicare și orice măsuri luate în baza exercitării drepturilor de care beneficiază, potrivit legii, persoana vizată, sunt oferite gratuit. 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:

a) fie să perceapă o taxa rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
b) fie să refuze să dea cursă cererii. În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.
6.1.7. În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea prin intermediul căreia își exercit drepturile de care beneficiază, potrivit legii, persoana vizată, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.
6.1.8. Informațiile care urmează să fie furnizate persoanelor vizate în temeiul legislației specifice, pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativ asupra prelucrării avute în vedere.
6.1.9. Pentru exercitarea drepturilor prevăzute de legislația specifică și de prezentul Regulament, persoanele vizate se pot adresa DPO din cadrul ARSVOM Constanța cu o cerere scrisă, datată și semnată la adresa de e-mail: dpo@arsvom.ro sau la următoarea adresă de corespondență: ARSVOM Constanța, Incinta Port Constanța, Dana 78, județul Constanța. Operatorul poate, dacă este cazul, să solicite persoanei vizate să pun la dispoziție informații suplimentare pentru a stabili identitatea acesteia.

6.2. Dreptul la informare

6.2.1. Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate direct de la persoană vizată.
6.2.1.1. În cazul în care datele cu caracter personal referitoare la o Persoana vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate următoarele informații:
a) identitatea și datele de contact ale operatorului și, dup caz, ale reprezentantului acestuia;
b) datele de contact ale responsabilului cu protecția datelor;
c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridică al prelucrării;
d) interesele legitime urmărite de operator sau de o parte terță, dup caz;
e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal în afara Spațiului UE în condițiile prevederilor GDPR sau, o trimitere la garanțiile

adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

6.2.1.2. În plus, față de informațiile menționate anterior, în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă:

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

b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;

c) atunci când prelucrarea se bazează pe consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;

d) dreptul de a depune o plângere în fata unei autorități de supraveghere;

e) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;

f) dacă este cazul, existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.2.1.3. În cazul în care operatorul intenționează 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 această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante în vederea obținerii consimțământului acesteia;

6.2.1.4. Prevederile precedente nu se aplică dacă și în măsura în care Persoana vizată deține deja informațiile respective.

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

6.2.2.1 În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, instituția furnizează persoanei vizate următoarele informații:
a) identitatea și datele de contact ale operatorului și, dup caz, ale reprezentantului acestuia;
b) datele de contact ale responsabilului cu protecția datelor, dup caz;
c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridică al prelucrării;
d) categoriile de date cu caracter personal vizate;
e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, dup caz;
f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal în afara Spațiului UE și al Zonei Economice Europene și existența sau absența unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție sau, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.
6.2.2.2. Pe lângă informațiile menționate anterior, **operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigură a o prelucrare echitabil și transparent în ceea ce privește persoana vizată**:
a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
b) interesele legitime urmărite de operator sau de o parte terță, dup caz;
c) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
d) atunci când prelucrarea se bazează pe consimțământul persoanei vizate, existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
e) dreptul de a depune o plângere în fața unei autorități de supraveghere;
f) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;
g) dacă este cazul, existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.2.2.3. Operatorul furnizează informațiile menționate anterior:
a) într-un termen rezonabil dup obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;
b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către menționată respectivă; sau
c) dacă se intenționează 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 intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de aceasta prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante.
6.2.2.5 **Prevederile precedente nu se aplică dacă și în măsura în care:**
a) Persoana vizată deține deja informațiile;
b) furnizarea acestor informații se dovedește a fi imposibil sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute de lege, sau în măsura în care obligația furnizării informațiilor este susceptibil să facă imposibil sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia masuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului;
c) obținerea sau divulgarea datelor este prevăzută în mod expresă de dreptul Uniunii Europene sau de dreptul intern sub incidența căruia intra operatorul și care prevede masuri adecvate pentru a proteja interesele legitime ale persoanei vizate, sau
d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul.
6.2.3. Informarea persoanelor vizate în contextul activităților specifice operatorului. În contextul realizării atribuiților stabilite de lege și desfășurării activității curente a ARSVOM inclusiv derulării raporturilor de muncă, activității comerciale/contractuale sau alte evenimente specializate organizate în incinta

imobilului instituției, precum și în contextul îndeplinirii obligațiilor legale, informarea persoanelor vizate se poate realiza, după cum urmează:
- În cadrul procesului de recrutare/selecție de personal, biroul de Resurse Umane din cadrul instituției va pune la dispoziția potențialului angajat o Notă de Informare, pe care acesta/aceasta o va citi și o va semna și prin care declar că a fost informat/ă în legătură cu prelucrarea datelor cu caracter personal la nivelul instituției, precum și în legătură cu drepturile de care beneficiază, potrivit legislației specifice. Notele de informare se vor păstra distinct în evidențele biroului de Resurse Umane.
- În contextul derulării raporturilor de muncă, biroul de Resurse Umane va pune la dispoziția fiecărui angajat din cadrul instituției, o Notă de informare, pe care acesta/aceasta o va citi și o va semna și prin care declară că a fost informat/a în legătură cu prelucrarea datelor cu caracter personal la nivelul operatorului precum și în legătură cu drepturile de care beneficiază, potrivit legislației specifice.
Notele de informare se vor păstra distinct în evidentele biroului de Resurse Umane.
- Persoanele vizate, respectiv angajații, clienții/potențialii clienți, vizitatorii și alte persoane care intră în sediul ARSVOM ale căror date sunt prelucrate prin intermediul sistemelor de supraveghere video sunt informate în acest sens prin intermediul unor Note de informare. Informările în cauza, vor fi aplicate la vederea publicului.
În cadrul derulării activității comerciale/contractuale sau alte evenimente specializate organizate în incinta ARSVOM sau în alte locuri publice, informarea persoanelor vizate se realizează prin:

1) Condițiile generale, tehnice și de participare ale instituției, care conțin prevederi referitoare la protecția datelor personale;
2) Formularul care conține prevederi referitoare la protecția datelor personale;
3) Documentația contractuală încheiată de operator care conține prevederi referitoare la protecția datelor personale;
4) Termenii și Condițiile specifice website-urilor operatorului, care conțin prevederi referitoare la protecția datelor personale;
5) Website-urile ARSVOM, în ipoteza abonării la Newsletter, în cazul înregistrării unui cont pentru achiziția de servicii/achitarea tarifului online, accesarea unor servicii specifice, precum și în cazul invitațiilor online adresate vizitatorilor specialiști în vederea participării acestora la anumite evenimente, etc. Derulatorii de contracte ai operatorului vor avea

responsabilitatea/obligativitatea inserării în contractele încheiate și gestionate de către aceștia a clauzelor specifice cu privire la protecția datelor cu caracter personal a GDPR și/sau cu privire la respectarea condițiilor generale, tehnice și de participare. Elementele de conținut ale Notelor de Informare, ale clauzelor contractuale și ale celorlalte instrumente de informare referitoare la protecția datelor personale sunt stabilite/actualizate, pe baza legislației specifice, de către Responsabilul cu protecția datelor - DPO din cadrul instituției și aprobate în prealabil de către directorul general.

6.3. Dreptul de acces al persoanei vizate

6.3.1. Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privește și, în caz afirmativ, accesul la datele respective și la următoarele informații:

a) scopurile prelucrării;

b) categoriile de date cu caracter personal vizate;

c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;

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

e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la menționată sau a dreptului de a se opune prelucrării;

f) dreptul de a depune o plângere în fata unei autorități de supraveghere;

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

h) dacă este cazul, existența unui proces decizional automatizat incluzând crearea de profiluri, precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

6.3.2. În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, menționată are dreptul să fie informată cu privire la garanțiile adecvate, prevăzute de lege referitoare la transfer.

6.3.3. Operatorul furnizează o copie a datelor cu caracter personal care face obiectul prelucrării gratuit, pentru prima oară, persoanei vizate. Pentru orice alte

copii solicitate de persoană vizată, operatorul poate percepe o taxa rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care menționată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

6.3.4. Dreptul de a obține o copie, menționată anterior, nu aduce atingere drepturilor și libertăților altora, astfel că persoanele vizate au drepturi fundamentale dar nu absolute.

6.4. Dreptul la rectificare.

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, menționată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

6.5. Dreptul la ștergerea datelor ("dreptul de a fi uitat")

6.5.1. Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplica unul dintre următoarele motive:

a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrarea;

c) Persoana vizată se opune prelucrării și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării, în cazul prelucrării în scop de marketing direct;

d) datele cu caracter personal au fost prelucrate ilegal;

e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se afla operatorul;

f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate în legislația specifică.

6.5.2. Alineatele anterioare nu se aplică în măsura în care prelucrarea este necesară:

a) pentru exercitarea dreptului la libera exprimare și la informare;

b) pentru respectarea unei obligații 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 autorități oficiale cu care este investit operatorul;
c) din motive de interes public în domeniul sănătății publice;
d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în măsura în care dreptul la ștergere este susceptibilă să facă imposibil sau sa afecteze în mod grav realizarea obiectivelor prelucrării respective; sau
e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

6.6. Dreptul la restricționarea prelucrării

6.6.1. Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri:
a) Persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată le solicit pentru constatarea, exercitarea sau apărarea unui drept în instanță; sau
d) 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.

6.6.2. În cazul în care prelucrarea a fost restricționată conform prevederilor anterioare, astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

6.6.3. O persoana vizată care a obținut restricționarea prelucrării este informată de către operator înainte de ridicarea restricției de prelucrare.

6.7. Obligația de notificare cu privire la rectificarea, ștergerea datelor cu caracter personal sau restricționarea prelucrării.

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau

restricționare a prelucrării, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

6.8. Dreptul la portabilitatea datelor

6.8.1. Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și 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:

a) prelucrarea se bazează pe Consimțământ sau pe un contract; și

b) prelucrarea este efectuată prin mijloace automate.

6.8.2. 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.

6.8.3. Exercitarea dreptului la portabilitatea datelor nu aduce atingere dreptului la ștergerea datelor. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul.

6.8.4. Dreptul la portabilitatea datelor nu aduce atingere drepturilor și libertăților altora.

6.9. Dreptul la opoziție și procesul decizional individual automatizat

6.9.1. Dreptul la opoziție

6.9.1.1. În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării datelor cu caracter personal care o privesc, inclusiv creării de profiluri, dacă este cazul. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

6.9.1.2. În ipoteza în care 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 legat 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 opoziție menționat este adusă în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

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

6.9.2. Procesul decizional automatizat, crearea de profiluri (unde este cazul)

6.9.2.1. Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automat, 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:**

a) este necesar pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;

b) este autorizat prin dreptul Uniunii sau dreptul intern care se aplica operatorului și care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau

c) are la baza consimțământul explicit al persoanei vizate.

6.9.2.3. În cazurile în care decizia este necesar pentru încheierea sau executarea unui contract între persoana vizată și un operator de date sau are la bază consimțământul explicit al persoanei vizate, operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

6.9.2.4. Deciziile menționate anterior nu au la baza categoriile speciale de date cu caracter personal, cu excepțiile prevăzute de lege (ex: Persoana vizată și-a dat consimțământul explicit) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

CAP. 7 RESTRICȚII

Prin legislația specifică care se aplică operatorului de date (sau persoanei împuternicite de operator) se poate restricționa domeniul de aplicare al obligațiilor și al drepturilor prevăzute în actuala legislație în măsura în care dispozițiile acesteia corespund drepturilor și obligațiilor menționate anterior, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

a) securitatea națională;

b) apărarea;

c) securitatea publică;

d) prevenirea, investigarea, depistarea sau urmărirea penală sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;

e) alte obiective importante de interes publică general ale Uniunii sau ale unui stat membru, în special un interes economică sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;

f) protejarea independenței judiciare și a procedurilor judiciare;

g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;

h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale;

i) protecția persoanei vizate sau a drepturilor și libertăților altora;

j) punerea în aplicare a pretențiilor de drept civil.

CAP. 8 OPERATORUL (ARSVOM Constanța) ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

8.1. Responsabilitatea Operatorului

8.1.1. Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, costurile implementării precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, ARSVOM pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în

conformitate cu prevederile GDPR. De asemenea, măsurile tehnice și organizatorice adoptate sunt necesare protejării datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. Respectivele măsuri se revizuiesc și se actualizează dacă este necesar. Pentru îndeplinirea cerințelor legale specifice protecției datelor cu caracter personal operatorul implementează măsuri tehnice și organizatorice orientate pe diferite direcții de acțiune, precum: alocarea/stabilirea responsabilităților pentru Responsabilul de protecția datelor, alocarea/responsabilităților pentru angajații care prelucrează date cu caracter personal, adaptarea activităților organizației la cerințele legale specifice, elaborarea/implementarea unor politici/proceduri IT adecvate pentru securitatea datelor personale, instruirea personalului, monitorizarea conformității, etc.

8.1.2. Masurile tehnice și organizatorice includ punerea în aplicare a unor politici/proceduri IT adecvate de protecție/securitate a datelor cu caracter personal.

8.1.3. Suplimentar măsurilor anterior precizate, în vederea asigurării unui nivel adecvat de protecție/securitate a datelor cu caracter personal se adoptă măsuri organizatorice și reguli, precum:

- Instalarea de sisteme de supraveghere video;
- Monitorizarea și intervenția în caz de alarmă, asigurat în permanență de personal specializat/autorizat din cadrul SC SECURITAS SRL;
- Toate documentele care conțin date cu caracter personal se înregistrează și urmează regulile de păstrare, procesare, multiplicare, transport, distrugere și arhivare stabilite prin Legea Arhivelor Naționale, legislația internă și internațională privind protecția datelor cu caracter personal și prin proceduri interne;
- Personalul este instruit în legătură cu aspectele legale privind protecția datelor personale și cu privire la riscurile pe care le comportă prelucrarea datelor personale;
- Directorul general, stabilește fiecărui utilizator tipurile de acces și operațiunile permise acestuia, strict necesare pentru îndeplinirea atribuțiilor de serviciu;
- Utilizatorul/angajatul operatorului poate prelucra date cu caracter personal doar pe perioada în care ocupă funcția respectivă.

Extinderea sau restrângerea atribuțiilor de prelucrare a datelor cu caracter personal se dispune de operator atunci când utilizatorul/angajatul se află în una dintre următoarele situații:

a) la modificarea raporturilor de muncă;

b) la modificarea atribuțiilor privind prelucrarea datelor cu caracter personal, prevăzute în fișa postului.

Dreptul de acces al utilizatorului la sistemul de evidență a datelor cu caracter personal se suspendă pe perioada în care acesta se află în una dintre următoarele situații:

a) se află în concediu fără plată, concediu medical, concediu pentru creșterea sau îngrijirea copilului minor, pentru o perioada mai mare de 3 luni;

b) se afla în concediu de maternitate sau concediu pentru incapacitate temporară de muncă;

c) urmează un curs sau o specializare cu scoatere din program, pentru o perioada mai mare de 3 luni;

d) pe perioada cercetării disciplinare, în situația în care față de utilizator se efectuează cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispozițiilor legale;

e) alte cazuri prevăzute de lege.

- Cu ocazia proiectării, întreținerii, actualizării aplicațiilor de gestiune a bazelor de date, **se interzice accesul providerilor/programatorilor/personalului de întreținere a sistemelor informatice la orice fel de date cu caracter personal deținute/create/accesate de personalul din structura respectivă a instituției.**

În aceste situații, se pun la dispoziția provider-ilor/programatorilor/personalului de întreținere numai date anonime/pseudonimizate;

- Pentru cazuri excepționale, numai pe durata intervenției la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezența unui utilizator desemnat de operator. În această situație, răspunderea pentru păstrarea confidențialității datelor aparține persoanelor în cauză, sens în care trebuie să semneze un "Angajament de confidențialitate";

- Operațiunile de colectare, introducere, modificare și actualizare a datelor cu caracter personal se realizează numai de personalul anume desemnat de către conducătorul operatorului, conform actelor de reglementare internă;

- ARSVOM dispune de măsurile tehnice necesare care să permită identificarea utilizatorului care a introdus, modificat sau actualizat datele cu caracter personal;

- Bazele de date cu caracter personal deținute/create și programele folosite de operatori/utilizatori **vor fi salvate**, prin copii de siguranță, la un interval de timp stabilit de conducerea organizației, în funcție de mărimea, volumul și importanța acestor baze de date;

- **Directorul general al ARSVOM desemnează/stabilește utilizatori care să aibă atribuții de serviciu și executarea copiilor de siguranță ale bazelor de date deținute/create și ale programelor folosite;**
- Accesul în încăperile în care se află documente ce conțin date cu caracter personal și/sau terminale de acces/echipamente care prelucrează date cu caracter personal este limitat la utilizatorii stabiliți de conducătorul operatorului și numai pentru îndeplinirea atribuțiilor de serviciu (acces restricționat/controlat);
- Documentele, terminalele de acces/echipamentele care conțin date cu caracter personal vor fi ținute/păstrate în fișete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare și/sau în încăperi/spații care se pot încuia.

Documentele care conțin date cu caracter personal speciale, folosite pentru realizarea anumitor operațiuni se vor preda persoanelor abilitate sau se vor depozita în fișete metalice prevăzute cu încuietori, asigurându-se măsuri suplimentare adecvate de protecție, care pot fi ulterior demonstrate la solicitarea autorităților autorizate în materie;

- Aplicațiile informatice care gestionează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acționează asupra datelor afișate pe ecran pe o perioadă de timp stabilit, prin proceduri de lucru/diagrame flux, în funcție de operațiunile care trebuie executate.
- Terminalele de acces trebuie să aibă setate funcția de închidere automat a ecranului și funcția „lock screen - screen saver" la o temporizare prestabilit, prin proceduri de lucru/diagrame flux, iar dacă acest lucru nu este posibil din punct de vedere tehnic, dup trecerea intervalului de timp stabilit, datele afișate trebuie ascunse sau sesiunea de lucru va fi închis. Terminalele de acces folosite în relația cu publicul se poziționează astfel încât datele afișate să fie vizualizate numai de către utilizatori;
- Accesul utilizatorilor/angajaților la datele cu caracter personal care se regăsesc în rețeaua acesteia, la serverele și stațiile de lucru, se va efectua controlat/restricționat pe bază de user și parolă, setate exclusiv de serviciile externalizate de IT, utilizatorii având drept de acces limitat, conform procedurilor interne (ex: read only, write, execute, modify, full control etc.);
- Nu este permisă scoaterea din organizație a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD etc.) care conțin date cu caracter personal, decât cu aprobarea prealabilă a conducerii operatorului;

- Se interzice utilizarea serviciului de e-mail în orice mod ce ar avea drept consecință transmiterea, distribuirea și livrarea de mesaje nesolicitate de poșta electronică în volum mare sau de mesaje comerciale nesolicitate ("Spam"). Prin spam înțelegem trimiterea de mesaje (comerciale) nesolicitate în urma cărora se primesc plângeri din partea celor care le primesc, folosirea sau distribuirea de liste de emailuri care aparțin unor persoane care nu și-au exprimat consimțământul anterior.
- Utilizatorii/angajații nu vor deschide email-uri de tip SPAM/Malware și/sau orice alte comunicații electronice care nu au legătură cu activitatea desfășurată în calitate de angajat. Totodată, angajații nu au voie să găzduiască sau să permită găzduirea site-urilor sau informațiilor a căror publicitate este făcuta prin emailuri SPAM. Nerespectarea politicii anti-spam constituie abatere disciplinară și se sancționează.
- Utilizatorii/angajații care prelucrează date cu caracter personal sunt obligați să își închidă sesiunea de lucru, să blocheze ecranul terminalelor de acces atunci când părăsesc locul de muncă, iar la sfârșitul programului de lucru să închidă terminalele de acces;
- Este interzis angajaților ARSVOM să transmită date cu caracter personal din cadrul operatorului de date cu caracter personal către alți beneficiari abilitați pe adresele de email personale yahoo.com sau gmail.com.
- Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizați, și, acolo unde echipamentul de imprimare permite, aceasta operațiune se va realiza controlat, pe bază de parolă. Prezentele reguli și măsuri se completează cu prevederile politicilor și procedurilor elaborate de ARSVOM, reglementări interne necesare pentru asigurarea adecvată a protecției/securității datelor cu caracter personal.

8.1.4. Aderarea la coduri de conduită aprobate sau la un mecanism de certificare aprobat, menționată de legislația specifică, poate fi utilizat ca element care să demonstreze respectarea obligațiilor de către operator.

8.2. Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

8.2.1. Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare (mijloace manuale și/sau automate - ex: sisteme

de operare, servere, stații de lucru, soluții de securitate, de backup, de stocare, programe/soluții software/aplicații IT achiziționate sau dezvoltate in-house etc.), cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate (ex: pseudonimizarea), care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentelor norme interne în domeniul protecției datelor personale și a proteja drepturile persoanelor vizate.

8.2.2. Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specifică al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția unei persoane, de un număr nelimitat de persoane.

8.2.3. Un mecanism de certificare aprobat menționat de legislația specifică poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute anterior.

8.3. Persoana împuternicită de Operator

8.3.1. Dacă prelucrarea urmează să fie realizată în numele operatorului, acesta contactează exclusiv persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.

8.3.2. Persoana împuternicită de operator nu recrutează o alta persoană împuternicită fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații 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 obiecții față de aceste modificări.

8.3.3. **Prelucrarea de către o persoana 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 și care stabilește obiectul și durata prelucrării,

natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului.
Respectivul contract sau act juridic prevede în special ca persoana împuternicită de operator:
a) prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică. În acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;
b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;
c) adoptă toate măsurile tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate a datelor personale corespunzător, în conformitate cu cerințele legislației specifice;
d) respectă condițiile menționate privind recrutarea unei alte persoane împuternicite de operator;
e) ținând seama de natura prelucrării, oferă asistență operatorului prin masuri tehnice și organizatorice adecvate, în măsură în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute de legislația specifică;
f) ajută operatorul să asigure respectarea obligațiilor privind securitatea prelucrării, notificarea Autorității Naționale de Supraveghere/Informarea persoanei vizate în cazul încălcării securității datelor, evaluarea impactului asupra protecției datelor, consultarea prealabilă, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;
g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal, sau legea prevede altfel;
h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea

auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

i) persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor.

8.3.4. în cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridică încheiat între operator și 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 garanții suficiente pentru punerea în aplicare a unor masuri tehnice și organizatorice adecvate.

În cazul în care aceasta a doua persoană împuternicită nu își respecta obligațiile privind protecția datelor, persoana împuternicită inițial rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor persoanei împuternicite subsecvent.

8.3.5. Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, sau la un mecanism de certificare aprobat, menționate de legislația specifică, poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate anterior.

8.3.6. Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic încheiat între persoana împuternicită de operator și o altă persoană împuternicită, se poate baza, integral sau parțial, 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 legislației specifice;

8.3.7. Contractul sau celălalt act juridic menționat anterior se formulează în scris, inclusiv în format electronic.

8.3.8. În cazul în care o persoană împuternicită de operator încalcă Regulamentul UE nr. 679/2016, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

8.3.9. În situațiile în care sunt prelucrate date cu caracter personal în numele operatorului de către persoane împuternicite (procesatori de date - ex: instituții de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariați, companii de curierat etc.) derulatorii de contract ai ARSVOM vor avea responsabilitatea/obligativitatea de a încheia cu fiecare dintre aceste persoane împuternicite Acorduri de prelucrare a datelor cu caracter personal, care vor avea în conținut elementele prevăzute în prezentul Regulament și legislația specifică, stabilite în prealabil de Responsabilul cu protecția datelor și aprobate de directorul general.

8.4. Desfășurarea activității de prelucrare sub autoritatea Operatorului sau a persoanei împuternicite de operator.

Persoana împuternicită de operator și orice persoană care acționează 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 excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru.

8.5. Evidențele activităților de prelucrare

8.5.1. Potrivit prevederilor GDPR, organizațiile care au mai puțin de 250 de angajați au obligația de a ține evidența prelucrării de date cu caracter personal, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum sunt prevăzute în legislația specifică. ANSPDCP recomandă ca toate instituțiile și autoritățile de pe teritoriul României vor avea desemnat/nominalizat un responsabil cu protectia datelor cu caracter personal – DPO. Desemnarea DPO va fi notificată on line ANSPDCP.

8.5.2. În situația în care, operatorul va intra sub incidența prevederilor anterior menționate, acesta păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor.

Respectiva evidență cuprinde următoarele informații:

a) numele și datele de contact ale operatorului și, dup caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

b) scopurile prelucrării;

c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și documentația care dovedește existenta unor garanții adecvate;
f) acolo unde este posibil, termenele-limita preconizate pentru ștergerea diferitelor categorii de date;
g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate adecvate;
8.5.3. Fiecare operator și, dup caz, persoană împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:
a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează aceasta persoană (aceste persoane), precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, dup caz;
b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
c) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și documentația care dovedește existența unor garanții adecvate;
d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate adecvate.
8.5.4. Evidențele menționate anterior se formulează în scris, inclusiv în format electronic.
8.5.5. Operatorul sau persoana împuternicită de acesta, precum și, sau al persoanei împuternicite de operator pun evidențele la dispoziția autorității de supraveghere, la cererea acesteia, cu notificarea prealabilă a Operatorului;

8.6. Cooperarea cu Autoritatea de supraveghere.

Instituția, în calitate de operator și persoana împuternicită de operator și, dup caz, reprezentantul acestora cooperează, la cerere, cu Autoritatea de Supraveghere în îndeplinirea sarcinilor lor, în conformitate cu prevederile GDPR.

8.7. Masuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal

8.7.1. Aspecte generale privind securitatea prelucrării

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

a) pseudonimizarea și criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă ale sistemelor și serviciilor de prelucrare;

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

d) un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

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

8.7.1.3. **Aderarea la un cod de conduită aprobată sau la un mecanism de certificare aprobat, menționate în legislația specifică, poate fi utilizat ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute anterior.**

8.7.1.4. Operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

8.7.2. Aspecte specifice privind securitatea prelucrării.

La nivelul operatorului de date cu caracter personal, măsurile tehnice și organizatorice menționate în legislația specifică, necesare asigurării unui nivel adecvat de protecție sunt implementate prin:

- Identificarea, ca urmare a unor activități de audit de specialitate a unor soluții tehnice IT adecvate, ținând cont de costurile implementării, natura, domeniul de aplicare, contextul, scopurile prelucrării și riscurile aferente, soluții care să acopere aspecte prevăzute de legislația specifică, precum:
- Cerințe de securitate de bază: testarea securității sistemului, întărirea sistemului, codificarea securizată, protecția împotriva programelor malware;
- Politica privind parolele: autentificarea utilizatorului, autentificare cu doi factori;
- Managementul schimbării: separarea mediilor de testare, testarea schimbărilor, accesul dezvoltatorilor;
- Controlul accesului: controlul accesului bazat pe roluri, securitatea conturilor de utilizator, revizuirea privilegiilor, Audit logs, conturi neutilizate, privilegiile utilizatorilor tehnici, consola de securitate, informații despre utilizatori;
- Managementul evenimentelor: log format documentation, log information, log protection and monitoring, log format, evenimente auditate;
- Securitatea datelor: criptarea datelor, securitatea datelor în ciclul lor de viață;
- Back-up: back-up copies, programul de back-up, back-up security,verificarea back-up-urilor, viabilitatea back-upurilor;
- Pseudominimizarea, minimizarea, integritatea datelor personale (computere, servere, terminale de acces, imprimarea datelor), disponibilitatea datelor, ștergerea și portabilitatea datelor, evidențele activităților de prelucrare;
- Elaborarea/implementarea/monitorizarea permanent de către DPO a unor politici/proceduri specifice de protecție/securitate a datelor cu caracter personal concretizate.
- Folosirea de Sisteme de operare certificate, cu soluții antivirus complete;

8.7.3. **Cartografierea datelor cu caracter personal**

În vederea cartografierii datelor cu carter personal din cadrul ARSVOM se va efectua anual un audit/inventariere sau analiză a măsurilor organizatorice și tehnice luate de operator în vederea conformității cu prevederile GDPR, care va viza nivelul actual al implementării Regulamentului UE, natura activităților desfășurate, structura organizatorică, datele prelucrate, categoriile vizate, temeiul legal al prelucrării, scopul și mijloacele prelucrării, măsurile de securitate care vizează protecția datelor personale, etc.

Auditul/inventarierea end to end în domeniul GDPR pot fi externalizate, putând fi efectuat de firme de consultanță specializate și acreditate în domeniu sau poate fi efectuată o analiză a măsurilor menționate anterior, de către o echipă de

implementare nominalizată de conducerea operatorului, sub directa îndrumare a DPO –ului, care se va ocupa și de instruirea și pregătirea personalului care accesează autorizat date cu caracter personal.

Raportul final al auditului/inventarierii/analizei datelor cu caracter personal din cadrul organizației se prezintă directorului general și reprezentanților structurilor funcționale (în părțile care îi privesc) și se păstrează în gestiunea responsabilului cu protectia datelor personale – DPO și va fi pus la dispoziția/solicitarea ANSPDCP și instituțiilor/autorităților abilitate de lege. Raportul se elaborează cel puțin anual sau ori de câte ori este nevoie, în funcție de modificarea sau actualizarea măsurilor organizatorice și tehnice din domeniul protecției datelor cu caracter personal.

Până la această dată, în cadrul ARSVOM Constanța au fost efectuate două activități de acest gen, respectiv un audit și o inventariere a datelor cu caracter personal, iar rapoartele finale se află în gestiunea DPO.

Întreaga activitate de prelucrare a datelor cu caracter personal din cadrul instituției va fi menționată, la zi, începând cu data de 25 mai 2018 (termen alocat de Parlamentul UE și Comisia UE), în Registrul de evidență a prelucrării datelor cu caracter personal care este elaborat în format fizic/letric cât și în format electronic și se află în gestiunea DPO. În ipoteza în care va fi necesară elaborarea unei DPIA în cadru organizației (când se identifică riscuri ridicate la adresa persoanelor vizate) se va consulta prevederile art. 1 din Decizia nr. 174/2018 emisă de ANSPDCP care stabilește condițiile elaborării acesteia. Dacă va fi cazul, elaborarea unei DPIA, se va efectua anterior prelucrării datelor cu caracter personal și se va consulta ANSPDCP.

8.7.4. **Reguli privind gestionarea de baze de date din punct de vedere RGPD**

Se interzice realizarea de comunicări comerciale în scop de marketing direct (ex. Newsletter) către persoanele vizate care se regăsesc la nivelul ARSVOM Constanța în diverse evidențe, baze de date, aplicații IT, **utilizând adrese de email de tipul nume.prenume@gmail.com, nume.prenume@yahoo.com sau alte adrese care conțin date cu caracter personal ori numere de telefon personale care se regăsesc în aceste evidente, în lipsa consimțământului expres, neechivoc, liber exprimat anterior dar și informat al persoanelor vizate și evidențiat distinct**. Comunicările comerciale în scop de marketing direct se vor putea realiza utilizând adrese de email de tipul nume.prenume@gmail.com, nume.prenume@yahoo.com sau alte adrese care conțin date cu caracter personal

ori numere de telefon personale (SMC) care se regăsesc în evidențele, aplicațiile, bazele de date utilizate la nivelul operatorului, numai în măsura în care:
- avem consimțământul expres neechivoc, liber exprimat anterior dar și informat al persoanelor vizate, și
- evidențele, aplicațiile, bazele de date utilizate la nivelul operatorului vor fi adaptate în sensul evidențierii în mod distinct a consimțământului persoanelor vizate, pentru controlul efectiv al acestui proces din punct de vedereal prevederilor RGPD, indiferent de modalitatea de obținere a acestuia. Datele trebuie să fie adecvate, relevante și strict limitate la ce este absolut necesar pentru scopurile în care sunt necesare pentru prelucrarea asumată. Fiecare conducător al locului de muncă, cu suportul serviciului IT externalizat, va identifica și inventaria, menține în rețeaua organizației, inclusiv în stațiile de lucru individuale, doar bazele de date care sunt utile în mod efectiv pentru desfășurarea activității curente a organizației, precum și eliminarea acelora care nu mai au relevanță și/sau a expirat termenul de arhivare, în condițiile legii.

Lista bazelor de date gestionate de fiecare birou (respectiv inventarierea resurselor informatice) va conține minim: denumirea bazei de date, locația de păstrare, responsabilul de gestionare (elaborare, modificare), persoanele cu drepturi de acces, perioada de păstrare, frecventa back-ul etc.

Fiecare conducător al locului de muncă care gestionează baze de date în rețeaua organizației și pe stațiile de lucru individuale, cu suportul serviciului IT externalizat, vor stabili reguli de acces controlat/restricționat (ex. Read only, write, execute, modify etc.) pentru utilizatorii acestor baze de date, revizuite în sensul celor de mai sus, pe bază de user și parola, la niveluri de acces (dacă este posibil). Bazele de date trebuie grupate în folder dedicate, atât a celor utilizate pentru activități comerciale/relații de afaceri cât și a bazei de date utilizată în scop de marketing direct pentru persoane fizice. În rețeaua organizației conducătorii locurilor de muncă, cu suportul serviciului IT externalizat, se vor menține doar documentele care conțin date cu caracter personal care sunt relevante, utile în mod efectiv pentru desfășurarea activității curente și eliminarea tuturor acelora care nu au relevanță, potrivit Regulamentului UE. Serviciul IT externalizat va realiza/asigura în permanență, conform programelor aprobate, salvarea bazelor de date cu caracter personal precum și a altor documente ce conțin date cu caracter personal în rețeaua organizației, prin copii de siguranță (backup), la intervalul stabilit.

8.8. Notificarea Autorității de Supraveghere în cazul încălcării securității datelor cu caracter personal

8.8.1. În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul, prin Responsabilul de protecția datelor, notifică acest lucru Autorității Naționale de Supraveghere, fără întârzieri nejustificate în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta. În cazul în care notificarea Autorității de Supraveghere nu are loc în termen de 72 de ore, aceasta va fi însoțită de o explicație motivată a întârzierii în cauză, potrivit legii.

8.8.2. Persoana împuternicită de operator (dacă aceasta există) înștiințează operatorul (informează Responsabilul cu protecția datelor al operatorului) fără întârzieri nejustificate după ce ia la cunoștință de o încălcare a securității datelor cu caracter personal.

8.8.3. Notificarea adresată Autorității cu privire la încălcarea securității datelor personale, conține cel puțin, următoarele elemente:

a) descrierea caracterului încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

b) numele și datele de contact ale DPO sau un alt punct de contact de unde se pot obține mai multe informații;

c) descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;

d) descrierea măsurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

8.8.4. Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

8.8.5. Operatorul, prin DPO, păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Aceasta documentație permite Autorității de Supraveghere să verifice conformitatea cu legislația specifică. ANSPDCP poate efectua controlul la operator sau poate solicita ca directorul general și DPO – ul să se prezinte la sediul autorității, în București.

8.8.6. Angajații au obligația de a informa de îndată șeful ierarhic, Responsabilul cu protecția datelor și conducătorul instituției în cazul identificării unei situații de încălcare a securității datelor cu caracter personal. Responsabilul cu protecția datelor analizează informațiile comunicate, iar dacă este cazul, solicită entităților funcționale date și informații suplimentare. În cazul în care situația de încălcare a securității datelor cu caracter personal este fundamentată rezonabil, Responsabilul cu protecția datelor întocmește Notificarea și solicită avizul conducerii pentru a fi transmisă la Autoritatea de Supraveghere. Notificarea se transmite către Autoritatea de Supraveghere în format electronic, conform cerințelor stabilite de ANSPDCP.

8.9. Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

8.9.1. În cazul în care încălcarea securității datelor cu caracter personal este susceptibil să genereze un riscă ridicat pentru drepturile și libertățile persoanelor fizice, operatorul, prin Responsabilul de protecția datelor, informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

8.9.2. În Informarea transmisă persoanei vizate, prevăzută anterior, se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin următoarele informații și măsuri:

- numele și datele de contact ale DPO sau un alt punct de contact de unde se pot obține mai multe informații;
- descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- descrierea măsurilor luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, dup caz, măsurile pentru atenuarea eventualelor sale efecte negative.

8.9.3. Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiții sunt îndeplinite:

a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată sa le acceseze, cum ar fi criptarea;

b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai sunt susceptibil să se materializeze;
c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

CAP. 9 EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR ȘI CONSULTAREA PREALABILĂ (DACĂ ESTE CAZUL)

9.1. Evaluarea impactului asupra protecției datelor

9.1.1. Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul, prin Responsabilul de protecția datelor, efectuează, *înaintea prelucrării*, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.
9.1.2. Responsabilul cu protecția datelor elaborează, la solicitarea operatorului, în colaborare cu angajații acestuia, evaluarea impactului asupra unui anumit tip de prelucrare de date cu caracter personal - DPIA.
9.1.3. Evaluarea impactului asupra protecției datelor se impune mai ales în cazul:
a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automat, inclusiv crearea de profiluri și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
b) prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale și infracțiuni menționate în legislația specifică; sau
c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.
9.1.4. Autoritatea de supraveghere a întocmit și publicat o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, respectiv Decizia nr. 174/2018.

9.1.5. **Autoritatea de supraveghere poate, de asemenea, a stabilit și a pus la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor.**

9.1.6. Evaluarea conține cel puțin:

a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, dup caz, interesul legitim urmărit de operator;

b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate; și

d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

9.1.7. 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 operator sau persoana împuternicită respectivă (dacă este cazul) a codului de conduită aprobat, menționat în legislația specifică, în special, în vederea unei evaluări a impactului asupra protecției datelor.

9.1.8. Operatorul, prin Responsabilul de protecția datelor, solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

9.1.9. Atunci când prelucrarea are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, prevederile anterioare nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

9.1.10. Acolo unde este necesar, operatorul, prin Responsabilul de protecția datelor, efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

9.2. Consultarea prealabilă a Autorității de Supraveghere

9.2.1. **Operatorul, prin Responsabilul de protecția datelor, consultă autoritatea de supraveghere înainte de prelucrare atunci când evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.**

9.2.2. Atunci când consultă autoritatea de supraveghere, operatorul, prin Responsabilul de protecția datelor, îi furnizează acesteia:

a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare;

b) scopurile și mijloacele prelucrării preconizate;

c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezentul regulament;

d) datele de contact ale DPO;

e) evaluarea impactului asupra protecției datelor; și

f) orice alte informații solicitate de autoritatea de supraveghere.

9.2.3. Dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină 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 protecția socială și sănătatea publică.

CAP.10 RESPONSABILUL DE PROTECȚIA DATELOR (DPO)

10.1. Alocarea responsabilităților/sarcinilor aferente DPO

La nivelul operatorului sarcinile/responsabilitatea DPO sunt atribuite printr-o Decizie a directorului general al ARSVOM Constanța. **Responsabilitățile alocate/stabilite prin decizie, fără a se limita la acestea, sunt cele prevăzute de art. 39 din GDPR, care sunt următoarele**:

- participă la procesul de tranziție către conformitatea cu Regulamentul privind Protecția Datelor cu Caracter Personal (RGPD);
- informează și consiliază conducerea operatorului, sau persoana împuternicită de operator, precum și angajații organizației care se ocupă de prelucrarea datelor cu caracter personal privind obligațiile (naționale și europene) referitoare la prelucrarea datelor cu caracter personal, precum și cu privire la orice aspect legat de protecția datelor cu caracter personal;
- acordă consiliere și se implica în mod direct în efectuarea evaluărilor de impact asupra protecției datelor, monitorizează funcționarea acestora, inclusiv privind consultarea prealabilă a Autorității de Supraveghere, dacă este cazul;
- monitorizează respectarea prevederilor legale (naționale și europene) și ale reglementărilor interne referitoare la protecția datelor personale la nivelul operatorului;
- monitorizează alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditul/inventarierea aferentă;
- participă la instruirea angajaților implicai în operațiunile de prelucrare a datelor personale;
- participă la activitatea de actualizare a evidenței operațiunilor de prelucrare a datelor personale și monitorizează corectitudinea acesteia;
- redactează și negociază clauze contractuale privind prelucrarea datelor cu caracter personal;
- monitorizează, utilizând metoda eșantionului, modul în care persoanele ale căror date cu caracter personal se procesează, au fost informate de drepturile pe care le au;
- asigură asistență privind gestionarea prelucrării de date cu caracter personal și pentru menținerea registrului de prelucrări a datelor personale precum și registrul privind incidentele de securitate și efectuează notificările privind încălcarea securității datelor personale;
- cooperează cu autoritatea de supraveghere (ANSPDCP) și acționează ca punct de contact (interfața operatorului) în relația cu autoritatea de supraveghere, persoanele vizate, precum și în cadrul instituției în legătură cu aspecte de prelucrare;

10.2. Responsabilitățile operatorului față de DPO

- conducerea entității funcționale se va asigura că DPO este implicat corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal și

va acorda întregul sprijin DPO, asigurându-i resursele necesare pentru executarea atribuțiilor sale, precum și pentru accesarea datelor cu caracter personal și a operațiunilor de prelucrare și pentru menținerea cunoștințelor sale de specialitate;
- **DPO nu va primi niciun fel de instrucțiuni în ceea ce privește îndeplinirea atribuțiilor sale în legătură cu RGPD de la conducerea operatorului.**
- persoanele vizate pot contacta și solicita asistență de specialitate din partea DPO cu privire la toate aspectele legate de prelucrarea datelor și de exercitarea drepturilor lor;
- conducerea operatorului și DPO se vor asigura ca niciuna din sarcinile celui din urmă nu generează un conflict de interese.
- Directorul general al ARSVOM va asigura pentru DPO accesul pe log-urile sistemelor de prelucrare automatizat a datelor.

CAP.11 TRANSFERURILE DE DATE CU CARACTER PERSONAL CATRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE(DACĂ ESTE CAZUL)

11.1. Orice decizie de a transfera date în afara spațiului UE și al Zonei Economice-Europene va fi supus, anterior transferului și în timp util, analizei DPO. Transferurile de date în afara spațiului UE și al Zonei Economice-Europene se pot face:
- În temeiul unei decizii a Comisiei Europene privind caracterul adecvat al nivelului de protecție;
- În baza unor garanții adecvate oferite de operator sau persoana împuternicită;
Garanțiile adecvate pot fi furnizate prin:
a) un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
b) reguli corporatiste obligatorii;
c) clauze standard de protecție a datelor adoptate de Comisia Europeană;
d) clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisia Europeană;

e) un cod de conduită aprobat, însoțit de un angajament obligatoriu și executoriu din partea ARSVOM sau a persoanei împuternicite (dacă este cazul) din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) un mecanism de certificare aprobat, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

11.2. **Sub rezerva autorizării din partea Autorității de Supraveghere, garanțiile adecvate pot fi furnizate, în special, prin**:

a) clauze contractuale, sau

b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

11.3. În absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, un transfer de date către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:

a) Persoana vizată și-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;

b) transferul este necesar pentru executarea unui contract între persoana vizată și ARSVOM sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

c) transferul este necesar pentru încheierea sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o alta persoană fizică sau juridică;

d) transferul este necesar din considerente importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridica de a-și exprima acordul;

g) transferul se realizează dintr-un registru care, potrivit dreptului UE sau al dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat de public în general, sau de orice persoană care poate face dovada unui interes legitim.

11.4. În lipsa unei decizii a Comisiei, a unor garanții adecvate dar și în lipsa condițiilor precizate anterior, un transfer către o țară terță sau o organizație internațională 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 asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și
- operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer.

CAP.12 CĂI DE ATAC, RĂSPUNDERI, MĂSURI ȘI SANCȚIUNI SPECIFICE

12.1. Dreptul de a depune o plângere la o autoritate de supraveghere

12.1.1.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 își are reședința obișnuită, 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 încălcă Regulamentul UE nr. 679/2016.

12.1.2. **Autoritatea de supraveghere la care s-a depus plângerea informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul legislației specifice.**

12.2. Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere

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

12.2.2. Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară

eficientă în cazul în care autoritatea de supraveghere competentă nu tratează o plângere sau nu informează persoana vizată în termenul prevăzut de lege cu privire la progresele sau la soluționarea plângerii depuse.

12.2.3. Acțiunile introduse împotriva unei autorități de supraveghere sunt aduse în fața instanțelor din statul membru în care este stabilit autoritatea de supraveghere.

12.2.4. În cazul în care acțiunile sunt introduse împotriva unei decizii a unei autorități de supraveghere care a fost precedată de un aviz sau o decizie a Comitetului european pentru protecția datelor în cadrul mecanismului pentru asigurarea coerenței, autoritatea de supraveghere transmite curții avizul respectiv sau decizia respectivă.

12.3. Dreptul la o cale de atacă eficientă împotriva unui operator sau a unei persoane împuternicite de operator

12.3.1. 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.

12.3.2. Acțiunile introduse împotriva unui operator sau unei persoane împuternicite de operator (dacă este cazul) sunt prezentate în fața instanțelor din statul membru unde operatorul sau persoana împuternicită de operator își are un sediu.

Alternativ, o astfel de acțiune poate fi prezentată în fața instanțelor din statul membru în care persoana vizată își are reședința obișnuită, cu excepția cazului în care operatorul sau persoana împuternicită de operator este o autoritate publică a unui stat membru ce acționează în exercitarea competentelor sale publice.

12.4. Dreptul la despăgubiri și răspunderea operatorului sau a persoanei împuternicite de operator (dacă este cazul)

12.4.1. Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a legislației specifice are dreptul să obțin despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

12.4.2. Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prevederile legislației specifice. Persoana împuternicită de operator (dacă este cazul) este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din legislația specifică care revin în mod specifică persoanelor

împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale/contractuale ale operatorului.

12.4.3. Operatorul sau persoana împuternicită de operator este exonerat de răspundere dacă dovedește că nu este răspunzător (răspunzătoare) în niciun fel pentru evenimentul care a cauzat prejudiciul.

12.5. Condiții generale pentru impunerea amenzilor administrative

12.5.1. Autoritatea de supraveghere asigură faptul că impunerea unor amenzi administrative pentru încălcările prevederilor legislației specifice este, în fiecare caz, **eficace, proporțională și disuasivă**.

12.5.2. În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate de legislația specific.

Autoritatea de Supraveghere poate:

- să emită avertizări;

- să emită mustrări;

- să dea dispoziții;

- să oblige operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor;

- să limiteze sau să interzică prelucrarea (măsuri complementare);

- să dispună rectificarea sau ștergerea datelor sau restricționarea prelucrării.

În cazul în care operatorul va fi sancționat administrativ pentru nerespectarea legislației privind protecția datelor cu caracter personal, Responsabilul de protecția datelor va analiza oportunitatea contestării sancțiunii administrative și va formula propuneri în legătură cu promovarea căii de atac, precum și, dacă este cazul, va elabora contestația, urmând să analizeze cel puțin următoarelor aspecte:

a) natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;

b) dacă încălcarea a fost comisă intenționat sau din neglijență;

c) orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;

d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia;

e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator (dacă este cazul);

f) gradul de cooperare cu Autoritatea de Supraveghere pentru a remedia încălcarea și/sau a atenua posibilele efecte negative ale încălcării;
g) categoriile de date cu caracter personal afectate de încălcare;
h) modul în care încălcarea a fost adusă la cunoștința Autorității de Supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
i) în cazul în care măsurile menționate de legislația specifică au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauza cu privire la același obiect, respectarea respectivelor măsuri;
j) aderarea la coduri de conduită sau la mecanisme de certificare aprobate, și
k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.
12.5.3. **Neconformarea față de prevederile RGPD poate atrage aplicarea de amenzi administrative de până la 300.000 lei (cu aprobarea președintelui ANSPDCP)**, potrivit legislației în materie, respectiv Legea nr. 190/2018 referitoare la protecția datelor cu caracter personal în România.

CAP.13 RESPONSABILITĂȚI ÎN CADRUL ARSVOM Constanța

13.1. Cunoașterea și aplicarea corespunzătoare a prezentului Regulament reprezintă o obligație a întregului personal potrivit limitelor de autoritate aprobate;
13.2. Responsabilitățile privind protecția datelor cu caracter personal revin gradual întregului personal al ARSVOM;
13.3. Responsabilitatea în ceea ce privește: elaborarea, avizarea, aprobarea, implementarea, supravegherea și evaluarea aplicabilității prezentelor norme interne în domeniul GDPR, precum și dispunerea măsurilor care se impun revin, după cum urmează:
13.3.1. ARSVOM (cu toate structurile organizatorice), în calitate de Operator:
a) asigură implementarea legislației comunitare-UE și naționale privind protecția datelor cu caracter personal la nivelul instituției, prin prezentul Regulament sau alte acte interne;
b) asigură conformarea tuturor activităților de prelucrare cu prevederile legislației comunitare-UE și naționale privind protecția datelor cu caracter personal;

c) asigură informarea persoanelor vizate și respectă drepturile acestora;
d) ia toate măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal;
e) asigură respectarea prezentului Regulament privind măsurile de protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal.
13.3.2. **Directorul general al ARSVOM Constanța**:
a) aprobă politici/proceduri operaționale și măsuri de implementare a prevederilor legale privind prelucrarea datelor cu caracter personal;
b) asigură prin instrumentele de control și/sau audit intern/extern/inventariere evaluarea proceselor aferente prezentului Regulament și aplicarea legislației în domeniul protecției datelor;
c) aprobă modificări ale prezentelor norme interne, în situația în care schimbările legislative impun acest lucru în regim de urgență.
13.3.3. **Organele de conducere ale operatorului și conducătorii structurilor sale organizatorice (servicii, birouri, compartimente etc.) sunt responsabili cu protecția datelor cu caracter personal pentru activitățile coordonate și au în acest sens următoarele responsabilități specifice, să**:
a) stabilească scopul și mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare în contextul îndeplinirii obligațiilor legale;
b) asigure elaborarea/actualizarea politicilor/procedurilor proprii și punerea lor în aplicare;
c) asigură implementarea și monitorizează respectarea actelor de reglementare internă și a legislației specifice, în materia prelucrării datelor cu caracter personal de către utilizatorii (angajații) din subordine;
d) coordoneze și monitorizeze activitatea personalului pe linia protecției datelor cu caracter personal la nivelul operatorului;
e) asigure desfășurarea pregătirii de specialitate și instruirea utilizatorilor în acest domeniu;
f) dispună măsuri de completare sau, dup caz, de modificare a fișei posturilor utilizatorilor;
g) analizeze și dispună în ceea ce privește suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidență a datelor cu caracter personal, în conidițiile legii;
h) dispună măsuri organizatorice pentru exercitarea drepturilor de către persoana vizată;

i) coordoneze procesul de furnizare a datelor și informațiilor necesare în vederea soluționării cererilor persoanelor vizate;
j) analizeze periodic activitatea utilizatorilor;
k) informeze operativ Responsabilul de protecția datelor despre vulnerabilitățile și riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii și orice încălcare a normelor de protecție a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate și propune măsuri pentru înlăturarea acestora;

13.3.4. **Utilizatorii, respectiv angajații care prelucrează date cu caracter personal au următoarele responsabilități specifice:**

a) să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum și ale prezentului regulament;
b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condițiile 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 și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, conidiile în care pot fi exercitate aceste drepturi etc.;
c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin șefilor ierarhici, pentru realizarea activităților specifice ale acestora;
d) să păstreze confidențialitatea 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;
e) să respecte măsurile de securitate, precum și celelalte reguli stabilite la nivelul instituției.
f) să informeze de îndată directorul general, șeful ierarhic și Responsabilul de protecția datelor despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință.

13.3.5. **Derulatorii de contracte din cadrul ARSVOM**

a) au responsabilitatea/obligativitatea inserării în contractele încheiate și gestionate de către aceștia a clauzelor specifice cu privire la protecția datelor cu caracter

personal și/sau cu privire la respectarea condițiilor generale, tehnice și de participare;

b) în situațiile în care sunt prelucrate date cu caracter personal în numele operatorului de către persoane împuternicite (procesatori de date-ex: instituii de credit, companii de asigurări, emitente de tichete de masă tipărite sau electronice, carduri beneficii salariai, 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 conținut elementele prevăzute în prezentele norme interne și legislația specifică (GDPR), stabilite în prealabil de Responsabilul de protecția datelor și aprobate de directorul general.

c) în situația prelucrării datelor personale în scop de marketing direct (dacă este cazul), derulatorii de contract, precum și salariații responsabili de operațiunile de marketing direct (inclusiv serviciile aferente IT) vor avea în vedere în mod obligatoriu consimțământul exprimat anterior prelucrării de către persoana vizată, pentru evitarea unor situații de neconformare față de prevederile legale privind protecția datelor personale.

13.3.6. **DPO este responsabil cu implementarea prezentelor norme interne din domeniul GDPR și controlul procesului**, incluzând:

- monitorizarea și controlul aplicării unitare a Regulamentului, testarea conformității, audituri/inventarieri de specialitate și informarea conducerii, participă la organizarea și administrarea programelor de pregătire continuă a angajaților în domeniul cunoașterii prevederilor RGPD;
- responsabilitățile acestuia sunt menționate în prezentele norme interne și în Fișa de post.

13.3.7. **Biroul Resurse Umane:**

a) asigură informarea potențialilor angajați și a angajații cu privire la prelucrarea datelor cu caracter personal și la drepturile de care beneficiază potrivit legii;

b) participă la organizarea și administrarea programelor de pregătire continuă a angajaților în domeniul protecției datelor personale;

13.3.8. la angajarea salariaților, pune la dispoziția acestora în vederea informării și luării la cunoștință cu privire la prevederile normelor interne și se asigură de semnarea de către salariați a angajamentului de conformare.

13.3.9 Prestatorul de servicii IT – **poate fi** responsabil cu:

a) luarea măsurilor tehnice și organizatorice, specifice zonei IT, prevăzute de prezentele norme interne;
b) elaborarea/implementarea/monitorizarea permanentă a politicilor/procedurilor specifice de protecție/securitate a datelor cu caracter personal la nivelul operatorului;
c) instruirea utilizatorilor/angajaților cu privire la politicile/procedurilor specifice de protecție/securitate a datelor cu caracter personal.
13.3.10 Compartimentul Fiscal/Contabil – asigură resursele financiare necesare aplicării RGPD.

CAP.14 ANGAJAMENTUL DE CONFORMARE A ANGAJAȚILOR FAȚĂ DE LEGISLAȚIA SPECIFICĂ ÎN DOMENIUL PROTECȚIEI DATELOR CU CARACTER PERSONAL

14.1. La angajare, înainte de începerea activităților de prelucrare a datelor cu caracter personal, dar și ulterior, cu ocazia derulării raporturilor de muncă, organizării de instruiri profesionale specifice, toți angajații care prelucrează date cu caracter personal trebuie să semneze un Angajament individual de conformare față de legislația specifică și a prezentelor Norme interne privind protecția datelor cu caracter personal din cadrul ARSVOM Constanța.
14.2. Confirmarea scrisă reprezintă asumarea individuala a angajamentului de respectare a legislației specifice și a Regulamentului UE privind protecția datelor cu caracter personal, în scopul protejării reputației operatorului și aplicării standardelor de etică și integritate.
14.3. Semnătura de confirmare înseamnă :
a) că angajatul a luat la cunoștință despre prevederile normelor interne privind protecția datelor cu caracter personal;
b) că angajatul a participat la programele de pregătire și a fost instruit conform prevederilor din acest domeniu;
c) că angajatul înțelege importanța respectării în totalitate a cerințelor cuprinse în legislația națională specifică privind protecția datelor cu caracter personal;
d) că angajatul își asumă necondiționat responsabilitatea în ceea ce privește conformarea cu cerințele cuprinse în legislația specifică privind protecția datelor cu caracter personal;

e) că angajatul înțelege că, în situația nerespectării principiilor și cerințelor privind protecția datelor cu caracter personal, se face direct răspunzător pentru încălcarea angajamentului individual și pentru consecințele ce decurg din acesta.
14.4. Refuzul de a semna confirmarea angajamentului individual înseamnă :
a) că este necesar identificarea motivelor reale care au condus la refuz;
b) că este necesară instruirea suplimentară, dacă motivul real este neînțelegerea mesajului sau informațiilor transmise;
c) că este necesară examinarea atentă a angajatului respectiv, urmat de luarea unor măsuri adecvate, prevăzute de lege, mai ales în situația în care acesta ocupă o funcție care prezintă un risc sensibil la adresa operatorului, dacă refuzul de a semna confirmarea nu are o motivație reală.
14.5. Un exemplar din Angajamentele de Conformare semnate de salariați se vor păstra în gestiunea DPO.

CAP. 15 PREGĂTIREA ȘI INSTRUIREA PERSONALULUI ABILITAT SĂ ACCESEZE ASTFEL DE INFORMAȚII

15.1. Planurile anuale de pregătire continuă, elaborate în condițiile legii, trebuie să conțină teme privind cunoașterea legislației naționale și comunitare în materia prelucrării datelor cu caracter personal, precum și teme specifice privind riscurile pe care le comportă prelucrarea datelor și măsurile minime de securitate, în funcție de specificul activității operatorului. Acestea sunt elaborate de DPO (**anexa nr. 1**) și sunt aprobate de directorul general.
15.2. Periodic, Responsabilul de protecția datelor – DPO organizează cu sprijinul conducerii, instruiri în domeniul GPDR cu personalul care ocupă funcțiile prevăzute în **anexa nr. 2**, pentru cunoașterea procedurilor specifice de lucru instituite și cu privire la riscurile generate de vulnerabilități și amenințări informatice la adresa datelor cu caracter personal prelucrate.
15.3. Instruirile se efectuează periodic, o dată la trei luni și în mod obligatoriu la modificarea cadrului legal în materie. Prelucrarea incidentelor se va realiza cu întregul personal implicat în activitatea de prelucrare a datelor cu caracter personal. Instruirea personalului angajat, care nu se regăsește în **anexa nr. 2**, se va realiza la locul de muncă, prin studiu individual.

15.4 Responsabilul cu protecția datelor cu caracter personal – DPO va elabora o evidență strictă a funcțiilor din cadrul compartimentelor funcționale ale instituției abilitate să prelucreze/acceseze date cu caracter personal, în condițiile legii (anexa nr. 2).

15.5 Obiectivul general al formării: Cunoașterea, instruirea, respectarea și implementarea prevederilor Regulamentului UE nr. 679/2016 referitor la protecția datelor cu caracter personal (GDPR) și a legislației naționale în domeniu.

15.6 Metode de formare (instruire) ce pot fi utilizate:

- prezentare interactivă
- conversație
- explicație
- studiu de caz
- studiu individual

15.7 După prezentarea/susținerea temei de pregătire personalul instruit în domeniul GDPR din cadrul ARSVOM Constanța va semna ***Fișa individuală de pregătire și instruire*** **(anexa nr. 3 și 4)**, care se află la șeful compartimentului funcțional (DPO), sau la personalul care ocupă funcții de conducere, după caz.

15.8 Pregătirea și instruirea personalului abilitat să acceseze datele cu caracter personal din cadrul ARSVOM Constanța se va efectua *"face to face"* sau *online*, în funcție de evoluția pandemiei cu coronavirus, cu respectarea tuturor măsurilor legale de protecție în acest domeniu.

CAP. 16 DISPOZIȚII FINALE

16.1. Prezentele Norme interne în domeniul GDPR, ca norme procedurale în domeniul protecției datelor cu caracter personal, emise de ARSVOM Constanța, intră sub incidența prevederilor Legii nr. 544/2001 referitoare la informațiile de interes public, au un caracter public și se află în gestiunea responsabilului cu protecția datelor cu caracter personal – DPO, unde pot fi consultate;

16.2. Prezentele norme se pot aplica și în activitatea Consiliului de Administrație al ARSVOM Constanța;

16.3. Nerespectarea prevederilor prezentelor norme atrage, dup caz, în funcție de gravitate, sancțiuni disciplinare și pecuniare conform codului muncii sau penale, în condițiile legii;

16.4. Dacă prin nerespectarea prezentelor norme interne de către angajați se produc prejudicii instituției, aplicând principiul proporționalității, sancționarea angajatului care a produs prejudiciul poate fi efectuată potrivit prevederilor legale în materie;
16.5. Prin DPO se înțelege responsabilul cu protecția datelor cu caracter personal – DPO din cadrul ARSVOM;
16.6. Aplicarea sancțiunilor administrative nu înlătură răspunderea penală, civilă, materială sau contravențională, dup caz, a persoanelor vinovate.
16.7. Prezentele norme interne, ca norme procedurale, completează orice alte acte de reglementare internă din cadrul ARSVOM Constanța;
16.8. Dacă ulterior datei intrării în vigoare a prezentelor reglementări, o prevedere legală modifică/completează/abrogă prevederile prezentelor norme interne, se vor aplica prevederile legale în vigoare.
16.9. Prezentele Norme interne de ordine interioară referitoare la respectarea **REGULAMENTULUI GENERAL PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL (RGPD)** intră în vigoare la data aprobării de către directorul general al ARSVOM Constanța.

Întocmit,
Exp. Răibuleț Cătălina

ANEXE

ANEXA Nr. 1

PLAN ANUAL DE INSTRUIRE ŞI PREGĂTIRE ÎN DOMENIUL PROTECŢIEI DATELOR CU CARACTER PERSONAL

Nr. crt.	TEMA	Responsabil întocmire material	Data prezentării	Metode de instruire	Luare la cunostinta a persoanei instruite	Observaţii
Trimestrul I ianuarie - martie						
1	Prezentare legislatie in domeniul protectiei datelor personale – GDPR	Consultant GDPR		Prezentare	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
2	Incidentul de securitate in contextul GDPR. Registrele de evidenta a activitatii de prelucrare a datelor personale	DPO		Studiu de caz	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
3	Regulamentul UE nr. 679/2016 referitor la protectia datelor personale	-		Studiu individual	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
Trimestrul II aprilie - iunie						
4	GDPR explicat "Grupul de lucru art 29 (UE)": Responsabilitatea şi guvernanţa în noua viziune GDPR	Consultant GDPR		Studiu de caz	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
5	GDPR Explicitat 11 "Data Protection Officer"	DPO		Prezentare	Mentionarea instruirii in *Fisa de pregatire individuala* a	

					participantilor	
6	Comparație între conceptul de "incident de securitate" și "încălcare a securității datelor cu caracter personal" în contextual GDPR și ISO 27001	-		Studiu individual	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
Trimestrul III iulie - septembrie						
7	Măsuri tehnice privind prelucrarea datelor cu caracter personal	Consultant GDPR		Studiu de caz	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
8	Verificarea legalității prelucrării datelor cu caracter personal și principiile de bază ale GDPR	DPO		Prezentare	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
9	Încălcări ale securității datelor cu caracter personal: primele 5 măsuri tehnice care trebuie luate în considerare	-		Studiu individual	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
Trimestrul IV octombrie - decembrie						
10	Informare privind supravegherea și monitorizarea video în cadrul A.R.S.V.O.M. Constanța	Consultant GDPR		Prezentare	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
11	Încălcări ale prevederilor GDPR sancționate de CODUL PENAL din 17/07/2009 (actualizat în 2014)	DPO		Studiu de caz	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	
12	Măsuri tehnice privind prelucrarea datelor cu caracter personal	-		Studiu individual	Mentionarea instruirii in *Fisa de pregatire individuala* a participantilor	

ANEXA Nr. 2

TABEL CU FUNCȚIILE PENTRU CARE SE FACE INSTRUIREA
(Grup nave)

Nr. Crt.	NAVA	LOCAȚIE	Funcții de la bordul navei pentru care se face instruirea	Observații
1.	R/M „HERCULES”	Dana 78	- Comandant - Of. Punte - Șef mecanic	
2.	SAR „ALBATROS”	Port Sulina	- - Of. Punte	
3.	SAR „OPAL SAR”	Dana 79	- Of. Punte	
4.	SAR „TOPAZ”	Port Mangalia	- Of. Punte	
5.	S/I „SAFIR”	Dana 79	- Of. Punte	
6.	S/I „RUBIN”	Dana 79	- Of. Punte	
7.	S/I „CRISTAL”	Dana 79	- Of. Punte	
8.	S/S „SORANA 1”	Dana 79	- Conducător șalupă	
9.	S/S „SORANA 2”	Port Sulina	- Conducător șalupă	
10.	S/S „SORANA 3”	Dana 79	- Conducător șalupă	
11.	S/S „SATURN”	Dana 79	- Conducător șalupă	
12.	S/S „JUPITER”	Dana 79	- Conducător șalupă	
13.	SAR „APOLLO”	Portul Tomis	- Comandant - Of. Punte	
14.	SAR “ARTEMIS”	Dana 77	- Comandant - Of. Punte	
15.	SAR „MAIA”	Port Mangalia	- Comandant - Of. Punte	
16.	R/M „BRIZO”	Dana 78	- Comandant - Of. Punte - Șef mecanic	

TABEL CU FUNCȚIILE PENTRU CARE SE FACE INSTRUIREA (Tesa)

Nr. Crt.	SERVICIU/BIROU/ COMPARTIMENT	LOCAȚIE	Funcții de la birourile tesa pentru care se face instruirea	Observații
1.	Directori	A.R.S.V.O.M. Cța Dana 78	- Director General - Director Exploatare	
2.	Birou resurse umane și comunicare	A.R.S.V.O.M. Cța Dana 78	- Șef birou	
3.	Serviciu planificare, logistică și investiții	A.R.S.V.O.M. Cța Dana 78	- Șef serviciu	
4.	Birou tehnic	A.R.S.V.O.M. Cța Dana 78	- Șef birou	
5.	Serviciu economic	A.R.S.V.O.M. Cța Dana 78	- Șef serviciu	
6.	Compartiment protecția muncii	A.R.S.V.O.M. Cța Dana 78	- Responsabil SSM	
7.	Compartiment juridic	A.R.S.V.O.M. Cța Dana 78	- Consilier juridic	
8.	Serviciu de coordonare, comunicare și securitate opetațională	A.R.S.V.O.M. Cța Dana 78	- Șef serviciu	
9.	Compartiment achiziții	A.R.S.V.O.M. Cța Dana 78	- Personal compartiment	

ANEXA Nr. 3

FIŞA INDIVIDUALĂ DE PREGĂTIRE ŞI INSTRUIRE

ÎN DOMENIUL GDPR* (personal de conducere)

NUME: _____

PRENUME: _____

FUNCŢIA: _____

STRUCTURA FUNCȚIONALĂ: _____

Nr. Crt	Tema pregătirii	Forma de pregătire	Locul	Perioada	Semnătura titularului de fişă	Observaţii
1.	Prezentare legislatie in domeniul protectiei datelor personale – GDPR	Prezentare				
2.	Incidentul de securitate in contextul GDPR. Registrele de evidenta a activitatii de prelucrare a datelor personale	Studiu de caz				
3.	Regulamentul UE nr. 679/2016 referitor la protectia datelor personale	Studiu individual				
4.	GDPR explicat "Grupul de lucru art 29 (UE)": Responsabilitatea şi guvernanţa în noua viziune GDPR	Studiu de caz				
5.	GDPR Explicitat 11 "Data Protection Officer"	Prezentare				
6.	Comparaţie între conceptul de "incident de securitate" şi "încălcare a securităţii datelor cu caracter personal" în contextual GDPR şi ISO 27001	Studiu individual				

7.	Măsuri tehnice privind prelucrarea datelor cu caracter personal	Studiu de caz				
8.	Verificarea legalității prelucrării datelor cu caracter personal și principiile de bază ale GDPR	Prezentare				
9.	Încălcări ale securității datelor cu caracter personal: primele 5 măsuri tehnice care trebuie luate în considerare	Studiu individual				
10.	Informare privind supravegherea și monitorizarea video în cadrul A.R.S.V.O.M. Constanța	Prezentare				
11.	Încălcări ale prevederilor GDPR sancționate de CODUL PENAL din 17/07/2009 (actualizat în 2014)	Studiu de caz				
12.	Măsuri tehnice privind prelucrarea datelor cu caracter personal	Studiu individual				

*Notă: Se va păstra în gestiunea DPO

ANEXA Nr. 4

FIŞA INDIVIDUALĂ DE PREGĂTIRE ŞI INSTRUIRE

ÎN DOMENIUL GDPR* (personal de execuţie)

NUME: _____

PRENUME: _____

FUNCŢIA: _____

STRUCTURA FUNCŢIONALĂ: _____

Nr. Crt	Tema pregătirii	Forma de pregătire	Locul	Perioada	Semnătura titularului de fişă	Observaţii
1.	Regulamentul UE nr. 679/2016 referitor la protectia datelor personale	Studiu individual				
2.	Comparaţie între conceptul de "incident de securitate" şi "încălcare a securităţii datelor cu caracter personal" în contextual GDPR şi ISO 27001	Studiu individual				
3.	Încălcări ale securităţii datelor cu caracter personal: primele 5 măsuri tehnice care trebuie luate în considerare	Studiu individual				
4.	Măsuri tehnice privind prelucrarea datelor cu caracter personal	Studiu individual				