UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNDRUMAR METODOLOGIC CU TEMATICA PRELUCRĂRII DATELOR CU CARACTER PERSONAL ÎN CONTEXTUL GESTIONĂRII FESI

Elaborat în cadrul proiectului

"Instruire în domeniul prelucrării datelor cu caracter personal pentru structurile din cadrul sistemului de coordonare, gestionare și control al FESI în România"

Cod proiect 3.1.107, Cod SMIS 2014+ 128212

AGENȚIA NAȚIONALĂ A FUNCȚIONARILOR PUBLICI

CUPRINS

CUVÂNT ÎNAINTE

Agenția Națională a Funcționarilor Publici (ANFP), în demersul său instituțional, și-a manifestat în mod constant preocuparea de a contribui la consolidarea capacității administrației publice din România. O atenție deosebită a fost acordată nevoii identificate de a dezvolta competențele personalului structurilor cu rol de coordonare, gestionare și control al fondurilor europene, precum și sporirii abilităților beneficiarilor de a scrie proiecte, de a implementa eficient şi eficace Fondurile Europene Structurale și de Investiții în România (FESI).

Începând din data de 25 mai 2018 au devenit obligatorii prevederile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date. Raportat la implicațiile majore asupra activităților specifice ale instituțiilor și autorităților publice abilitate cu rol în coordonarea, gestionarea și controlul FESI în România, Agenția a venit în întâmpinarea necesității de clarificare a modului de respectare și aplicare a Regulamentului, prin facilitarea de dezbateri tematice, dezvoltarea de instrumente și instruire.

Îndrumarul metodologic cu tematica prelucrării datelor cu caracter personal în contextul gestionării FESI elaborat în cadrul proiectului cod 3.1.107 are rolul de a facilita înțelegerea normelor cu privire la prelucrarea datelor cu caracter personal și transferul acestora de la un operator de date la altul (inclusiv în afara teritoriului României). Totodată, documentul prezintă mecanisme și metode care să contribuie la prevenirea și/sau corectarea acțiunilor neconforme ale beneficiarilor în ceea ce privește aplicarea prevederilor din domeniul prelucrării datelor cu caracter personal.

Ghidul elaborat reprezintă și un rezultat al dezbaterilor tematice, cu caracter practic, susținute în vederea sincronizării și asigurării premiselor pentru o aplicare unitară a prevederilor Regulamentului (UE) 679/2016 la nivelul sistemului FESI. Acest demers a implicat eforturile conjugate ale instituțiilor cu rol în coordonarea, gestionarea și controlul FESI și ale mediului academic, participante la evenimentele tip seminar organizate de ANFP în octombrie 2020.

Ne exprimăm încrederea că materialul dezvoltat va conduce către o mai bună înțelegere a legislației relevante din aria protecției datelor cu caracter personal și va constitui un instrument util, dedicat administrației publice, în gestionarea activităților specifice din domeniul fondurilor europene.

PREZENTARE PROIECT

Agenția Națională a Funcționarilor Publici este beneficiarul proiectului co-finanțat din Fondul European de Dezvoltare Regională prin Programul Operațional Asistență Tehnică (POAT) 2014-2020 (Axa Prioritară 3, Obiectivul specific 3.1., Acțiunea 3.1.1.)

Obiectivul general reprezintă dezvoltarea capacității manageriale a structurilor cu rol de coordonare, gestionare și control al FESI prin asigurarea înțelegerii modalității de aplicare a reglementărilor în materie de prelucrare și protecție a datelor cu caracter personal în derularea activităților specifice.

Obiectivul specific 1 este reprezentat de furnizarea unui modul de formare tematic pentru un grup țintă de aproximativ 700 de persoane din cadrul structurilor cu rol de coordonare, gestionare și control al FESI.

Obiectivul specific 2 este reprezentat de întărirea cooperării interinstituționale, familiarizarea cu operațiunile specifice și conștientizarea importanței acestor activități în domeniul prelucrării datelor cu caracter personal pentru un grup de aproximativ 50 de persoane din cadrul structurilor cu rol de coordonare, gestionare și control al FESI.

Acest îndrumar metodologic, cu tematica prelucrării datelor cu caracter personal în contextul gestionării FESI, cuprinde informații și instrumente care să-și găsească aplicabilitate în activitatea curentă a personalului din sistemul de management și control al FESI.

1. Noțiuni generale, cadrul legislativ european și național, concepte (instituții juridice și terminologie) specifice domeniului – „protecția datelor cu caracter personal”

Regulamentul general privind protecția datelor (denumit în continuare **RGPD**) a fost aprobat de Comisia Europeană (CE) la 27 aprilie 2016 și a devenit aplicabil la 25 mai 2018. Acest Regulament înlocuiește legislația comunitară anterioară care reglementa protecția datelor și anume, Directiva privind protecția datelor din 1995. Una din diferențele majore dintre RGPD și actul legislativ anterior este că RGPD este un regulament și nu o directivă. Ceea ce înseamnă că se aplică direct, iar fiecare dintre țările care compun Uniunea Europeană are obligația să asigure aplicarea dispozițiilor acestuia fără a mai fi necesară integrarea ori transpunerea în cadrul legislativ intern.

Din 1995 și până în mai 2018, principalul instrument juridic al Uniunii Europene care a asigurat reglementarea domeniului protecției datelor cu caracter personal a fost Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (Directiva privind protecția datelor), transpusă în legislația internă prin intermediul Legii nr.677/2001.

Adoptarea în 2016 a Regulamentului general privind protecția datelor a produs o adevărată reformă a legislației Uniunii Europene în materie de protecție a datelor cu caracter personal, obiectivele urmărite fiind asigurarea unei protecții adecvate în ceea ce privește drepturile fundamentale circumscrise noțiunii de viață privată în contextul provocărilor economice și sociale ale erei digitale. RGPD menține, clarifică și dezvoltă principiile și drepturile persoanei vizate transpuse prin intermediul Directivei privind protecția datelor. Mai mult, RGPD a introdus obligații care impun operatorului de date cu caracter personal să ia în considerare, încă din faza de proiectare, mecanismele și mijloacele de prelucrare a datelor cu caracter personal, integrarea unor mecanisme prin care să se asigure pe de o parte, reducerea la minim a datelor cu caracter personal prelucrate în vederea atingerii unui scop și, pe de altă parte, protecția implicită a datelor prin mecanisme prin care să se asigure că datele sunt prelucrate doar în scopul în care au fost colectate, să numească un responsabil cu protecția datelor și să asigure respectarea principiului

responsabilității, care este mai eficient proiectat. Conform legislației UE, în principiu, regulamentele sunt aplicabile în mod direct, nu este necesară adoptarea unor măsuri de punere în aplicare la nivel național.

În aceste condiții, Regulamentul general privind protecția datelor stabilește un set unic de norme de protecție a datelor în întreaga UE.

Cu toate acestea, deși RGPD este aplicabil în mod direct, statele membre au obligația să își actualizeze anumite aspecte, expres prevăzute în Regulament, prin revizuirea legislațiilor naționale în materie de protecție a datelor cu caracter personal pentru a crea cadrul necesar implementării RGPD.

Legislația relevantă în domeniul Protecției Datelor cu Caracter Personal

Cadrul legislativ European

Directive

1. **Directiva (UE) 2016/680** a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date;
2. **Directiva 2002/58/CE** a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) a fost modificată prin Directiva 2009/136/CE din 25 noiembrie 2009;

Regulamente

3. **Regulamentul (UE) 2016/679** privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);

4. **Regulamentul (UE) 2018/1725** al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE a intrat în vigoare la 11 decembrie 2018.

Decizii

5. **Decizia 2010/87/UE din 5 februarie 2010** privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului

Recomandări

6. **Recomandarea 2009/387/CE din 12 mai 2009** privind aplicarea principiilor de respectare a vieţii private şi de protecţie a datelor în aplicaţiile bazate pe identificarea prin radiofrecvenţă.

Link-uri utile

Comitetul European pentru Protecția Datelor – Recomandări și bune practici: https://edpb.europa.eu/our-work-tools/general-guidance/RGPD-guidelines-recommendations-best-practices_ro

Cadrul legislativ național

7. **Legea nr. 129 /2018** pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
8. **Legea nr. 190 /2018** privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi

privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor);

9. **Legea nr. 682 / 2001** privind ratificarea Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981;
10. **Legea nr. 506 / 2004** privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice;

Decizii ANSPDPC

11. **Decizia nr. 128/2018** privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE;
12. **Decizia nr. 133/2018** privind aprobarea Procedurii de primire și soluționare a plângerilor;
13. **Decizia nr. 161/2018** privind aprobarea Procedurii de efectuare a investigațiilor;
14. **Decizia nr. 238/2019** privind modificarea anexei nr. 2 la Procedura de efectuare a investigaţiilor;
15. **Decizia nr. 174/2018** privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal.

Link-uri utile: Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, **https://www.dataprotection.ro**

Concepte (instituţii juridice şi terminologie) specifice domeniului - „protecția datelor cu caracter personal”

Terminologie - definiții, detalierea termenilor:

1. **“date cu caracter personal”** înseamnă orice informații privind o persoană fizică identificată sau identificabilă (persoana 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 online, 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, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

3. **“restricționarea prelucrării”** înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

4.**”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 află persoana fizică respectivă sau deplasările acesteia;

5. **“pseudonimizare”** 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 de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

6. **“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;

7. **“operator”** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur(ă) sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern;

8. **“persoana împuternicită de operator”** înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

9. **“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 respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

10. **“parte terță”** înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism, altul decât persoana vizată, operatorul, persoana 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;

11. **“consimțământ 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;

12. **“încălcarea securității datelor cu caracter personal”** înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a

datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

13. **“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 rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

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

15. **“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;

16. **“sediu principal”** înseamnă:(a) în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal; (b) în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament;

17. **“reprezentant”** înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27 din Regulamentul (UE) 2016/679, care reprezintă operatorul sau persoana împuternicită

în ceea ce privește obligațiile lor care le revin în temeiul prezentului regulament;

18. **"întreprindere"** înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfașoară în mod regulat o activitate economică;

19. **"grup de întreprinderi"** înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;

20**. "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;

21. **"autoritate de supraveghere"** înseamnă Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;

22. **"autoritate de supraveghere vizată"** înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:

(a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;

(b) persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau

(c) la autoritatea de supraveghere respectivă a fost depusă o plângere;

23. **"prelucrare transfrontalieră"** înseamnă:

(a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau

(b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre;

24. **"obiecție relevantă și motivată"** înseamnă o obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii;

25**. "serviciile societății informaționale"** înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva 2015/1535/CE a Parlamentului European și a Consiliului;

26. **"organizație internațională"** înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

27. **"stocarea"** reprezintă păstrarea pe orice fel de suport a datelor cu caracter personal culese.

28. **"codul numeric personal"** reprezintă 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.

29. **"date anonimizate"** sunt date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă.

30. **"date cu caracter personal cu functie de identificare de aplicabilitate generală (date cu caracter special)"** reprezintă numere prin care se identifică o persoană fizică în anumite sisteme de evidență și care au aplicabilitate generală, cum ar fi: codul numeric personal, seria și numărul actului de identitate, numărul pașaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate.

31. **“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;

32. **“procedura”** înseamnă prezentarea în scris, a tuturor pașilor ce trebuie urmați, a metodelor de lucru stabilite și a regulilor de aplicat necesare îndeplinirii atribuțiilor și sarcinilor, având în vedere asumarea responsabilităților;

33. **“procedura operațională”** înseamnă prezentarea formalizată, în scris, a tuturor pașilor ce trebuie urmați, a metodelor de lucru stabilite și a regulilor de aplicat în vederea realizării activității, cu privire la aspectul procesual;

34. **“ediție a unei proceduri operaționale”** înseamnă forma inițială sau actualizată, după caz, a unei proceduri operaționale, aprobată și difuzată;

35. **“revizia în cadrul unei ediții”** înseamnă acțiunile de modificare, adăugare, suprimare sau altele asemenea, după caz, a uneia sau a mai multor componente ale unei ediţii a procedurii operaționale, acțiuni care au fost aprobate și difuzate.

2. Principiile esențiale ale legislației europene privind protecția datelor cu caracter personal

Articolul 5 din Regulamentul general privind protecția datelor/RGPD stabilește principiile care reglementează prelucrarea datelor cu caracter personal. Aceste principii se referă la următoarele:

- ⇒ legalitate, echitate și transparență
- ⇒ limitări legate de scop
- ⇒ reducerea la minimum a datelor
- ⇒ exactitatea datelor
- ⇒ limitări legate de stocare
- ⇒ integritate și confidențialitate
- ⇒ principiul responsabilităţii (art.5 alin.2)

2.1 Legalitate, echitate și transparență

Pentru ca prelucrarea datelor cu caracter personal în cadrul FESI să fie legală, aceasta trebuie să îndeplinească cel puțin unul dintre cele 6 criterii de mai jos:

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 învestit 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 persoana vizată este un copil.**

Criteriul prevăzut la litera (f) nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor. Aceasta nu înseamnă că acest criteriu lipsește cu desăvârșire în procesul de asigurare a legalității la nivelul instituțiilor publice, înseamnă că acesta nu poate legitima decât anumite prelucrări de date cu caracter personal care nu țin de îndeplinirea funcțiilor instituției respective. Persoana vizată trebuie să fie informată cu

privire la riscuri, pentru a se asigura faptul că prelucrarea nu are efecte negative neprevăzute.

Principiul echității prelucrării reglementează în primul rând relația dintre operator și persoana vizată.

Prelucrarea datelor cu caracter personal trebuie efectuată în mod transparent. Autoritățile de management (FESI) au obligația ca operatori de a lua toate măsurile adecvate pentru a informa persoanele vizate care pot fi angajați sau beneficiari – cu privire la modul în care sunt utilizate datele lor cu caracter personal.

Transparența vizează în primul rând informațiile furnizate persoanei fizice înainte de începerea prelucrării, care ar trebui să fie ușor accesibile persoanelor vizate, precum și la informațiile furnizate persoanelor vizate în urma unei cereri de acces la propriile lor date.

Înainte de a prelucra datele persoanelor vizate, operatorii trebuie să informeze persoanele vizate, printre altele, cu privire la scopul prelucrării, cu privire la identitatea și adresa sediului operatorului.

Informațiile privind operațiunile de prelucrare trebuie furnizate întrun **limbaj clar și simplu**, pentru a permite persoanelor vizate să înțeleagă cu ușurință normele, riscurile, garanțiile și drepturile implicate.

Persoanele vizate au dreptul de acces la datele care îi privesc, indiferent de locul unde sunt prelucrate acestea.

Operatorii ar trebui să înștiințeze persoanele vizate și publicul larg că vor prelucra datele într-un mod legal și transparent și trebuie să fie în măsură să demonstreze conformitatea operațiunilor de prelucrare cu RGPD. Operațiunile de prelucrare în cadrul FESI nu trebuie efectuate în secret, iar persoanele vizate ar trebui să fie conștiente de riscurile potențiale.

În plus, operatorii, în măsura în care este posibil, trebuie să acționeze într-un mod care să respecte cu promptitudine voința persoanei vizate, în special atunci când consimțământul acesteia constituie temeiul juridic al prelucrării datelor.

2.2 Principiul limitărilor legate de scop

Principiul impune ca orice prelucrare a datelor cu caracter personal să se facă în scopuri determinate, explicite, și doar în acele scopuri suplimentare care sunt compatibile cu scopul inițial[1]. Prelucrarea datelor cu caracter personal în scopuri nedefinite și/sau nelimitate este, așadar, ilegală. Nu este legală nici prelucrarea datelor cu caracter personal fără un scop determinat, bazată exclusiv pe considerația că o astfel de prelucrare ar putea fi utilă la un moment dat în viitor. Legitimitatea prelucrării datelor cu caracter personal este strâns legată de scopul prelucrării, care trebuie să fie explicit, determinat și legitim, scopul fiind elementul determinat al prelucrării. În concluzie, nu putem vorbi de o prelucrare legală și legitimă în lipsa unui scop legal și legitim.

Orice scop nou de prelucrare a datelor care nu este compatibil cu scopul inițial trebuie să aibă propriul temei juridic, dintre criteriile enumerate mai sus, și nu se poate baza pe faptul că datele au fost colectate sau prelucrate inițial în alt scop legitim. Legitimitatea este o caracteristică ce trebuie să guverneze atât scopul inițial al prelucrării, cât și scopul de prelucrare suplimentar. În acest context, este necesar a fi precizat că, spre deosebire de Directiva 95/46/CE care impunea aceeași condiție de compatibilitate între scopul inițial al prelucrării și scopurile de prelucrare suplimentară dar fără a stabili un mecanism sau criterii de realizarea a compatibilității între scopuri, RGDP stabilește în cuprinsul art.6 alin.(4) cinci criterii care trebuie avute în vedere pentru determinarea

[1] Regulamentul general privind protecția datelor, art. 5 alin. (1) lit. (b).
Regulamentul general privind protecția datelor, art. 5 alin. (1) lit. (d); Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, STE 108, art. 5 alin. (4) lit. (d)

compatibilității între scopuri, creând în acest sens un adevărat mecanism.

Regulamentul general privind protecția datelor prevede că „prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice" este considerată a priori compatibilă cu scopul inițial.

Cu toate acestea, trebuie aplicate măsuri de protecție adecvate, cum ar fi anonimizarea, criptarea sau pseudonimizarea datelor și restricționarea accesului la date în cazul unei prelucrări ulterioare a datelor cu caracter personal.

2.3 Principiul reducerii la minimum a datelor

Prelucrarea datelor trebuie **să se limiteze la ceea ce este necesar** pentru îndeplinirea unui scop legitim. Reducerea la minim a datelor vizează în principal determinarea în concret a categoriilor de date cu caracter personal necesare pentru atingerea scopului urmărit prin prelucrare. Mecanismul este esențial în ceea ce teoreticienii denumesc a fi "protecția persoanei față de prelucrare", reducerea la minim reprezentând chiar esența acestei protecții.

Prelucrarea datelor cu caracter personal în contextul FESI ar trebui să aibă loc numai atunci când scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. De aceea, trebuie avut în vedere elementul determinant al inițierii reformei legislației europene în materie de protecție a datelor, respectiv avansul tehnologic și impactul produs de utilizarea noilor tehnologii în ceea ce privește viața privată. În acest context, trebuie introdusă și înțeleasă și ideea de evaluare a impactului prelucrării asupra protecției datelor, respectiv prin necesitatea limitării prelucrării la minimul necesar.

Prelucrarea datelor nu poate interveni în mod disproporționat asupra intereselor, drepturilor și libertăților fundamentale a persoanei vizate în cauză.

2.4 Principiul exactității datelor

Un operator care deține informații cu caracter personal nu stochează și nu prelucrează aceste informații fără a lua măsuri pentru a se asigura

cu suficientă certitudine că datele sunt exacte și actualizate[2]. Totuși, ideea de exactitate trebuie corelată cu scopul prelucrării, acesta fiind așa cum am arătat, elementul determinant. Astfel, întrun anumit context anumite date pot fi prelucrate fără a avea un nivel de acuratețe desăvârșit dacă scopul prelucrării poate fi atins în acest mod, spre exemplu, crearea unei grupe de copii pentru cor, scopul putând fi atins dacă vor fi prelucrate doar prenumele acestora în timp ce, pentru înregistrarea în sistemul de învățământ, spre exemplu, datele trebuie să aibă un nivel de acuratețe desăvârșit.

Operatorul trebuie să pună în aplicare principiul exactității datelor în cadrul tuturor operațiunilor de prelucrare.

Datele inexacte trebuie să fie șterse sau rectificate fără întârziere.

Este posibil să fie necesar ca datele să fie verificate periodic și actualizate pentru a se asigura exactitatea acestora.

2.5 Principiul limitării legate de stocare

Principiul limitărilor legate de stocare implică eliminarea sau anonimizarea datelor imediat ce acestea nu mai servesc scopurilor pentru care au fost colectate.

Limitarea duratei de stocare a datelor cu caracter personal se aplică numai datelor păstrate într-o formă care permite identificarea persoanelor vizate. Prin urmare, stocarea legală a datelor care nu mai sunt necesare se poate realiza, de exemplu, prin anonimizarea acestora, pentru domeniul FESI trebuie analizată stocarea fizică și electronică (MYSMIS 2014) în contextul regulamentelor europene aplicabile.

Datele arhivate în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice pot fi păstrate pe perioade mai lungi,

[2] Regulamentul general privind protecția datelor, articolul 5 alineatul (1) litera (d); Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, STE 108, art. 5 alin. (4) lit. (d)

cu condiția ca respectivele date să fie utilizate exclusiv în aceste scopuri[3].

2.6 Principiul securității datelor

Principiul securității datelor **implică punerea în aplicare, în cadrul prelucrării datelor cu caracter personal, a măsurilor tehnice sau organizatorice adecvate** pentru a asigura protecția datelor împotriva accesului, utilizării, modificării, divulgării, pierderii, distrugerii sau deteriorării accidentale, neautorizate sau ilegale[4].

În funcție de circumstanțele specifice ale fiecărui caz, măsurile tehnice și organizatorice adecvate ar putea include, de exemplu, pseudonimizarea și criptarea datelor cu caracter personal și/sau testarea și evaluarea periodică a eficacității măsurilor, pentru a asigura faptul că prelucrarea datelor se face în condiții de siguranță.

Aceste măsuri includ, printre altele:

- ✓ pseudonimizarea și criptarea datelor cu caracter personal;
- ✓ asigurarea confidențialității, integrității, disponibilității și rezistenței continue ale sistemelor și serviciilor de prelucrare;
- ✓ restabilirea disponibilității datelor cu caracter personal și a accesului la acestea, în cazul în care are loc o pierdere de date printr-un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor pentru a garanta securitatea prelucrării.

Securitatea datelor nu se realizează numai prin utilizarea echipamentelor corespunzătoare hardware și software. Aceasta necesită și norme organizatorice interne adecvate. Ideal, acestea ar trebui să trateze următoarele aspecte:

- ✓ punerea la dispoziția tuturor angajaților, periodic, a informațiilor despre normele privind securitatea datelor și obligațiile lor în temeiul

[3] Regulamentul general privind protecția datelor, art. 5 alin. (1) lit. (e); Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, STE 108, art. 5 alin. (4) lit. (b) și art. 11 alin. (2)

[4] Regulamentul general privind protecția datelor, considerentul 39 și articolul 5 alineatul (1) litera (f); Convenția 108 modernizată, articolul 7.

legislației privind protecția datelor, în special obligațiile lor de confidențialitate;
✓ distribuirea clară a responsabilităților și sublinierea clară a competențelor în materie de prelucrare a datelor, în special cu privire la deciziile de prelucrare a datelor cu caracter personal și de transmitere a datelor către terți sau către persoanele vizate;
✓ utilizarea datelor cu caracter personal numai în conformitate cu instrucțiunile persoanei competente sau în conformitate cu normele generale puse în aplicare;
✓ protejarea accesului în spațiile și la echipamentele hardware și software ale operatorului sau ale persoanei împuternicite de operator, inclusiv verificări ale autorizației de acces;
✓ asigurarea faptului că autorizațiile de acces la date cu caracter personal au fost acordate de persoana competentă și că sunt emise pe baza documentației adecvate;
✓ protocoale automatizate privind accesul electronic la datele cu caracter personal și verificarea periodică a acestor protocoale de către oficiul intern de supraveghere (prin urmare, necesitatea înregistrării tuturor activităților de prelucrare a datelor).

Consimțământul

Consimțământul, ca **temei juridic pentru prelucrarea datelor cu caracter personal,** trebuie acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului pentru prelucrare.

Prelucrarea categoriilor speciale de date cu caracter personal necesită un consimțământ explicit.

Dreptul UE stabilește mai multe elemente necesare pentru ca un consimțământ să fie valabil, care au ca scop garantarea intenției efective a persoanelor vizate de a accepta o anumită utilizare a datelor lor[5]:

[5] Regulamentul general privind protecția datelor, articolul 7.

- ✓ Consimțământul trebuie acordat printr-o acțiune neechivocă care **să constituie o manifestare liber exprimată, specifică**, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal. O astfel de manifestare poate fi o acțiune sau o declarație.
- ✓ Persoana vizată **trebuie să aibă dreptul de a-și retrage în orice moment** consimțământul.
- ✓ În contextul unei declarații scrise care include și alte aspecte, cum ar fi „condițiile de utilizare", cererile de acordare a consimțământului trebuie să fie formulate într-un limbaj clar și simplu și într-o formă inteligibilă și ușor accesibilă, care să distingă în mod clar consimțământul de alte aspecte; dacă o parte din această declarație încalcă RGPD, aceasta nu are caracter obligatoriu.

Consimțământul va fi valabil numai în contextul legislației privind protecția datelor, cu condiția îndeplinirii tuturor acestor cerințe.

Este responsabilitatea operatorului să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale.

Consimțământul trebuie să fie explicit atunci când se referă la prelucrarea datelor sensibile și poate fi acordat verbal sau în scris. Acesta din urmă poate fi acordat prin mijloace electronice. În cadrul legislației UE, acordul pentru prelucrarea datelor cu caracter personal ale unei persoane trebuie să fie exprimat printr-o declarație sau printr-o acțiune neechivocă. Astfel, consimțământul nu poate fi dedus din absența unui răspuns, din căsuțe bifate în prealabil, din formulare completate în prealabil sau din absența unei acțiuni[6].

Cerințe privind consimțământul pentru copii

RGPD prevede o protecție specifică pentru copii în contextul apartenenței la grupurile țintă FESI, întrucât aceștia „*pot fi mai puțin*

[6] Regulamentul general privind protecția datelor, considerentul 32; Raportul explicativ privind Convenția 108 modernizată, punctul 42.

conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal". Prin urmare, în conformitate cu dreptul UE, atunci când în cadrul proiectelor FESI se prelucrează date cu caracter personal ale unor copii cu vârsta sub 16 ani pe baza consimțământului, această prelucrare va fi legală „*numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului*".

3. Drepturile persoanei vizate şi modalităţi concrete de prelucrare a datelor cu caracter personal în cadrul activităţilor specifice ale sistemului de coordonare, gestionare şi control al FESI

Orice persoană vizată are dreptul de a primi informații privind orice prelucrare a datelor sale cu caracter personal de către un operator de date, sub rezerva unor excepții limitate

3.1 Drepturile persoanelor vizate

RGPD stabilește un set de drepturi pe care persoana vizată le poate exercita și pe care operatorul care deține datele personale trebuie să le asigure și la care să răspundă, în caz de solicitare, în general, în 30 de zile.

- **Dreptul de a fi informat** - oferă dreptul persoanei vizate de a fi informată cu privire la datele ce vor fi colectate, scopul, de către cine, unde vor fi transferate datele;
- **Dreptul de acces** - oferă posibilitatea persoanei vizate de a avea o copie a datelor cu caracter personal pe care o societate le deţine şi care se referă la ea;
- **Dreptul de rectificare** - oferă posibilitatea persoanei vizate de a solicita corecţia sau actualizarea datelor cu caracter personal dacă acestea sunt greșite sau inexacte;
- **Dreptul la ștergere** - oferă posibilitatea persoanei vizate de a solicita ştergerea datelor sale;
- **Dreptul de a restricționa procesarea** - oferă posibilitatea persoanei vizate de a solicita întreruperea prelucrării datelor în cazul în care există motive să se procedeze astfel;

- **Dreptul la portabilitatea datelor** - oferă posibilitatea persoanei vizate de a obține datele sale într-un format structurat, utilizat în mod curent și care poate fi citit automat în vederea exercitării dreptului de a transmite aceste date altui operator;
- **Dreptul de a obiecta** - oferă posibilitatea persoanei vizate de a solicita oprirea prelucrării;
- **Automatizarea procesului decizional și a profilării** - oferă posibilitatea persoanei vizate de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar întro măsură semnificativă.

În conformitate cu RGPD, atunci când se colectează date cu caracter personal de la persoana vizată, operatorul, în momentul obținerii acestor date cu caracter personal, are obligația de a furniza persoanei vizate următoarele informații[7]:

- ✓ identitatea și datele de contact ale operatorului, inclusiv datele de contact ale responsabilului cu protecția datelor (DPO/RPD), dacă există;
- ✓ scopul și temeiul juridic al prelucrării, și anume obligația legală sau contractuală;
- ✓ interesul legitim urmărit de operatorul de date, în cazul în care acesta constituie temeiul juridic al prelucrării;
- ✓ destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- ✓ dacă datele vor fi transferate către o țară terță sau o organizație internațională și dacă acest transfer se bazează pe o decizie privind caracterul adecvat al nivelului de protecție a datelor sau pe garanții adecvate;
- ✓ perioada pentru care vor fi stocate datele cu caracter personal și, dacă stabilirea acestei perioade nu este posibilă, criteriile utilizate pentru a stabili perioada de stocare;
- ✓ drepturile persoanelor vizate în ceea ce privește prelucrarea, cum ar fi dreptul de a obține acces la date, rectificarea sau

[7] Regulamentul general privind protecția datelor, articolul 13 alineatul (1).

ștergerea acestora ori restricționarea prelucrării sau dreptul de a se opune prelucrării;

- ✓ dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală, dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
- ✓ existența unui proces decizional automatizat incluzând crearea de profiluri;
- ✓ dreptul de a depune o plângere în fața unei autorități de supraveghere;
- ✓ existența dreptului de a retrage consimțământul.

3.2 Procedura de răspuns la cererile persoanelor vizate

Conform art.12 din RGPR următoarele aspecte se aplică tuturor solicitărilor persoanelor vizate:

- ✓ Informațiile trebuie oferite într-o formă concisă, transparentă și ușor accesibilă;
- ✓ Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic;
- ✓ Trebuie acționat la cererea unei persoane vizate, cu excepția cazului în care nu i se poate stabili identitatea;
- ✓ Informațiile trebuie furnizate fără întârzieri nejustificate și în termen de maxim o lună de la primirea cererii;
- ✓ Timpul de răspuns poate fi prelungit cu două luni atunci când este necesar;
- ✓ Informațiile sunt furnizate în format electronic acolo unde este posibil;
- ✓ În cazul în care nu se va da curs unei cereri, persoana vizată trebuie informată fără întârziere și cel târziu în termen de o lună, menționând motivul (motivele) și informând persoana vizată asupra dreptului de a se adresa cu o plângere Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal și/sau de a se adresa instanței de judecată;
- ✓ Răspunsurile la cererile persoanelor vizate vor fi acordate gratuit, cu excepția cazului în care acestea sunt "vădit nefondate sau excesive" (în special din cauza caracterului lor repetitiv), caz în care se poate percepe o remunerație rezonabilă (ținând cont de costurile administrative);

Procesarea cererilor persoanelor vizate trebuie tratate cu celeritate și în mod transparent. Autoritățile de management (FESI) au obligația ca operatori de a lua toate măsurile adecvate pentru a informa persoanele vizate - cu privire la modul în care își pot exercita drepturile și să trateze solicitările acestora în timp util fără întârzieri nejustificate pentru că pot risca amenzi, conform prevederilor legale în vigoare!

Tabelul următor prezintă drepturile persoanelor vizate pentru fiecare bază de prelucrare. Acesta trebuie utilizat doar ca ghid general, deoarece circumstanțele specifice pot afecta evaluarea cererii.

Dreptul persoanei vizate	**Baza legală a prelucrării**					
	Consimțământ Art. 6(a)	**Contract Art. 6(b)**	**Obligație legală Art. 6(c)**	**Interes vital Art. 6(d)**	**Interes public Art. 6(e)**	**Interes legitim Art. 6(f)**
Retragerea consimțământului	Da	Nu	Nu	Nu	Nu	Nu
Informare	Da	Da	Da	Da	Da	Da
Acces	Da	Da	Da	Da	Da	Da
Rectificare	Da	Da	Da	Da	Da	Da
Ștergere	Da	Nu	Nu	Nu	Nu	Da
Restricționarea procesării	Da	Da	Da	Da	Da	Da
Portabilitatea datelor	Da	Da	Nu	Nu	Nu	Nu
De a obiecta	N/A	Nu	Nu	Nu	Da	Da

Decizii automatizate și profilare	N/A	Nu	Nu	Da	Da	Da

4. Responsabilul cu protecția datelor cu caracter personal (Data Protection Officer - DPO)

Responsabilii cu protecția datelor cu caracter personal (DPO) sunt persoane care oferă consultanță privind respectarea normelor de protecție a datelor în cadrul organizațiilor care prelucrează date. Aceștia reprezintă „un punct de referință pentru responsabilitate", deoarece facilitează respectarea normelor, acționând în același timp ca intermediari între autoritățile de supraveghere, persoanele vizate și organizația care i-a desemnat.

Conform art. 37 alin. (5) extras din Regulamentul RGPD responsabilul cu protecţia datelor este desemnat pe baza **calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor**, precum şi **pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39**.

Responsabilul cu protecţia datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să îşi îndeplinească sarcinile în baza unui contract de servicii.

Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecţia datelor şi le comunică autorităţii de supraveghere.

Conform Art. 37(6) din RGPD, calitățile profesionale pe care trebuie să le posede un DPO sunt:

- ⇒ cunoștințe de specialitate în dreptul și practicile în domeniul protecției datelor, precum și pe baza capacității de a-și îndeplini sarcinile;
- ⇒ nivelul de expertiză necesar ar trebui determinat pe baza operațiunilor de prelucrare efectuate și a protecției necesare pentru datele cu caracter personal prelucrate. De exemplu, în

situația în care o operațiune de prelucrare a datelor este deosebit de complexă sau în cazul în care este implicat un volum mare de date speciale, DPO poate necesita un nivel mai ridicat de expertiză și suport.

Aptitudinile și expertiza relevante includ:

- **a.** experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere complexă a RGPD;
- **b.** înțelegerea operațiunilor de prelucrare efectuate;
- **c.** înțelegerea tehnologiilor de informații și de securitate a datelor;
- **d.** cunoașterea sectorului de afaceri și a organizației (societății) sau a instituției publice;
- **e.** abilitatea de a promova protecția datelor în cadrul organizației/instituției și de a forma o cultură a protecției datelor în cadrul acesteia.

Condițiile numirii DPO conform *Ghidului privind Responsabilul cu protecția datelor (DPO)* *adoptat în data de 13 decembrie 2016, Revizuit și adoptat în data de 5 aprilie 2017, emitent: GRUPUL DE LUCRU „ARTICOLUL 29" PENTRU PROTECȚIA DATELOR*:

1. **DPO-ul trebuie să fie „ușor accesibil"** pentru persoanele vizate; Noțiunea de accesibilitate se referă la sarcinile DPO ca punct de contact în ceea ce privește persoanele vizate, autoritatea de supraveghere, dar și pe plan intern în cadrul organizației/instituției, având în vedere că una dintre sarcinile DPO este *„de informare și consiliere a operatorului și persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului Regulament"*; Disponibilitatea unui DPO (fie fizică în același sediu cu angajații, fie prin intermediul unei linii telefonice sau prin alte mijloace sigure de comunicare) este esențială pentru a garanta că persoanele vizate vor fi în măsură să contacteze DPO; accesibilitatea DPO trebuie să fie efectivă: DPO trebuie să fie localizat pe teritoriul UE, chiar

dacă operatorul sau persoana împuternicită de operator nu este stabilită pe teritoriul UE;

2. **Trebuie să fie în măsură să comunice eficient** cu persoanele vizate și să coopereze cu autoritățile de supraveghere implicate;

3. **Expertiza și abilitățile DPO:**

- **Nivelul de expertiză**

Nivelul de expertiză necesar nu este strict definit, dar trebuie să fie proporțional cu sensibilitatea, complexitatea și volumul de date prelucrate de organizație/instituție. De exemplu, în situația în care o operațiune de prelucrare a datelor este deosebit de complexă sau în cazul în care este implicat un volum mare de date speciale, **DPO poate necesita un nivel mai ridicat de expertiză și suport.** Există de asemenea diferențe în măsura în care organizația/instituția transferă în mod sistematic date cu caracter personal în afara UE sau dacă aceste transferuri sunt ocazionale. Astfel, DPO ar trebui ales cu atenție, ținând seama de aspectele de protecție a datelor care apar în cadrul organizației/instituției.

- **Calitățile profesionale ale DPO**

Cu toate că art. 37(5) nu precizează calitățile profesionale care ar trebui să fie luate în considerare la desemnarea unui DPO, un element relevant ar fi ca **DPO să aibă experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere complexă a RGPD.** De asemenea, ar fi util dacă autoritățile de supraveghere ar promova o formare adecvată și regulată pentru DPO. **Este utilă cunoașterea instituției/sectorului de afaceri și a organizării operatorului**. **DPO ar trebui, de asemenea, să înțeleagă operațiunile de prelucrare efectuate, precum și sistemele de informații și necesitățile de securitate și protecție a datelor ale operatorului.**

- **DPO trebuie să aibă capacitatea de a-și îndeplini sarcinile**

Capacitatea de a-și îndeplini sarcinile ce revin DPO trebuie interpretată ca referindu-se atât la calitățile lor personale și la cunoștințe, cât și la poziția lor în cadrul organizației/instituției. Calitățile personale trebuie să includă integritatea și etica

profesională; principala preocupare a DPO trebuie să fie respectarea RGPD. DPO joacă un rol-cheie în promovarea unei culturi de protecție a datelor în cadrul organizației și ajută la implementarea elementelor esențiale al RGPD, cum ar fi principiile de prelucrare a datelor, drepturile persoanelor vizate, asigurarea protecției datelor începând cu momentul conceperii și în mod implicit, înregistrarea activităților de prelucrare, securitatea prelucrării, precum și notificarea și comunicarea încălcărilor de securitate.

- **DPO trebuie să aibă capacitatea de implicare**
  Operatorul se asigură că DPO este „implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal" și are capacitatea de a asigura această implicare. DPO sau echipa sa, trebuie să fie implicat, cât mai devreme posibil, în toate aspectele legate de protecția datelor. În ceea ce privește evaluările impactului asupra protecției datelor.

  RGPD prevede în mod explicit implicarea timpurie a DPO și precizează că operatorul solicită avizul DPO atunci când se efectuează o astfel de evaluare a impactului.

  Asigurarea că DPO este informat și consultat de la bun început va facilita respectarea RGPD, va promova o abordare pro-activă și, prin urmare, ar trebui să fie o procedură standard în cadrul fiecărei instituții. În plus, este important ca DPO să fie văzut ca un partener de discuție în cadrul organizației și ca acesta să facă parte din grupurile de lucru relevante care se ocupă cu activități de prelucrare a datelor din cadrul organizației/instituției.

DPO este invitat să participe în mod regulat la ședințele conducerii la nivel înalt și la nivel mediu.

- Prezența DPO este recomandată în cazul în care se iau decizii cu implicații asupra protecției datelor. Toate informațiile relevante trebuie să fie transmise DPO în timp util pentru a permite ca acesta să ofere o consiliere corespunzătoare.

- Avizului DPO trebuie să i se acorde întotdeauna o importanță deosebită. În caz de dezacord, WP29[8] recomandă, ca bună practică, documentarea motivelor pentru care nu a fost urmat avizul DPO.
- DPO trebuie să fie consultat cu promptitudine imediat ce a avut loc o încălcare a securității datelor sau un alt incident.

- **DPO trebuie să aibă capacitatea de a aloca timp suficient activităţii operatorului în vederea îndeplinirii atribuţiilor sale.**

Având în vedere mărimea și structura organizației, ar putea fi necesară crearea unei echipe DPO (un DPO și personalul său). În astfel de cazuri, structura internă a echipei și sarcinile și responsabilitățile fiecărui membru ar trebui să fie în mod clar elaborate.

În mod similar, atunci când funcția de DPO este exercitată de un furnizor extern de servicii, o echipă de persoane fizice care lucrează pentru respectiva entitate poate îndeplini în mod eficient sarcinile unui DPO ca o echipă, sub responsabilitatea unui punct de contact principal desemnat pentru client.

⇒ Să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent

DPO nu trebuie să fie instruit cum să se ocupe de o problemă, de exemplu, ce rezultat ar trebui atins, cum să fie investigată o plângere sau dacă să consulte autoritatea de supraveghere. Mai mult, acesta nu trebuie să fie instruit să adopte o anumită perspectivă a problemei legată de legislația privind protecția datelor, de exemplu, o anumită interpretare a legii.

⇒ Să nu existe conflict de interese

Organizația trebuie să se asigure că nicio altă atribuție a DPO „nu generează un conflict de interese”. Este strâns legată de obligația de a acționa în mod independent.

Bune practici pentru organizaţiile ce implementează fonduri FESI:

[8] WP 29 – Grupul de lucru al articolului 29/pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal

- să identifice funcțiile ce ar fi incompatibile cu funcția de DPO;
- să elaboreze norme interne în acest sens pentru a evita conflictele de interese;
- să declare că DPO-ul lor nu se află în niciun conflict de interese în ceea ce privește funcția sa ca și DPO, ca și modalitate de creștere a gradului de conștientizare a acestei cerințe;
- să includă garanții în normele interne ale organizației și să se asigure că anunțul de post vacant pentru funcția de DPO sau contractul de prestări servicii este suficient de precis și detaliat pentru a evita conflictul de interese. În acest context, trebuie avut în vedere faptul că respectivele conflicte de interese pot lua diverse forme în funcție de faptul dacă DPO este angajat intern sau furnizor extern.

În situația în care funcția DPO este exercitată de un furnizor de servicii extern, o echipă de persoane fizice angajate ale respectivei entități poate îndeplini eficient sarcinile DPO ca o echipă, sub responsabilitatea unei singure persoane desemnate ca persoană de contact principală și „persoană responsabilă" pentru client.

În această situație, **este esențial ca fiecare membru al organizației care exercită funcțiile unui DPO să îndeplinească toate cerințele aplicabile potrivit RGPD**.

RGPD prevede că desemnarea unui DPO este obligatorie în trei cazuri specifice:

- ⊕ în cazul în care o autoritate sau un organism public efectuează prelucrarea;
- ⊕ în cazul în care activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă;
- ⊕ în cazul în care activitățile principale constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal referitoare la condamnări penale și infracțiuni.

Sarcinile și atribuțiile DPO sunt detaliate la articolul 39 din RGPD. Acestea includ cerința de a informa și consilia instituția/societatea și angajații care efectuează prelucrarea cu privire la obligațiile care le revin în temeiul legislației și de a monitoriza respectarea normelor UE și naționale privind protecția datelor prin efectuarea de audituri și prin formarea personalului implicat în operațiunile de prelucrare. De asemenea, DPO trebuie să coopereze cu autoritatea de supraveghere și să acționeze ca punct de contact pentru aceasta privind aspectele legate de prelucrarea datelor, cum ar fi, de exemplu, o încălcare a securității datelor.

În ceea ce privește datele cu caracter personal gestionate de instituțiile și organele UE, Regulamentul (CE) nr. 45/2001 prevede că fiecare instituție și organism al Uniunii trebuie să desemneze un DPO.

5. Măsuri/instituții/instrumente/proceduri aplicabile la nivel național și european și interdependența lor în domeniul specific FESI

5.1 Codurile de conduită, certificarea și conformitatea RGPD

Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate contribui la demonstrarea îndeplinirii cerinței de securitate a prelucrărilor în cadrul FESI.

Recunoscând importanța acestor coduri pentru aplicarea eficace a legislației privind protecția datelor, RGPD invită statele membre, autoritățile de supraveghere, Comisia și Comitetul European pentru Protecția Datelor **să încurajeze elaborarea de coduri de conduită menite să contribuie la buna aplicare a regulamentului în întreaga UE[9].**

[9]- Regulamentul general privind protecția datelor, articolul 40 alineatul (1).

Codurile ar putea preciza modul în care se aplică regulamentul în sectoare specifice, de exemplu FESI, inclusiv aspecte precum colectarea datelor cu caracter personal, informațiile care trebuie furnizate persoanelor vizate și publicului și exercitarea drepturilor persoanelor vizate. Pentru a se asigura că prin codurile de conduită se respectă normele stabilite în RGPD, codurile trebuie prezentate autorității competente de supraveghere înainte de a fi adoptate. Autoritatea de supraveghere emite apoi un aviz cu privire la conformitatea cu regulamentul a proiectului de cod prezentat și îl aprobă în cazul în care constată că acesta oferă garanții adecvate. Autoritățile de supraveghere trebuie să publice codurile de conduită aprobate, precum și criteriile pe baza cărora au fost aprobate.

Pentru a asigura responsabilitatea în operațiunile de prelucrare a datelor cu caracter personal, operatorii și persoanele împuternicite de operatori trebuie să păstreze evidențe cu activitățile de prelucrare desfășurate sub responsabilitatea lor și să le pună la dispoziția autorităților de supraveghere, la cererea acestora.

Regulamentul general privind protecția datelor stabilește mai multe instrumente pentru promovarea conformității:

- ✓ numirea unor responsabili cu protecția datelor în anumite situații;
- ✓ efectuarea unei evaluări a impactului înainte de începerea activităților de prelucrare susceptibile să genereze riscuri ridicate pentru drepturile și libertățile persoanelor fizice;
- ✓ consultarea prealabilă a autorității de supraveghere relevante în cazul în care evaluarea impactului indică faptul că prelucrarea prezintă riscuri care nu pot fi atenuate;
- ✓ coduri de conduită pentru operatori și persoanele împuternicite de operatori care precizează modul în care se aplică regulamentul în diferite domenii de prelucrare;
- ✓ **mecanisme de certificare,** de exemplu certificarea autorităților ce gestionează FESI conform standardului ISO/IEC 27701 Securitatea datelor cu caracter personal care este o extensie a ISO/IEC 27001 care definește cerințele pentru un sistem de management al securității informației şi este aliniat cu prevederile Regulamentului European 2016/679 – RGPD.

Principiul responsabilității este deosebit de important pentru a garanta aplicarea normelor privind protecția datelor în Europa. **Operatorul este responsabil pentru respectarea normelor privind protecția datelor și trebuie să-și demonstreze conformitatea.**

5.2 Transferuri Internaţionale de date cu caracter personal

Codurile de conduită împreună cu angajamentele obligatorii și executorii, pot fi utilizate ca garanții adecvate pentru transferul datelor către țări terțe.

Pentru o cooperare eficientă în cazurile transfrontaliere, RGPD prevede că autoritatea de supraveghere a sediului principal sau a sediului unic al operatorului sau al persoanei împuternicite de operator este competentă să acționeze în calitate de autoritate de supraveghere principală[10]. **Autoritatea de supraveghere principală este responsabilă pentru cazurile transfrontaliere**, este singurul interlocutor al operatorului sau al persoanei împuternicite de operator și coordonează cooperarea cu alte autorități de supraveghere pentru a ajunge la un consens. Cooperarea include schimbul de informații și asistența reciprocă pentru monitorizare, investigare și adoptarea de decizii cu caracter obligatoriu.

Alte modalități de obținere a conformităţii sunt:

- **Un acord administrativ obligatoriu din punct de vedere juridic (numai organismele publice);**
- **Reguli corporatiste obligatorii;**
- **Utilizarea clauzelor standard în contracte;**
- **Înscrierea/ aderarea la un cod de conduită aprobat sau o schemă de certificare.**

5.3 Autoritatea de Supraveghere

Autoritatea de supraveghere este principalul organism care, în temeiul dreptului intern, asigură respectarea legislației UE privind protecția datelor. Autoritățile de supraveghere au un portofoliu cuprinzător de sarcini și competențe pe lângă monitorizare,

[10] Regulamentul general privind protecția datelor, articolul 56 alineatul (1).

care includ activități de supraveghere proactive și preventive. Pentru îndeplinirea acestor sarcini, autoritățile de supraveghere trebuie să dispună de competențe de investigare, corective și de consiliere adecvate, **astfel cum sunt enumerate în articolul 57 și 58 din RGPD**, pentru a asigura următoarele:

- ⇒ să ofere consiliere operatorilor și persoanelor vizate cu privire la toate aspectele legate de protecția datelor;
- ⇒ să autorizeze clauze contractuale standard, reguli corporatiste obligatorii sau acorduri administrative;
- ⇒ să investigheze operațiunile de prelucrare a datelor și să intervină în mod corespunzător;
- ⇒ să solicite prezentarea oricărei informații relevante pentru supravegherea activităților operatorului;
- ⇒ să emită avertizări sau mustrări adresate operatorilor și să solicite înștiințarea persoanelor vizate cu privire la încălcările securității datelor cu caracter personal;
- ⇒ să dispună blocarea accesului la date sau rectificarea, ștergerea sau distrugerea datelor;
- ⇒ să interzică temporar sau definitiv prelucrarea sau să impună amenzi administrative;
- ⇒ să sesizeze o instanță de judecată.

Potrivit Curții de Justiție a UE (CJUE), competențele autorității de supraveghere trebuie interpretate în sens larg, pentru a se asigura eficacitatea deplină a protecției datelor pentru persoanele vizate în UE.

Fiecare autoritate de supraveghere are competența de a exercita prerogative de investigare și de intervenție pe teritoriul său. Cu toate acestea, având în vedere că activitățile operatorilor și ale persoanelor împuternicite de operatori sunt deseori transfrontaliere, iar prelucrarea datelor afectează persoane vizate din mai multe state membre, se pune problema alocării competențelor între diferitele autorități de supraveghere.

5.4 Comitetul European pentru Protecția Datelor

Importanța autorităților de supraveghere independente și competențele principale atribuite acestora în temeiul legislației europene privind protecția datelor au fost descrise anterior. **Comitetul European pentru Protecția Datelor (CEPD) este un alt actor**

important pentru asigurarea aplicării eficiente și consecvente a normelor de protecție a datelor în întreaga UE.

RGPD a instituit CEPD ca organ al UE cu personalitate juridică[11].Acesta este succesorul Grupului de lucru „Articolul 29", instituit de Directiva privind protecția datelor pentru a consilia Comisia cu privire la orice măsuri ale UE care afectează drepturile persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și respectarea vieții private, pentru a promova aplicarea uniformă a directivei și pentru a furniza expertiză Comisiei cu privire la aspectele legate de protecția datelor.

5.5 Răspundere și penalități la nivel național privind RGPD

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

Încălcarea dispozițiilor enumerate la art. 83 alin. (4)-(6) din Regulamentul general privind protecția datelor constituie contravenție.

Sancțiunile contravenționale principale sunt avertismentul și amenda contravențională.

Încălcarea prevederilor art. 3-9 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare, constituie contravenție și se sancționează în condițiile prevăzute la art. 83 alin. (5) din Regulamentul general privind protecția datelor.

[11]Regulamentul general privind protecția datelor, articolul 68.

Constatarea contravențiilor prevăzute de lege și aplicarea sancțiunilor contravenționale, precum și a celorlalte măsuri corective prevăzute de art. 58 din Regulamentul general privind protecția datelor se fac de Autoritatea națională de supraveghere, în conformitate cu dispozițiile Regulamentului general privind protecția datelor, ale Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările și completările ulterioare.

Autoritatea națională de supraveghere, în funcție de circumstanțele fiecărui caz în parte, poate aplica sancțiunea contravențională a amenzii, cu luarea în considerare a criteriilor prevăzute la art. 83 alin. (2) din Regulamentul general privind protecția datelor.

Constituie contravenție încălcarea de către autoritățile/ organismele publice a următoarelor dispoziții din Regulamentul general privind protecția datelor, referitoare la: a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu prevederile art. 8, art. 11, art. 25-39, art. 42 și 43;b) obligațiile organismului de certificare în conformitate cu art. 42 și 43;c) obligațiile organismului de monitorizare în conformitate cu art. 41 alin. (4). Constituie contravenție încălcarea de către autoritățile/organismele publice a dispozițiilor art. 3-9 din prezenta lege în vigoare, Legea nr. 190/ 2018 cu modificările ulterioare.

Contravențiile prevăzute la art. 14 alin. (2) și (3) din Legea nr. 190/ 2018, cu modificările ulterioare, se sancționează cu amendă de la 10.000 lei până la 100.000 lei.

Constituie contravenție încălcarea de către autoritățile/organismele publice a următoarelor dispoziții din Regulamentul general privind protecția datelor, referitoare la:a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu art. 5-7 și art. 9; b) drepturile persoanelor vizate în conformitate cu art. 12-22;c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu art. 44-49;d) orice obligații în temeiul legislației naționale adoptate în temeiul capitolului IX; e) nerespectarea unei decizii sau a unei limitări temporare sau definitive asupra prelucrării sau a suspendării fluxurilor de date, emisă

de către Autoritatea națională de supraveghere în temeiul art. 58 alin. (2), sau neacordarea accesului, prin încălcarea dispozițiilor art. 58 alin. (1).

Constituie contravenție încălcarea de către autoritățile/ organismele publice a unei decizii emise de Autoritatea națională de supraveghere în conformitate cu art. 58 alin. (2) coroborat cu art. 83 alin. (2) din Regulamentul general privind protecția datelor.

Prin derogare de la prevederile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, **contravențiile prevăzute la art. 14 alin. (7) se sancționează cu amendă de la 10.000 lei până la 200.000 lei.**

Considerentul (45) din RGPD precizează: "În cazul în care prelucrarea este efectuată în conformitate cu o obligaţie legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care face parte din exercitarea autorităţii publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existenţa unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operaţiuni de prelucrare efectuate în conformitate cu o obligaţie legală a operatorului. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern.

5.6 Managementul riscurilor de protecție a datelor cu caracter personal în domeniul FESI

O abordare sistematică a managementului riscului de protecție a datelor cu caracter personal este necesară pentru a identifica necesitățile organizaționale FESI privind cerințele de protecție a datelor cu caracter personal și pentru a crea un sistem eficace de gestionare a securității informației prelucrate în cadrul diverselor programe operaționale.

Din punct de vedere al asigurării protecției datelor cu caracter personal au fost identificate trei riscuri care se vor analiza în continuare:

- Accesul neautorizat (nelegitim) la datele cu caracter personal
- Modificarea nedorită (neautorizată) a datelor cu caracter personal;
- Dispariția (distrugerea) datelor cu caracter personal.
- Tipul surselor ce pot genera riscuri:
- Sursa umană internă – angajați, operatori, specialiști IT&C, manageri;
- Sursa umană externă – destinatari ai datelor cu caracter personal, terțe părți autorizate, furnizori de servicii, vizitatori, foști angajați, colaboratori, beneficiari, hackeri;
- Surse neumane – viruși (malware), apa (conducte, inundații), substanțe inflamabile, corozive, explozive, dezastre naturale, epidemii.
- Acțiuni ce pot conduce la materializarea riscurilor:
- Accesul neautorizat (nelegitim) – utilizarea frauduloasă, observarea, spionaj, pierdere, manipulare;
- Modificarea nedorită (neautorizată) alterare, utilizare anormală, supraîncărcare, manipulare;
- Dispariția (distrugerea) utilizare anormală, supraîncărcare, alterare, distrugere, pierdere .

5.7 Măsuri tehnice şi organizaționale aplicabile FESI

Controlul admiterii/accesului fizic

În cadrul Regulilor cu privire la Datele cu Caracter Personal se impune "…prevenirea accesului persoanelor neautorizate la sistemele în cadrul cărora datele cu caracter personal sunt procesate sau întrebuințate" (controlul privind accesul).

Termenul de "admitere" se referă la accesul fizic al persoanelor în clădirile și sediile în care sunt operate și utilizate sisteme IT. Acestea pot fi, de exemplu, centre de computere unde sunt operate servere web, servere de aplicații, baze de date, unități centrale şi sisteme de stocare și birouri în care angajații utilizează computere desktop. Sunt incluse aici şi sediile unde sunt amplasate și dispuse componente şi cabluri de rețea.

Propunem identificarea unor măsuri organizatorice de protejare a stocării, procesării şi arhivării documentelor ce conţin date cu caracter personal (de ex. vitrare specială, sisteme de detectare a intruşilor, turnicheţi operati cu carduri cu chip, sisteme de acces securizate pentru o singură persoană, sistem de încuiere) sau măsuri organizaţionale (de ex. agenţi de protecţie şi pază) vor fi luate pentru a proteja zonele de securitate şi punctele de acces ale acestora împotriva pătrunderii persoanelor neautorizate.

Cerinţele pentru autorizaţia generală de acces, precum şi grupul persoanelor care o deţin trebuie definite, iar autorizaţiile de acces în zonele de securitate relevante trebuie limitate ("principiul autorizării minimale"). Accesul va fi interzis oricărei persoane fără autorizaţie.

Vor fi descrise regulile şi procedurile pentru blocarea autorizaţiilor de acces. În cazul în care o persoană părăseşte instituţia sau se mută într-un alt departament, toate mijloacele de acces şi autorizaţiile de acces către toate locaţiile care nu mai sunt necesare pentru îndeplinirea atribuţiilor respectivei persoane vor fi returnate/revocate imediat. Toate persoanele cărora li se încredinţează atribuţii legate de securitate, în special atribuţii de securitate a căilor de acces, vor fi informate cu privire la angajaţii care au părăsit instituţia sau ale căror atribuţii s-au schimbat. Autorităţile centrale şi locale care implementează fonduri europene, FESI vor trebui să-şi elaboreze proceduri de lucru adecvate care să asigure prevenirea utilizării de către persoane neautorizate a sistemelor de procesare a datelor care stochează, procesează sau folosesc date cu caracter personal.

Controlul accesului la date

În cadrul Regulilor cu privire la Datele cu Caracter Personal se impune "…asigurarea faptului că sistemele de procesare a datelor nu pot fi folosite de persoane neautorizate" (controlul privind refuzul la utilizare).

Parolele trebuie schimbate la intervale regulate. Parolele iniţiale trebuie schimbate imediat. Implementarea cerinţelor privind lungimea

parolelor, complexitatea şi valabilitatea parolelor va fi asigurată prin setări tehnice.

- Parola trebuie să conţina cel puţin 8 caractere.
- Parola trebuie să conţină o combinaţie de caractere. Caracterele disponibile se împart în patru categorii:
- Litere mici, precum abcdefgh...
- Litere mari, precum ABCDEFGH...
- Cifre, precum 123456...
- Caractere speciale, precum !“§$%...
- Combinaţia de caractere trebuie să conţină cel puţin trei dintre categoriile indicate mai sus.
- Cuvinte uşor de ghicit şi parole banale nu vor putea fi utilizate ca parole.
- Parolele vor fi schimbate la intervale regulate.
- La schimbarea parolelor, niciuna dintre ultimele 4 parole nu poate fi refolosită.
- Parolele nu vor fi vizibile în text lizibil pe ecran la momentul tastării.
- Parolele iniţiale trebuie furnizate utilizatorului prin canale securizate şi/sau utilizatorului trebuie cel puţin să i se ceară să schimbe parola imediat după prima autentificare.

În cadrul Regulilor cu privire la Datele cu Caracter Personal se impune “…asigurarea faptului că persoanele autorizate pentru folosirea sistemelor de procesare a datelor au posibilitatea de a accesa în mod exclusiv datele la care acestea au acces autorizat şi a faptului că datele cu caracter personal nu pot, cu ocazia procesării, întrebuinţării sau ulterior înregistrării, să fie citite, copiate, modificate sau şterse de persoane neautorizate” (controlul accesului la date).

Cerinţele privind controlul accesului la date au rolul de a permite doar persoanelor autorizate să acceseze datele pe care sunt autorizate să le acceseze şi să prevină manipularea sau citirea datelor de către persoane neautorizate.

Controlul tranzitării datelor

În cadrul Regulilor cu privire la Datele cu Caracter Personal se impune “…asigurarea faptului că, în cursul transmiterii electronice sau cu ocazia transportului sau înregistrării pe suporturi de date, datele cu

caracter personal nu pot fi citite, copiate, modificate sau șterse de către persoane neautorizate și a faptului că este posibilă verificarea și identificarea operatorilor spre care sunt transmise datele cu caracter personal prin intermediul echipamentului de transmitere a datelor" (controlul asupra transmiterii datelor).

Stabilirea instanțelor/persoanelor autorizate să primească/transmită date

Operatorul trebuie să decidă ce organizații/persoane au dreptul de a trimite date precum și calea specifică de transmitere în acest sens.

Legalitatea transmiterii către alte țări/ Transmiterea către sisteme externe

În cazul în care datele personale sunt transmise către sisteme externe, este absolut necesară criptarea acestora inclusiv pentru schimburile de mailuri cu atașamente conținând date cu caracter personal.

Implementarea de căi de acces securizate la punctele de transfer ale rețelei

Sistemele IT/NT pe care sunt procesate datele personale vor fi protejate împotriva accesului neautorizat sau scurgerii de date atât din aceeași rețea, cât și din alte rețele, utilizând măsurile cele mai performante (de regulă, firewalls). Indiferent dacă aceste firewalls sunt implementate la nivel de rețea/echipament sau dacă sunt utilizate și firewalls la nivel local, acestea trebuie activate permanent. Trebuie luate măsurile pentru prevenirea efectivă a oricărei forme de dezactivare sau ocolire a funcțiilor de către utilizatori. Regulile trebuie stabilite astfel încât orice legătură de comunicare să fie blocată automat.

Întărirea sistemelor back-end

Sistemele back end trebuie întărite cu cea mai performantă tehnologie pentru a preveni accesarea neautorizată a sistemelor și datelor de către atacatori ca urmare a vulnerabilităților.

Descrierea tuturor interfețelor și a câmpurilor transmise conținând date cu caracter personal

Toate interfețele către alte procese IT vor fi documentate. Această documentare trebuie să conțină cel puțin următoarele informații:

- Toate câmpurile conținând date cu caracter personal
- Direcţia transmiterii (import/export)
- Scopul respectiv al transmiterii
- Procesele/interfața IT către care sunt exportate datele
- Tipul de autentificare utilizată de către interfață
- Protecția transmiterii (de ex. criptare)

În special interfețele de import şi export de la şi către fișiere trebuie descrise, alături de modul de protejare a utilizării lor prin măsuri tehnice sau organizaționale. Vor fi de asemenea descrise ca interfețe migrările de date.

Stocarea securizată a datelor

Pentru stocarea securizată a datelor personale cu cel mai înalt grad de protecție, va fi furnizat un sistem criptat de stocare a datelor. Aceasta se aplică şi oricăror backup-uri.

Stocarea securizată pe mediile de date mobile

Stocarea datelor pe medii mobile ar trebui evitată din pricina riscului înalt de pierdere. Totuși, în cazul în care stocarea datelor pe astfel de medii nu poate fi evitată, utilizarea acestora va fi controlată, iar pentru datele stocate acolo, criptarea va fi asigurată tehnic în mod automat. Toate datele care nu mai sunt necesare trebuie șterse imediat în conformitate cu regulile de protecție a datelor. Echipamentele utilizate vor fi de asemenea protejate împotriva pierderii/furtului (prin folosirea cablurilor de Securitate, containere de transport corespunzătoare etc.).

Procesul de colectare şi eliminare

Trebuie stabilit şi descris un proces pentru colectarea, eliminarea, distrugerea sau ștergerea mediilor de date sau mediilor de informare ne-electronice. Autoritățile FESI trebuie să elaboreze reguli şi proceduri pentru colectarea securizată şi transmiterea internă, precum şi pentru stocarea şi distrugerea mediilor care trebuie descrise într-o politică/proces organizațional, având în vedere proprietățile specifice mediilor respective. Distrugerea sau ștergerea mediilor de date în conformitate cu regulile de protecție a datelor va fi realizată

la stația de lucru la timp, pentru evitarea stocării temporare a mediilor. Aceasta limitează numărul persoanelor care manipulează mediile de date şi sporește gradul de securitate. Vor fi luate măsuri organizaționale pentru evitarea metodelor alternative de eliminare. Angajații vor fi informați în acest sens în mod regulat.

Introducerea metodelor de ștergere şi distrugere în conformitate cu reglementările de protecție a datelor

Din motive de securitate, mediile de date criptate trebuie șterse în conformitate cu regulile de protecție a datelor înainte de a fi refolosite intern (de ex. schimbarea utilizatorului primar) sau transferate unor părți externe. Formatarea este nepotrivită ca metodă sigură de ștergere. Alte metode sigure de ștergere/distrugere trebuie selectate, care să facă extrem de dificilă reconstituirea datelor.

Transmiterea mediilor de date

Din motive de securitate, datele necriptate trebuie șterse întotdeauna în conformitate cu regulile de protecție a datelor înainte de a fi transmise către organizații externe.

Medii detașabile (removable)

Este interzisă conectarea mediilor de date externe (detașabile) (USB, carduri de memorie, CD/DVD etc.) la sistemele de procesare a datelor ale persoanelor vizate, precum şi copierea datelor persoanelor vizate la medii de date externe (detașabile), cu excepția cazului în care aceasta este parte explicită a îndeplinirii îndatoririi şi a fost aprobată de către conducerea instituției.

Controlul disponibilității

În cadrul Regulilor cu privire la Datele cu Caracter Personal se impune "…asigurarea faptului că datele cu caracter personal sunt protejate împotriva distrugerii accidentale sau pierderii" (controlul privind disponibilitatea).

Operatorul trebuie notificat cât mai curând posibil cu privire la orice perturbare (precum atacuri intenționate interne sau externe) sau oprire a lucrărilor de procesare a datelor. În cazul în care sunt identificate semnele unei perturbări, trebuie acționat imediat pentru limitarea pagubelor şi evitarea producerii altora. În acest scop, trebuie

realizat un plan de urgenţă, care să identifice măsurile ce trebuie luate şi persoanele care trebuie notificate cu privire la incident, în special cele din partea Operatorului.

Controlul scopului utilizării

În cadrul Regulilor cu privire la Datele cu Caracter Personal se impune "…asigurarea faptului ca datele cu caracter personal care au fost colectate pentru diferite scopuri pot fi procesate separat" (regula separării).

Limitarea la minim a volumului de date colectate

Vor fi colectate, stocate sau procesate doar datele esențiale care servesc în mod direct scopului concret, realizării lucrărilor. Acest scop nu poate fi modificat pe parcursul niciunuia dintre pașii ulteriori ai procesului, inclusiv după transmitere.

Controlul organizațional

Implementarea măsurilor de instruire

Toate persoanele care lucrează cu date personale sau care sunt în alt mod implicate în implementarea FESI trebuie instruite în mod verificabil în următoarele domenii:

- Principiile protecției datelor, inclusiv măsurile tehnice şi organizaţionale
- Cerința de a păstra secretul datelor şi confidențialitatea
- Utilizarea corectă, atentă a datelor, mediilor de date şi a altor documente
- Secretul telecomunicațiilor
- Alte informații specifice care pot rezulta din contractele semnate din FESI.

Separarea funcțiilor trebuie definită, documentată şi explicată, şi anume ce funcții nu pot fi combinate între ele şi astfel nu pot fi exercitate de către aceeași persoană în același timp.

Pentru toate procesele de stabilit o perioadă determinată de stocare a datelor cu caracter personal.

Regulamentul interzice transferul de date cu caracter personal în afara UE către un stat terț care nu are instituite măsuri adecvate de protecție a datelor. Comisia Europeană are competența de a aproba

anumite state în privința gradului de protecția a datelor oferit de acestea, luând în considerare legislația în vigoare referitoare la protecția datelor din statul respectiv precum și angajamentele internaționale ale acestuia.

Pentru transferul de date către orice stat nemenționat pe listă, trebuie să se încheie un contract în care se stipulează faptul că destinatarul non-UE consimte la măsurile obligatorii de protecție a datelor. Regulamentul recunoaște și promovează în mod explicit utilizarea regulilor corporatiste obligatorii drept un mecanism valabil de transfer de date.

6. Conformitatea cu RGPD a instituției publice

6.1 Principiul responsabilității și suportul managerial

Având în vedere numeroasele modalități posibile de organizare a instituţiilor publice, **articolul 6 alineatul (1) litera (e) din RGPD prevede că datele cu caracter personal pot fi prelucrate în mod legal dacă prelucrarea „este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul”.**

Operatorii pot asigura respectarea acestei cerințe în diverse moduri, printre care:

- ✓ păstrarea unor evidențe cu activitățile de prelucrare și punerea acestora la dispoziția autorității de supraveghere, la cererea acesteia;
- ✓ în anumite situații, desemnarea unui responsabil cu protecția datelor care să fie implicat în toate aspectele legate de protecția datelor cu caracter personal;
- ✓ efectuarea unor evaluări ale impactului asupra protecției datelor pentru tipurile de prelucrare care ar putea genera un risc ridicat pentru drepturile și libertățile persoanelor fizice;
- ✓ asigurarea protecției datelor din faza de proiectare și a protecției implicite a datelor;
- ✓ punerea în aplicare a unor metode și proceduri prin care persoanele vizate să își poată exercita drepturile;
- ✓ aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate.

Prin urmare, PRINCIPUL RESPONSABILITĂȚII impune operatorilor obligația de a demonstra în mod activ conformitatea, fără să aștepte ca persoanele vizate sau autoritățile de supraveghere să semnaleze deficiențele.

Singurul rol care este explicit mandatat în RGPD este acela al Responsabilului pentru protecția datelor (DPO).

6.2 Conștientizarea importanței RGPD, asigurarea confidențialității și securității datelor, secretul profesional și formarea angajaților

❖ **Confidențialitatea datelor**

Potrivit articolului 5 alineatul (1) litera (f) din RGPD, datele cu caracter personal trebuie să fie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, **inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).** Obligația de confidențialitate nu se extinde asupra situațiilor în care datele sunt aduse la cunoștința unei persoane în calitatea acesteia de persoană fizică, nu de angajat al unui operator sau al unei persoane împuternicite de operator.

În acest caz, articolele 32 și 28 din RGPD nu se aplică, întrucât utilizarea datelor cu caracter personal de către persoane fizice este exceptată integral de la aplicabilitatea regulamentului în cazul în care o astfel de utilizare se încadrează în limitele așa-numitei excepții privind activitățile domestice[12].

Pentru **persoanele împuternicite** de operatori, confidențialitatea înseamnă că nu pot divulga datele unor părți terțe sau altor destinatari fără autorizație.

În cazurile în care are loc o încălcare a securității datelor cu caracter personal, RGPD impune operatorului să comunice autorității de supraveghere competente, fără întârzieri nejustificate, faptul că a avut loc o încălcare care generează riscuri pentru drepturile și libertățile persoanelor. Se prevede o obligație similară de comunicare, către persoana vizată, în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile respectivei persoane. Comunicarea acestor încălcări persoanelor vizate trebuie să folosească un limbaj clar și simplu. Dacă persoana împuternicită de operator ia cunoștință de o încălcare a securității datelor cu caracter personal, trebuie să

[12]Regulamentul general privind protecția datelor, articolul 2 alineatul (2) litera (c).

informeze imediat operatorul. În anumite situații, se pot aplica excepții de la obligația de notificare. De exemplu, operatorul nu are obligația de a anunța autoritatea de supraveghere atunci când „încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice”.

❖ **Securitatea datelor**

În cazul în care există un risc deosebit de încălcare a securității rețelei publice de comunicații FESI, de exemplu MySMIS, operatorii trebuie să informeze utilizatorii cu privire la acest risc. Dacă, în pofida măsurilor de securitate puse în aplicare, se produce o încălcare a securității, operatorii trebuie să notifice încălcarea securității datelor cu caracter personal autorității naționale competente.

Confidențialitatea comunicațiilor necesită interzicerea, în principiu, a ascultării, interceptării, stocării sau a oricărui tip de supraveghere sau interceptare a comunicațiilor și a metadatelor. De asemenea, directiva interzice comunicațiile nesolicitate (denumite adesea „spam”), cu excepția cazului în care utilizatorii și-au dat acordul pentru primirea acestora, și conține norme privind stocarea modulelor„cookie” pe computere și dispozitive.

❖ **Secretul profesional**

În conformitate cu legislația națională, **anumite comunicări pot face obiectul secretului profesional**.

Secretul profesional poate fi înțeles ca o datorie etică specială care implică o obligație juridică inerentă anumitor profesii și funcții care se bazează pe încredere. Persoanele și instituțiile care îndeplinesc aceste funcții au obligația de a nu divulga informațiile confidențiale pe care le primesc în cursul îndeplinirii îndatoririlor lor.

Secretul profesional nu este un drept fundamental, dar este protejat ca o formă a dreptului la respectarea vieții private.

Pe de altă parte, obligațiile de păstrare a secretului profesional impuse operatorilor și persoanelor împuternicite de operatori cu privire la anumite date cu caracter personal pot restrânge drepturile persoanelor vizate, în special dreptul de a primi informații.

❖ **Identificarea nevoilor de formare in domeniul RGPD**

La nivel instituțional/ organizațional trebuie să identificați nevoile de formare ale persoanelor care îndeplinesc diferite roluri în obținerea conformității cu RGPD. Acest lucru se poate face prin definirea competențelor necesare și efectuarea unui exercițiu de verificare prin intermediul unui chestionar, dar și prin organizarea de cursuri, seminarii, ateliere de lucru, studii de caz, și bineînțeles, asimilarea și parcurgerea în mod constant a Regulamentului. Practica curentă arată că este nevoie de instruire în domenii precum cartografierea datelor, evaluarea impactului protecției datelor, dar și în ceea ce priveste gestionarea incidentelor de securitate.

6.3 Cartografierea prelucrărilor de date cu caracter personal

Toți operatorii din sistemul public, persoanele împuternicite de operator, au obligația cartografierii prelucrărilor de date cu caracter personal efectuate, raportat la prevederile art. 30 din Regulamentul General privind Protecția Datelor.

În acest sens: Pentru a evalua în mod eficient impactul RGPD/GDPR asupra activității entității publice este necesară identificarea prelucrărilor de date cu caracter personal efectuate și păstrarea evidenței activităţilor de prelucrare.

Pentru a avea o evidență completă și exactă a prelucrărilor de date cu caracter personal efectuate și pentru a răspunde noilor exigențe, trebuie identificate, în prealabil, cu precizie:

- diferitele prelucrări de date cu caracter personal;
- categoriile de date cu caracter personal prelucrate;
- scopurile urmărite prin operaţiunile de prelucrare a datelor;
- persoanele care prelucrează aceste date;
- fluxurile de date, indicând originea și destinația datelor, în special pentru a identifica eventualele transferuri de date în afara Uniunii Europene.

Evidența păstrată de operator va cuprinde:

(a) numele și datele de contact ale operatorului și, după 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, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf din Regulamentul General privind Protecția Datelor, documentația care dovedește existența unor garanții adecvate;

(f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

(g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de Securitate menționate la articolul 32 alineatul (1) din Regulamentul General privind Protecția Datelor.

Ca atare, pentru fiecare prelucrare de date cu caracter personal, este necesar a se avea în vedere urmatoarele:

CINE?

Se înscriu în evidență numele și coordonatele operatorului (și ale reprezentantului său legal) și, după caz, ale responsabilului cu protecția datelor;

Se întocmește lista persoanelor împuternicite, după caz.

CE?

Se identifică categoriile de date cu caracter personal prelucrate;

Se identifică datele susceptibile de a prezenta riscuri datorită naturii lor sensibile deosebite (datele privind sănătatea sau infracțiunile)

DE CE?

Se precizează scopul sau scopurile în care sunt colectate sau prelucrate datele cu caracter personal (ex. gestionarea relației comerciale, managementul resurselor umane, geolocalizare, videosupraveghere etc.)

UNDE?

Se stabilește locația sistemului de evidență și, dacă e cazul, destinatarii datelor.

Se stabilesc statele către care sunt, eventual, transferate datele.

PÂNĂ CÂND?

Se precizează, pentru fiecare categorie de date, perioada de stocare.

CUM?

Se precizează măsurile de securitate implementate pentru a reduce la minimum riscurile de acces neautorizat la date și, în consecință, impactul asupra vieții private a persoanelor vizate.

Orice operațiune FESI care implică prelucrarea datelor cu caracter personal poate intra sub incidența normelor de protecție a datelor și poate face obiectul dreptului la protecția datelor cu caracter personal. De exemplu, în cazul în care un angajator înregistrează informații referitoare la numele și remunerația plătită angajaților, simpla înregistrare a acestor informații nu poate fi considerată ca fiind o ingerință în viața privată. O astfel de ingerință ar putea fi însă invocată dacă, de exemplu, angajatorul a transferat informațiile cu caracter personal ale angajaților către părți terțe. Angajatorii trebuie să respecte în orice situație normele de protecție a datelor, **deoarece înregistrarea informațiilor despre angajați constituie o operațiune de prelucrare a datelor.**

Prelucrarea datelor cu caracter personal trebuie să urmarească un scop legitim!

Scopul legitim poate fi oricare dintre interesele publice numite sau protejarea drepturilor și libertăților celorlalți. Scopurile legitime care ar putea justifica o intervenție sunt, potrivit articolului 8 alineatul (2) din Convenția europeană a drepturilor omului, **interesele securității naționale, siguranței publice sau bunăstării economice a unei țări, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei și protecția drepturilor și libertăților altor persoane.**

Inventarul datelor cu caracter personal descrie/conține datele care au fost prelucrate, scopul, metoda prelucrării, durata stocării, persoana vizată, destinatarul, termenele limită preconizate, descrierea generală a măsurilor tehnice și organizatorice de securitate menționate la art. 32 alin. (1) din RGPD.

Inventarul datelor oferă suport oricăror măsuri suplimentare care trebuie aplicate (cum ar fi criptarea) sau stabilirea temeiului

juridic pentru care datele pot fi colectate și prelucrate (de exemplu: consimțământ/ contractual). Se recomandă să se utilizeze un formular inventar al datelor cu caracter personal pentru a capta o imagine de ansamblu a tuturor datelor personale pe care le deții, cât și pentru a documenta circuitul datelor personale atât în interiorul cât și în exteriorul instituției/ organizației dvs.

Abordarea globală pe care ați decis să o luați în ceea ce privește păstrarea datelor poate fi reflectată în politica de păstrare a înregistrărilor.

6.4 Evaluarea impactului asupra protecției datelor

Articolul 35 „Evaluarea impactului asupra protecției datelor-DPIA":
„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 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".

Acesta este un domeniu relativ nou pentru multe organizații, dar este în mod explicit impus de RGPD. Proiectele noi, de exemplu o aplicație IT sau schimbările semnificative ale proceselor existente, de ex. MySMIS, vor trebui să ia în considerare impactul asupra datelor cu caracter personal ("DPIA") ca parte a evaluării și planificării acestora, cu instituirea unor controale adecvate, pe baza unei evaluări corecte a riscului.

RGPD instituie că elaborarea DPIA este necesară numai în cazul în care există un risc ridicat.

6.5 Persoane vizate în contextul RGPD

În dreptul UE, persoanele fizice sunt singurii beneficiari ai normelor de protecție a datelor și numai persoanele în viață sunt protejate în temeiul legislației UE privind protecția datelor[13].

Mai multe informații au fost furnizate la Capitolul 3.

Persoanele vizate nu dețin un drept general de a se opune prelucrării datelor lor[14]. Articolul 21 alineatul (1) din RGPD dă dreptul persoanei vizate să formuleze obiecții pentru motive legate de situația sa particulară atunci când temeiul juridic al prelucrării este îndeplinirea de către operator a unei sarcini care servește unui interes public sau dacă prelucrarea se bazează pe interesele legitime ale operatorului; Dreptul la opoziție se aplică activităților de creare de profiluri.

Asigurați-vă că permiteți ca drepturile persoanei vizate să fie exercitate fără obstacole. Acest fapt reprezintă un factor important în respectarea normelor RGPD și este de natură să atragă atenția autorității de supraveghere dacă acest lucru nu este efectuat în mod corespunzător. Deși oferim un formular în cadrul evaluării, cel mai eficient mod de a permite persoanei vizate să acceseze și să păstreze datele personale este prin intermediul unui portal pe care utilizatorul să îl poată accesa via internet, în mod direct.

În mod similar, formularele standard pot fi furnizate prin intermediul unui astfel de portal pentru solicitări precum obiecții și restricții de procesare. Va trebui să vă asigurați că aveți fluxul de lucru adecvat din spatele formularelor pentru a vă asigura că sunt înregistrate corect, că sunt procesate de persoanele potrivite în

[13]Considerentul 27. Vezi, de asemenea, Avizul 4/2007 al Grupului de lucru „Articolul 29" privind conceptul de date cu caracter personal, WP 136, 20 iunie 2007, p. 22.

[14]Vezi, de asemenea, Hotărârea CEDO din 27 august 1997 în cauza M.S./Suedia, nr. 20837/92 (în care datele medicale au fost comunicate fără consimțământ sau posibilitatea de opoziție); Hotărârea CEDO din 26 martie 1987 în cauza Leander/Suedia, nr. 9248/81; Hotărârea CEDO din 10 mai 2011 în cauza Mosley/Regatul Unit, nr. 48009/08.

intervalul de timp necesar și că identitatea solicitantului este confirmată.

Ținând cont că unele solicitări vor necesita asumarea deciziilor va fi necesar să definiți o procedură de răspuns la cererile persoanelor vizate.

De asemenea, va trebui să luați în considerare cel mai bun mod de a comunica persoanei vizate **notificarea dvs.** privind confidențialitatea, asigurându-vă că acoperă informațiile solicitate de RGPD.
Cele mai bune moduri de a face acest lucru depind de modul în care interacționați cu persoanele vizate (de ex. prin Internet, telefon, față în față)!

6.6 NOTIFICAREA privind încălcarea securității datelor cu caracter personal

Încălcarea securității datelor cu caracter personal înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a datelor cu caracter personal sau la accesul neautorizat la acestea[15] **și conduce la furt de identitate sau la fraudă, la pierderi financiare sau daune materiale, la pierderea confidențialității datelor cu caracter personal protejate prin secretul profesional și la prejudicierea reputației persoanei vizate**. În Orientările privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, Grupul de lucru „Articolul 29" explică faptul că încălcările pot avea trei tipuri de impact asupra datelor cu caracter personal: divulgarea, pierderea și/sau modificarea.

[15] Regulamentul general privind protecția datelor, articolul 4 punctul 12; vezi, de asemenea, Orientările din 3 octombrie 2017 ale Grupului de lucru „Articolul 29" privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679, WP 250, Bruxelles, 3 octombrie 2017, p. 8.

Dreptul UE stabilește un regim detaliat care reglementează termenul de transmitere și conținutul notificărilor[16]. Astfel, operatorii trebuie să notifice autorităților de supraveghere încălcarea securității datelor fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la momentul în care au luat cunoștință de încălcare. În cazul în care se depășește termenul de 72 de ore, notificarea trebuie să fie însoțită de o explicație privind întârzierea. Operatorii sunt scutiți de obligația de notificare numai în cazul în care pot demonstra că încălcarea securității datelor nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor în cauză.

- **Formularul notificării**

Notificarea trebuie să cuprindă cel puțin o descriere a caracterului încălcării securității datelor și a categoriilor și a numărului aproximativ al persoanelor vizate afectate, o descriere a posibilelor consecințe ale încălcării și a măsurilor luate de operator pentru a remedia problema și a atenua consecințele acesteia. În plus, trebuie furnizate numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact, pentru a permite autorității de supraveghere competente să obțină informații suplimentare, dacă este necesar.

În cazul în care încălcarea securității datelor este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorii trebuie să informeze aceste persoane (persoanele vizate), fără întârzieri nejustificate, cu privire la încălcare. Măsurile întreprinse de operator după producerea încălcării prin care se asigură că riscul pentru drepturile persoanelor vizate nu mai este susceptibil să se materializeze pot constitui, de asemenea, un temei pentru scutirea operatorului de obligația de a notifica încălcarea securității datelor persoanelor vizate.

În sfârșit, dacă notificarea ar necesita un efort disproporționat din partea operatorului, persoanele vizate pot fi informate despre încălcare prin alte mijloace, de exemplu printr-o informare publică sau prin măsuri similare.

[16]Regulamentul general privind protecția datelor, articolele 33 și 34.

Obligația de informare a autorităților de supraveghere și a persoanelor vizate cu privire la încălcările securității datelor le aparține operatorilor. Cu toate acestea, pot apărea încălcări ale securității datelor indiferent dacă prelucrarea este efectuată de un operator sau de o persoană împuternicită de operator. Din acest motiv, este esențial să se asigure faptul că și persoanele împuternicite de operatori au obligația de a raporta încălcările securității datelor.

O procedură adecvată și testată de gestionare a incidentelor este o necesitate. RGPD insistă asupra faptului că autoritatea națională de supraveghere trebuie să fie informată cu privire la încălcările care reprezintă un risc ridicat pentru persoanele vizate și specifică cu privire la termenele și informațiile care trebuie furnizate.

6.7 Evidența activității de prelucrare

Evidența trebuie să cuprindă următoarele informații:

- ⇒ numele și datele de contact ale operatorului și ale operatorului asociat, ale reprezentantului operatorului și ale DPO, după caz;
- ⇒ scopurile prelucrării;
- ⇒ descrierea categoriilor de persoane vizate și a categoriilor de date cu caracter personal prelucrate;
- ⇒ informații privind categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal;
- ⇒ informații care să indice dacă s-au efectuat sau se vor efectua transferuri de date cu caracter personal către o țară terță sau o organizație internațională;
- ⇒ acolo unde este posibil, termenele limită preconizate pentru ștergerea diferitelor categorii de date, precum și o descriere generală a măsurilor tehnice adoptate pentru a asigura securitatea prelucrării.

Autoritatea de supraveghere ar putea oricând să solicite să consulte înregistrările privind prelucrarea datelor cu caracter personal pe care le efectuați, așadar este important **să păstrați un istoric al prelucrărilor informațiilor principale, dar trebuie să fiți conștienți și de înregistrările cum ar fi jurnalele și traseele de audit care există la un nivel inferior, reflectând detaliile a ceea ce s-a făcut atunci.**

Imaginea completă în scopuri RGPD va consta într-o gamă largă **de elemente, cum ar fi evaluările impactului protecției datelor,** notificările privind confidențialitatea, registrele, etc., care reflectă împreună cât de importantă este protecția datelor cu caracter personal în cadrul organizației. Acest lucru va deveni deosebit de important în cazul unei încălcări a datelor atunci când autoritatea de supraveghere va decide asupra nivelului de sancțiune care ar putea fi adecvată.

6.8 Revizuirea transferurilor internaționale

Pe lângă protejarea datelor personale din cadrul organizației proprii, aveți nevoie să analizați locația/ destinatarul datelor și cum este asigurată protecția acolo. Primul pas este să știți ce date trimiteți, unde și de ce. **Apoi, aveți diferite opțiuni disponibile pentru aplicarea transferului, în funcție de factori precum destinația, tipul de date și scopul.**

7. Conformitatea cu RGPD a proiectelor implementate din Fonduri Europene Stucturale și de Investiții

În anexa 1 a prezentului îndrumar vă prezentăm un model de plan de conformare RGPD.

Asigurarea protecției datelor cu caracter personal trebuie realizată încă de la momentul conceperii (privacy by design) unei aplicații sau a unei prelucrări prin:

- ✓ minimizarea colectării datelor în funcție de scop;
- ✓ stabilirea politicii de cookies;
- ✓ stabilirea perioadei de stocare;
- ✓ stabilirea informațiilor ce vor fi furnizate persoanelor vizate;
- ✓ obținerea consimțământului persoanelor vizate;
- ✓ securitatea și confidențialitatea datelor cu caracter personal;
- ✓ garantarea rolului și responsabilității părților implicate în efectuarea prelucrării datelor;

Asigurarea protecției datelor cu caracter personal trebuie realizată și prin aplicarea de măsuri tehnice și organizatorice adecvate **pentru a se asigura că, în mod implicit, sunt prelucrate numai acele**

date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării (privacy by default), având în vedere: volumul de date colectate, gradul de prelucrare a acestora, perioada de stocare și accesibilitatea lor, astfel încât datele cu caracter personal să nu fie accesate de un număr nelimitat de persoane.

Dupa evaluarea **Privacy by Design and By default**[17] se efectuează pașii similari de mai sus, dar adaptați contextului.

Deosebirea majoră între un proiect de conformare la RGPD al unei instituții publice și respectarea RGPD a proiectelor finanțate din Fonduri Europene Structurale și de Investiții constă în drepturile pe care o persoană vizată le poate exercita. În funcție de natura activității și indicatorii proiectului participanții/părțile din proiect nu pot solicita:

- ✓ Ștergerea datelor;
- ✓ Portabilitatea datelor.

în schimb pot solicita:

- ✓ accesarea datelor cu caracter personal;
- ✓ restricționarea prelucrării în cazul în care există justificarea corespunzătoare.
- ❖ **Anonimizarea**

Potrivit principiului limitărilor legate de stocare inclus atât în RGPD, cât și în legislația internă conexă domeniului, datele trebuie păstrate *„într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele*”.

În consecință, datele trebuie fie șterse, fie criptate sau anonimizate în cazul în care un operator dorește să le stocheze după ce nu mai sunt necesare și nu mai servesc scopului inițial.

Procesul de anonimizare a datelor desemnează eliminarea tuturor elementelor de identificare dintr-un set de date cu caracter personal, astfel încât persoana vizată să nu mai fie identificabilă. Dacă datele au fost anonimizate cu succes, acestea nu mai sunt date cu

[17] confidenţialitarea datelor începând cu momentul conceperii şi implicit

caracter personal, iar legislația privind protecția datelor nu mai este aplicabilă în cazul lor.

RGPD prevede că persoana sau organizația care administrează prelucrarea datelor cu caracter personal nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării Regulamentului.

Există totuși **o excepție semnificativă** aferentă acestei norme: ori de câte ori persoana vizată, în scopul exercitării dreptului de acces, rectificare, ștergere, restricționare a prelucrării și a portabilității datelor, oferă operatorului informații suplimentare care permit identificarea sa, datele care au fost anonimizate anterior redevin date cu caracter personal[18].

- **Pseudonimizarea**

Informațiile cu caracter personal conțin atribute, cum ar fi numele, data nașterii, sexul, adresa sau alte elemente care ar putea duce la identificare. Procesul de pseudonimizare a datelor cu caracter personal presupune înlocuirea acestor atribute cu un pseudonim.

RGPD recunoaște diferite utilizări ale pseudonimizării drept măsuri tehnice adecvate pentru îmbunătățirea protecției datelor, pseudonimizarea fiind menționată în mod specific în relație cu proiectarea și securitatea prelucrării datelor pe care le asigură. Aceasta constituie, de asemenea, o garanție adecvată care poate fi utilizată pentru prelucrarea datelor cu caracter personal în alte scopuri decât cele pentru care au fost colectate inițial.

8. Prelucrarea datelor cu caracter personal în sistemul MySMIS 2014

Sistemul MySMIS 2014 reprezintă un instrument/sistem utilizat în gestiunea proiectelor finanțate din Fonduri Europene Structurale și de Investiții/(FESI).

[18]Regulamentul general privind protecția datelor, articolul 11.

Atunci când se realizează cartografierea datelor cu caracter personal utilizate în procesele instituției, sau a proiectelor, **principiile RGPD trebuie extinse și aplicate atât la nivelul prelucrărilor efectuate în format fizic cât și la nivelul prelucrărilor efectuate în sisteme/soluții informatice**. **Exemplu:** ștergerea datelor nu se efectuează doar la nivelul documentelor prin distrugerea acestora, ci și la nivelul sistemelor/soluțiilor utilizate în prelucrarea datelor.

Având în vedere natura și scopul sistemului MySMIS și anume colector de date cu caracter personal, se recomandă ca acesta să respecte standarde ridicate de protecție a datelor cu caracter personal.

În vederea asigurării conformității la RGPD a MySMIS 2014, recomandăm să se creeze un plan de asigurare a conformității dedicat exclusiv sistemului care să treacă cel puțin prin următoarele etape:

I. Inventarierea prelucrărilor care se efectuează la nivelul soluției MySMIS prin identificarea:

- Scopurilor prelucrărilor
- Temeiurilor de prelucrare
- Categoriile de persoane vizate
- Categoriile de date prelucrate
- Destinatari, inclusiv din afara Spațiului Economic European
- Stabilirea termenelor limită de păstrare
- Măsurilor tehnice și organizatorice implementate.

Asigurarea integrității datelor în uz, în tranzit și în staționare presupune proceduri și procese solide de oferire a accesului la date, de schimbare a datelor confidențiale de acces, de folosire de tehnologii de validare suplimentară a autorizării și de stocare sigură a acestora.

II. Evaluarea impactului asupra protecției datelor- DPIA este necesară în cazul în care un tip de prelucrare – în mod special cele în care se utilizează noi tehnologii – poate genera un risc ridicat pentru drepturile și libertățile persoanelor fizice (art. 35 (1) din RGPD).

III. În urma analizei de necesitate se identifică strategia de realizare a DPIA, se elaborează modelul de DPIA și se desemnează persoana / grupul de persoane care o realizează.

IV. După realizarea DPIA, se recomandă revizuirea prelucrărilor de date cu caracter personal astfel încât să se diminueze riscurile pentru pentru drepturile și libertățile persoanelor fizice conform Art. art. 35, alin. (1) din Regulament.

V. Revizuirea prelucrărilor de date cu caracter personal realizate în cadrul sistemului MySMIS în vederea aplicării principiilor RGPD. Indiferent de necesitatea realizării unei DPIA, prelucrările de date efectuate în cadrul soluției MySMIS trebuie revizuite și aplicate principiile RGPD:

⇒ Principiul de legalitate și scop
⇒ Principiul limitării legate de scop
⇒ Principiul reducerii la minim a datelor

VI. Pentru prelucrările care au ca și temei interesul legitim se recomandă realizarea unei Analize a Interesului Legitim (LIA).

VII. La nivelul Soluției MySMIS trebuie adoptate mecanisme și proceduri privind Gestionarea Drepturilor Persoanelor Vizate astfel:

⇒ Identificarea categoriilor de persoane vizate;
⇒ Elaborarea notificărilor de informare a categoriilor de persoane vizate aplicându-se Principiul Transparenței;
⇒ Elaborarea formularelor / paginilor în cadrul soluției de colectarea a consimțământului persoanelor vizate, acolo unde prelucrarea se bazează pe consimțământ;
⇒ Stabilirea modalității de informare și obținere a consimțământului persoanelor vizate;
⇒ Stabilirea modalității de elaborare a registrului privind consimțământul persoanelor vizate și menținerea lui permanentă;
⇒ Stabilirea modalității de informare atunci când au loc modificări la nivelul notificărilor de informare sau elaborarea unei proceduri de informare periodică;
⇒ Elaborarea de proceduri de exercitare a drepturilor persoanelor vizate;
⇒ Elaborarea registrului privind cererile persoanelor vizate.

VIII. Implementarea politicilor și procedurilor privind:

⇒ Politica de protecție a datelor /Politica de securitate;

⇒ Procedura de exercitare a drepturilor persoanelor vizate;
⇒ Procedura privind gestionarea incidentelor de securitate;
⇒ Politica privind cookies;
⇒ Politica/Procedura de instruire în domeniul protecției datelor la nivelul Sistemului MySMIS
⇒ Procedura de evaluare a furnizorilor (persoanelor împuternicite de operator);
⇒ Procedurile de ștergere, anonimizare, pseudoanonimizare;
⇒ Politica Privacy by Design and By Default;
⇒ Altele, care se identifică a fi necesare.

IX. Implementarea măsurilor tehnice și organizatorice privind securitatea datelor cu caracter personal. Având în vedere scopul și dimensiunea Sistemului MySMIS, recomandăm implementarea următoarelor:

a. Managementul accesului
   ⇒ Implementarea de politici de securizare a accesului la platformă prin definirea unei matrici de acces la sistem prin separarea sarcinilor și responsabilităților;
   ⇒ Matricea implementată să țină cont și de drepturile de descărcare a documentelor stocate în MySMIS;
   ⇒ Implementarea unor politici/proceduri de acces la bazele de date, serverele de aplicații astfel încât doar personalul autorizat să aibă acces la aceste resurse;
   ⇒ Implementarea de proceduri de retragere a accesului utilizatorilor de îndată ce aceștia nu mai sunt autorizați să utilizeze resursele;
   ⇒ Efectuarea unei analize anuale privind drepturile de acces.

b. Autentificarea utilizatorilor
   ⇒ Definirea pentru fiecare utilizator unui identificator unic;
   ⇒ Aplicarea de politici de securizare a parolei

c. Monitorizarea accesului şi managementul incidentelor de securitate
   - Configurarea jurnalelor pentru înregistrarea activității utilizatorilor, anomaliilor și evenimentelor legate de securitate;
   - Implementarea unei proceduri de jurnalizare a accesului furnizorilor externi de servicii IT pe serverele unde este

găzduit sistemul, astfel încât să existe o trasabilitate a acțiunilor întreprinse;
- Monitorizarea utilizării sistemului și efectuarea de analize în vederea identificării anomaliilor sau accesărilor;
- Implementarea unui serviciu de evaluare și scanare periodică a vulnerabilităților sistemelor IT - Vulnerability Assessment and Management. Realizarea de teste de penetrare a rețelei atât din Internet, cât și din interiorul rețelei pentru a testa reziliența sistemelor IT la atacuri și descoperirea de vulnerabilități;
- Realizarea de teste periodice de penetrare pentru descoperirea posibilelor vulnerabilități existente și pentru a testa reziliența la atacurile malițioase din Internet;
- Realizarea și implementarea unei proceduri de tratare a incidentelor de securitate.

d. Protejarea stațiilor de lucru ale utilizatorilor Sistemului MySMIS, în special cei care au drepturi de descărcare documente din sistem.
   - Implementarea de politici de securitate pentru accesul la stațiile de lucru, prin acces pe baza de user și parola. Crearea de conturi nominale pentru utilizatori și dezactivarea celor cu nume generic;
   - Aplicarea de politici de securizare a parolei: schimbare la timp predefinit;
   - Stațiile de lucru configurate să se blocheze automat în momentele de inactivitate și la reluarea activității să ceară parola utilizatorului, pentru a preveni accesul neautorizat la stațiile de lucru;
   - USB sau alte echipamente portabile de stocare a datelor. Acceptarea transferului de date doar către echipamentele portabile acceptate în instituție. Criptarea acestor echipamente portabile de transfer a datelor;
   - Implementarea unei soluții antivirus comerciale cu suport și actualizări din partea producătorului.
   - Eliminarea programelor antivirus gratuite de pe computerele utilizatorilor și înlocuirea lor cu soluții antivirus profesioniste cu suport comercial și cu consola de management centralizat, ce permite monitorizarea în timp real a situației actualizărilor semnăturilor;

- Eliminarea programelor de acces de la distanță de pe stațiile de lucru. Pot fi extrase date din instituție!

e. Protejarea rețelei interne
   - Limitarea accesului la serviciile neesențiale (VoIP, peer to peer, etc.)
   - Gestionarea rețelelor Wi-Fi prin utilizarea celor mai noi tehnologii de criptare (WPA2 sau WPA2-PSK cu parole complexe)
   - Implementarea unui VPN pentru acces la distanță, precum și, dacă este posibil, o metodă de autentificare complexă a utilizatorului (cartelă inteligentă, parolă unică generată de fiecare dată etc.).
   - Asigurarea că nicio interfață de administrare nu este direct accesibilă de pe Internet, iar întreținerea la distanță este realizată printr-o rețea VPN.

f. Asigurarea continuității activității
   - Efectuarea de copii de siguranță, periodic, protejarea acestora asigurând același nivel de securitate ca și cel pentru datele stocate pe serverele operaționale;
   - Proceduri backup, implementare sisteme securitate backup: firewall;
   - Testare periodică (anuală) a vulnerabilităților și punerea în aplicare a unui Plan de Continuitate;
   - Cumpărarea de generatoare/baterii pentru serverele locale; contractarea și impunerea asigurării continuității furnizării energiei electrice la serverele de stocare. Utilizarea unei surse de alimentare continuă pentru a proteja echipamentul utilizat;
   - RECOMANDARE OPȚIONALĂ: implementarea unui provider secundar de Internet, care să asigure funcționalitatea continuă a serviciului de acces la Internet.

g. Arhivarea securizată / stocarea electronică a documentelor
   - Elaborarea și implementarea unei proceduri de gestionare a arhivei electronice, incluzând metode specifice de acces la datele arhivate electronic;
   - Măsuri de asigurare back-up la toate stocurile de documente care conțin date;

- Aplicarea de măsuri care să garanteze distrugerea arhivei electronice în întregimea sa, inclusiv backup-ul arhivelor;

h. Serverele

- Sincronizarea ceasurilor tuturor echipamentelor din infrastructura IT cu același server de tip NTP (Network Time Protocol) - Echipamente de rețea, servere, stații de lucru;
- Asigurarea protecției fizice adecvate pentru echipamentele din camera unde este găzduit serverul intern. Realizarea unui jurnal cu evidențe de acces în această cameră, pentru a avea trasabilitatea accesului fizic la serverele pe care este gazduită soluția;
- Asigurarea unei temperaturi optime de lucru pentru echipamentele din camera serverelor;
- Verificarea echipamentelor de protecție împotriva vârfurilor de tensiune - UPS, din camera serverelor. Realizarea de teste de performanță și înlocuirea lor acolo unde este cazul. Conectarea tuturor echipamentelor la UPS-uri.
- Asigurarea protecției fizice adecvate pentru echipamentele de tip DVR/NVR. Securizarea lor în rack-uri specializate, închise cu cheie.
- Verificarea echipamentelor de tip UPS ce oferă protecție împotriva vârfurilor de tensiune pentru echipamentele de tip DVR/NVR din toată infrastructura.

ATENȚIE! Planul propuns pentru asigurarea conformității la RGPD a prelucrărilor care se efectuează în cadrul Soluției MySMIS reprezintă o propunere, o analiză detaliată este necesară pentru a rafina activitățile la nivel de detaliu, de a stabili responsabili, precum și a modului în care se realizează anumite activități.

9. Studii de caz – exemple privind aplicabilitatea RGPD

DREPTUL LA VIAȚĂ PRIVATĂ

⇒ **Exemplu:** În cauza Digital Rights Ireland, CJUE a fost sesizată să se pronunțe cu privire la valabilitatea Directivei 2006/24/CE în ceea ce privește drepturile fundamentale la protecție a datelor cu caracter personal și la respectarea vieții private, consacrate în Carta drepturilor fundamentale a UE. Directiva impunea furnizorilor de servicii de comunicații electronice destinate publicului sau rețelelor publice de comunicații să păstreze datele din telecomunicații ale cetățenilor pe o perioadă de până la doi ani, pentru a se asigura disponibilitatea datelor în scopul prevenirii, investigării și urmăririi penale a infracțiunilor grave.
Măsura viza numai metadatele, datele de localizare și datele necesare identificării abonatului sau a utilizatorului, fără a se aplica conținutului comunicațiilor electronice. **CJUE a considerat că directiva aduce atingere dreptului fundamental la protecția datelor cu caracter personal „întrucât prevede o prelucrare a datelor cu caracter personal”**. În plus, Curtea a constatat că directiva aduce atingere dreptului la respectarea vieții private. Luate în ansamblu, datele cu caracter personal păstrate în temeiul directivei și la care puteau avea acces autoritățile competente ar fi putut permite „*deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, precum obiceiurile din viața cotidiană, locurile de ședere permanente sau temporare, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele*”. Cele două drepturi au fost încălcate în mod global și deosebit de grav.

CJUE a declarat Directiva 2006/24/CE nulă, constatând că, deși aceasta urmărea un scop legitim, încălcarea drepturilor la protecția datelor cu caracter personal și la viața privată era gravă și nu se limita la ceea ce era strict necesar.

NECESITATEA ȘI PROPORȚIONALITATEA

Articolul 52 alineatul (1) din Cartă prevede că, sub rezerva principiului proporționalității, exercițiul drepturilor și libertăților fundamentale recunoscute de Cartă poate fi restrâns numai dacă acest lucru este necesar.

Proporționalitatea înseamnă că avantajele care rezultă din limitare trebuie să depășească dezavantajele pe care aceasta le creează în ceea ce privește exercițiul drepturilor fundamentale în cauză. Pentru a reduce dezavantajele și riscurile la adresa exercițiului drepturilor la respectarea vieții private și la protecția datelor, este important ca limitările să fie însoțite de garanții adecvate.

> ⇒ **Exemplu:** În cauza Volker und Markus Schecke, CJUE a concluzionat că prin impunerea unei obligații de publicare a datelor cu caracter personal ale fiecărei persoane fizice care a beneficiat de ajutor de la anumite fonduri agricole fără a face distincție în funcție de criterii relevante, cum ar fi perioadele în care acele persoane au primit un astfel de ajutor, frecvența acestui ajutor sau natura și valoarea acestuia, Consiliul și Comisia au depășit limitele pe care le impune respectarea principiului proporționalității.

DREPTUL DE ACCES LA INFORMAȚIILE OFICIALE

În temeiul legislației UE, dreptul de acces la documentele oficiale este garantat de Regulamentul (CE) nr. 1049/2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (Regulamentul privind accesul la documente). Articolul 42 din Cartă și articolul 15 alineatul (3) din TFUE au extins acest drept de acces „la documentele instituțiilor, organelor, oficiilor și agențiilor Uniunii, indiferent de suportul pe care se află aceste documente”.

> ⇒ **Exemplu:** În cauzele conexate Volker und Markus Schecke și Hartmut Eifert/ Land Hessen, CJUE a trebuit să se pronunțe asupra proporționalității publicării, impusă de legislația UE, a numelor beneficiarilor subvențiilor agricole ale UE și a sumelor pe care aceștia le-au primit. Publicarea urmărea creșterea transparenței și contribuția la controlul public al utilizării adecvate a fondurilor

publice de către administrație. Mai mulți beneficiari au contestat proporționalitatea acestei publicări.

Remarcând faptul că dreptul la protecția datelor nu este absolut, CJUE a argumentat că publicarea pe un site a datelor nominale ale beneficiarilor a două fonduri ale UE de ajutoare pentru agricultură și a sumelor exacte primite constituie o ingerință în viața privată, la nivel general, și în protecția datelor cu caracter personal ale acestora, la nivel particular.

Cu toate acestea, **CJUE a considerat că publicarea numelor persoanelor fizice care beneficiază de ajutor pentru agricultură din partea UE în cadrul acestor două fonduri și a sumelor exacte primite constituie o măsură disproporționată și nejustificată în conformitate cu articolul 52 alineatul (1) din Cartă.** Curtea a recunoscut că, într-o societate democratică, este important ca persoanele contribuabile să fie informate cu privire la utilizarea fondurilor publice. Cu toate acestea, întrucât „nu se poate recunoaște obiectivului transparenței nicio superioritate automată asupra dreptului la protecția datelor cu caracter personal", instituțiile UE aveau obligația de a stabili un echilibru între interesul Uniunii în ceea ce privește transparența, pe de o parte, și limitarea exercițiului drepturilor la respectarea vieții private și la protecția datelor care le fusese impusă beneficiarilor ca rezultat al publicării, pe de altă parte.

CJUE a considerat că instituțiile UE nu au efectuat corect acest exercițiu de echilibrare, întrucât era posibil să fie concepute măsuri prin care se aduc atingeri mai puțin grave drepturilor fundamentale ale persoanelor, astfel încât să contribuie în același timp în mod eficient la obiectivul transparenței urmărit de publicare. De exemplu, în locul unei publicări generale care afectează toți beneficiarii, indicând numele acestora și sumele exacte primite de fiecare dintre ei, se putea face o distincție în funcție de criterii relevante, precum perioadele în care aceste persoane au primit astfel de fonduri, frecvența sau tipul și valoarea acestora. Astfel, CJUE a declarat parțial nulă legislația UE privind publicarea informațiilor referitoare la beneficiarii fondurilor UE pentru agricultură.

SECRETUL PROFESIONAL

⇒ **De exemplu**, CJUE a statuat că, în anumite cazuri, „interzicerea divulgării anumitor informații calificate drept confidențiale poate fi necesară pentru a garanta dreptul fundamental al unei întreprinderi la respectarea vieții private, prevăzut la articolul 8 din Convenția europeană a drepturilor omului [...] și la articolul 7 din Cartă. Și CEDO a fost sesizată cu solicitarea de a se pronunța asupra faptului dacă restricțiile legate de secretul profesional constituie o încălcare a articolului 8 din Convenția europeană a drepturilor omului, după cum se arată la exemplul de mai jos.

În cauza Pruteanu/România, reclamantul a acționat în calitate de avocat al unei societăți comerciale căreia i s-a interzis să efectueze tranzacții bancare ca urmare a unor acuzații de fraudă. În cadrul examinării cauzei, instanțele române au autorizat autoritățile de urmărire penală să intercepteze și să înregistreze convorbirile telefonice ale unui partener de afaceri al societății în cauză pentru o anumită perioadă. Înregistrările și interceptările au inclus comunicările cu avocatul său.

Domnul Pruteanu a susținut că acest lucru a adus atingere dreptului său la respectarea vieții private și a corespondenței. În hotărârea sa, CEDO a subliniat statutul și importanța relației dintre avocat și client. Interceptarea conversațiilor avocatului cu clientul său a încălcat fără îndoială secretul profesional, pe care se întemeia relația dintre aceste două persoane. Într-un astfel de caz, avocatul ar putea, de asemenea, să acuze o ingerință în dreptul său la respectarea vieții private și a corespondenței. CJUE a concluzionat că s-a încălcat articolul 8 din Convenția europeană a drepturilor omului.

SEPARAREA COMPLETĂ A ASPECTELOR LEGATE DE VIAȚA PRIVATĂ ȘI CEA PROFESIONALĂ

Jurisprudența CEDO cu privire la articolul 8 din Convenția europeană a drepturilor omului confirmă că separarea completă a aspectelor legate de viața privată și cea profesională poate fi dificilă.

⇒ **Exemplu:** În cauza Bărbulescu/Romania, reclamantul fusese concediat pentru că a folosit internetul angajatorului său în

timpul orelor de lucru, încălcând reglementările interne. Angajatorul său i-a monitorizat comunicările, iar înregistrările acestora, care puneau în evidență mesaje cu caracter pur personal, au fost prezentate în cadrul procedurii în fața instanței naționale. Constatând că articolul 8 este aplicabil în speță, CEDO a lăsat deschisă întrebarea dacă reglementările restrictive ale angajatorului permiteau ca reclamantul să aibă așteptări rezonabile în ceea ce privește viața privată, dar în orice caz a considerat că instrucțiunile unui angajator nu puteau reduce la zero viața socială privată la locul de muncă. Cu privire la fond, statele contractante trebuiau să beneficieze de o marjă largă de apreciere pentru a evalua necesitatea stabilirii unui cadru juridic care să reglementeze condițiile în care un angajator poate reglementa comunicările de altă natură decât profesională ale angajaților săi – în format electronic sau de alt tip – la locul de muncă. Cu toate acestea, autoritățile naționale trebuiau să se asigure că introducerea de către angajator a unor măsuri de monitorizare a corespondenței și a altor comunicări, indiferent de amploarea și de durata acestor măsuri, este însoțită de garanții adecvate și suficiente împotriva abuzurilor. Proporționalitatea și garanțiile procedurale împotriva arbitrarului măsurilor sunt esențiale, iar CEDO a identificat o serie de factori relevanți în speță. Acești factori includ, de exemplu, amploarea monitorizării de către angajator a angajaților și gradul de intruziune în viața privată a acestora din urmă, consecințele pentru angajați și dacă s-au oferit garanții adecvate. În plus, autoritățile naționale trebuiau să se asigure că un angajat ale cărui comunicări fuseseră monitorizate avea acces la o cale de atac în fața unei instanțe judecătorești competente să determine, cel puțin în fond, cum au fost respectate criteriile stabilite și dacă măsurile contestate erau legale. CEDO a constatat în această speță că s-a încălcat articolul 8, deoarece autoritățile naționale nu au acordat o protecție adecvată dreptului reclamantului la respectarea vieții private și a corespondenței și, prin urmare, nu au reușit să asigure un echilibru just între interesele concurente în cauză.

DREPTUL DE ACCES

⇒ **Exemplu:** Cauza *Smaranda Bara și alții/Președintele Casei Naționale de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF)* viza transmiterea datelor fiscale referitoare la venitul persoanelor fizice care desfășoară activități independente de la Agenția Națională de Administrare Fiscală către Casa Națională de Asigurări de Sănătate din România, pe baza acestor date solicitându-se plata contribuțiilor datorate la asigurările de sănătate. CJUE i s-a solicitat să stabilească dacă persoanei vizate ar fi trebuit să i se furnizeze informații privind identitatea operatorului de date și scopul transmiterii datelor înainte de prelucrarea acestor date de către Casa Națională de Asigurări de Sănătate. CJUE a stabilit că, atunci când o autoritate a administrației publice dintr-un stat membru transmite date cu caracter personal unei alte autorități a administrației publice care prelucrează ulterior aceste date, persoanele vizate trebuie să fie informate cu privire la această transmitere sau prelucrare.

10. Jurisprudenţă relevantă

Hotărâri CJUE și CEDO

⇒ Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții.

⇒ Hotărârea CEDO [MC] din 4 mai 2000 în cauza Rotaru/România, nr. 28341/95.

⇒ Hotărârea CEDO din 18 octombrie 2011 în cauza Khelili/Elveția, nr. 16188/07

⇒ Hotărârea CJUE din 17 iunie 2010 în cauzele conexate C-92/09 și C-93/02, Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen, și Concluziile avocatului general Sharpston, punctul 71.

⇒ Hotărârea CJUE [MC] din 16 decembrie 2008 în cauza C-73/07, Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy și Satamedia Oy, punctele 56, 61 și 62.

⇒ Hotărârea CEDO din 24 iunie 2004 în cauza Von Hannover/Germania, nr. 59320/00; Hotărârea CEDO din 11 ianuarie 2005 în cauza Sciacca/Italia, nr. 50774/99; Hotărârea CJUE din 11 decembrie 2014 în cauza C-212/13, František Ryneš/Úřad pro ochranu osobních údajů.

⇒ Hotărârea CEDO [MC] din 7 februarie 2012 în cauza Axel Springer AG/Germania, nr. 39954/08

⇒ Hotărârea CJUE [MC] din 9 noiembrie 2010 în cauzele conexate C-92/09 și C-93/09, Volker und Markus Schecke GbR și Hartmut Eifert/Land Hessen [Conceptul „date cu caracter personal”; proporționalitatea obligației legale de a publica date cu caracter personal privind beneficiarii unor anumite fonduri agricole ale UE]

⇒ Hotărârea CEDO din 3 februarie 2015 în cauza Pruteanu/România, nr. 30181/05

⇒ Hotărârea CEDO din 14 martie 2013 în cauza Bernh Larsen Holding AS și alții/Norvegia, nr. 24117/08

⇒ Hotărârea CEDO [MC] din 5 septembrie 2017 în cauza Bărbulescu/România, nr. 61496/08, punctul 121.

⇒ Hotărârea CJUE din 11 decembrie 2014 în cauza C-212/13, František Ryneš/Úřad pro ochranu osobních údajů, punctul 25.

⇒ Hotărârea CEDO din 27 octombrie 2009 în cauza Haralambie/România, nr. 21737/03.

⇒ Hotărârea CJUE din 1 octombrie 2015 în cauza C-201/14, Smaranda Bara și alții/Casa Națională de Asigurări de Sănătate și alții, punctele 28-46.

⇒ Hotărârea CJUE [MC] din 8 aprilie 2014 în cauzele conexate C-293/12 și C-594/12, Digital Rights Ireland Ltd/Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții.

⇒ Hotărârea CEDO din 27 aprilie 2010 în cauza Ciubotaru/Moldova, nr. 27138/04, punctele 51 și 59.

⇒ Hotărârea CEDO din 6 iunie 2006 în cauza Segerstedt-Wiberg și alții/Suedia, nr. 62332/00, punctele 89 și 90; vezi, de asemenea, de exemplu, Hotărârea CEDO din 18 aprilie 2013 în cauza M.K./Franța, nr. 19522/09.

Anexa 1. Plan de conformare RGPD la nivelul instituţiei - Model

1.Numirea unui DPO
1.1.Analiza asupra persoanei
a) Stabilirea criteriilor pentru alegerea persoanei care să ocupe poziția de DPO și analiza nevoii de a desemna un DPO intern sau extern
b) Identificarea persoanei care să ocupe funcţia de DPO, angajarea sau contractarea externă
c) Emiterea deciziilor de numire a DPO
d) Stabilirea responsabilităţilor în contract sau fişa postului
e) Alocarea resurselor necesare desfăşurării activităţii
f) Notificarea numirii DPO la autoritate și comunicarea internă a datelor de contact
g)Elaborarea procedurii de lucru cu DPO
h)Punerea în practică a procedurii de lucru cu DPO
2.Elaborare şi implementare documentaţii
2.1.Elaborare registru inventar-cartografiere date cu caracter personal
a) Realizarea modelului de registru, stabilirea modului de completare și desemnarea persoanelor din fiecare departament/entitate responsabilă cu completarea registrului (funcţiuni).
b) Inventarierea proceselor interne prin care sunt prelucrate date cu caracter personal
• identificarea scopurilor prelucrării,
• identificarea temeiurilor de prelucrare,
• identificarea categoriilor de persoane vizate,
• identificarea categoriilor de date prelucrate,
• identificarea destinatarilor (inclusiv din afara Spațiului Economic European),
• stabilirea termenelor limită de păstrare,
• inventarierea măsurilor tehnice și organizatorice implementate.
c)Identificarea şi inventarierea aplicaţiilor şi programelor software
d)Verificarea registrului inventar întocmit de persoanele desemnate

e)Elaborarea modelului de evaluare a interesului legitim, identificarea metodologiei, (LIA), desemnarea persoanelor care urmează să realizeze evaluările
f) Efectuarea testelor pentru prelucrarea în interes legitim, verificarea lor de către DPO și luarea deciziei cu privire la activitatea de prelucrare (în funcție de rezultatul evaluării): da sau nu
g) Determinarea necesităţii de realizare de evaluări a impactului asupra protecției datelor (DPIA)
h) Elaborarea modelului DPIA, identificarea metodologiei, desemnarea persoanei care va efectua DPIA
l) Efectuarea DPIA, verificarea de către DPO și luarea deciziei cu privire la activitatea de prelucrare (în funcție de rezultatul evaluării)
j) Aplicarea principiilor RGPD și revizuirea prelucrărilor în consecință.
• Principiul de legalitate și echitate
• Principiul limitării legate de scop
• Principiul reducerii la minim a datelor
k) Măsuri pentru actualizare permanentă
2.2.Gestionarea drepturilor persoanei vizate
a)Identificarea categoriilor de persoane vizate potrivit registrului inventar
b) Elaborarea notelor de informare pe categorii de persoane vizate (Principiul transparenței)
c) Elaborarea formularelor de colectare a consimţământului pentru activitățile de prelucrare întemeiate pe acest temei legal conform registrului inventar
d) Stabilirea modurilor de transmitere a notelor de informare și de colectare a consimțămintelor
e) Transmiterea notelor de informare
f) Transmiterea solicitărilor de obţinere a consimţământului și colectarea formularelor completate
g) Elaborarea și implementarea procedurilor de exercitare a drepturilor persoanelor vizate (acces, restricționare, opoziție, portabilitate, ștergere)

h) Identificarea şi elaborarea documentelor publice, pentru canale publice de colectare (ex: site, conturi de rețele de socializare)
i) Elaborarea şi menţinerea registrelor de evidenţă a consimţămintelor şi cererilor persoanelor vizate
2.3.Elaborare şi implementare politici şi proceduri
a) Politica generală de protecţie a datelor
b) Consultare specialişti IT, analiză vulnerabilităţi, identificare cookies
c) Politica cookies pentru site
d) Politică site privind datele sau informare generală cu privire la ce se colectează şi postează pe site
e) Procedură de administrare a solicitărilor de exercitare drepturi persoane vizate (exercitare drepturi), răspuns şi intervenţie
f) Procedura privind gestionarea incidentelor de securitate
g) Aprobarea și aducerea la cunoștință, conform modului/uzanțelor interne, a tuturor actelor enumerate la această etapă.
3.Gestionarea drepturilor şi alocarea responsabilităţilor angajaţilor
3.1.Gestionarea drepturilor angajaţilor
a) Identificarea canalelor de colectare pentru datele potențialilor angajați și cele ale angajaţilor existenţi
b) Elaborarea și implementarea documentelor pentru respectarea dreptului la informare al angajaţilor; elaborarea formularului de consimţământ pentru eventuale beneficii suplimentare şi pentru utilizarea unor date suplimentare de către instituţie (ex: fotografie)
c) Elaborarea și implementarea modificărilor la regulamentul intern/regulament de organizare şi funcţionare pentru confirmarea acordării drepturilor angajaţilor
d) Procedura pentru utilizarea logisticii puse la dispoziţia angajaţilor - Proceduri interne (mașini de serviciu, telefoane mobile, laptopuri)
e) Elaborarea unui set de reguli generale de securizare a datelor
f) Elaborare procedură de securitate a datelor
3.2.Alocarea responsabilităţilor angajaţilor

a) Implementarea de modificări ale Regulamentului intern, a politicilor şi procedurilor existente pentru a include prevederi specifice în materia protecției datelor
b) Elaborarea prevederilor şi completări la fişa postului fiecărui angajat, în funcţie de responsabilităţi
c) Elaborarea și implementarea procedurilor de raportare către DPO
d) Elaborarea și implementarea procedurilor de raportare a incidentelor de securitate
e) Elaborarea și implementarea procedurii privind transferul de date
f) Implementarea unei politici de clasificare a informațiilor prin care se vor defini diferite niveluri de confidențialitate și prin care se vor marca documentele și emailurile care conțin date cu caracter confidențial
g) Verificarea periodică a respectării procedurilor operaționale privind datele personale
4.Creșterea gradului de conștientizare cu privire la confidențialitate și securitate la nivelul Instituției/Societății
4.1.Organizarea sesiunilor de instruire
a) Organizarea de sesiuni de instruire pentru Conducerea Instituției
b) Oganizarea de sesiuni de instruire pe funcţiuni/ departamente
c) Transmiterea periodică de actualizări privind procedurile relevante pentru personal
d) Transmiterea de instrucţiuni și informări periodice cu privire la protecția datelor (prin email)
e) Documentarea, actualizarea și menţinerea la dispoziția tuturor utilizatorilor implicați a politicilor şi a procedurilor în materia protecţiei datelor
4.2.Instruire utilizatori sisteme informatice
a) Elaborarea și implementarea unei Proceduri IT
b) Prezentarea și verificarea cunoașterii regulilor de protecție a datelor cu caracter personal și a sancțiunilor aplicabile în cazul nerespectării acestora
c) Prezentarea și verificarea cunoașterii domeniului de aplicare al procedurii IT

d) Prezentarea și verificarea cunoașterii condițiilor de administrare a sistemului informatic
e) Prezentarea și verificarea respectării procedurilor de utilizare a echipamentelor IT și a resurselor de telecomunicații disponibile utilizatorului
5.Gestionarea arhivelor fizice
5.1.Elaborarea nomenclatorului arhivistic
a) Emiterea deciziei interne pentru nominalizarea persoanelor care vor fi responsabile de inventarierea documentelor fiecărui departament sau nominalizarea unei singure persoane care să realizeze această inventariere.
b) Inventarierea documentelor primite/elaborate, conform deciziei emise pentru inventarierea documentelor
c) Stabilirea perioadelor de stocare pe fiecare document
d) Analiză asupra necesităţii şi oportunităţii colectărilor de date / documente
e) Stabilirea și implementarea sistemului de arhivare
f) Arhivarea cu anonimizare/ștergerea documentelor electronice a căror perioadă de arhivare a expirat
g) Distrugerea sau anonimizarea arhivelor fizice vechi / la împlinirea termenelor
6.Calificarea contractelor
6.1. Elaborare documente
a) Draft acorduri specifice (împuterniciţi şi operatori asociaţi) şi clauze contractuale minime
b) Draft note de informare reprezentanţi şi persoane de contact, formulare de consimţământ
6.2. Identificarea contractelor
a) Identificarea contractelor în execuţie
b) Calificarea partenerilor contractuali în funcție de calitatea deținută în prelucrarea datelor cu caracter personal
c) Implementarea de acorduri specifice pentru fiecare partener contractual (conform 6.1. de mai sus), în funcție de calitatea în care prelucrează date cu caracter personal
d) Negociere acorduri
e) Semnare acorduri
7. Securitate Informaţională
7.1. Managementul accesului la sistemele IT

a) Elaborarea și implementarea unei proceduri privind definirea unei matrice de acces la sistem prin separarea sarcinilor și a responsabilităților astfel încât să fie limitat accesul
b) Elaborarea și implementarea unei proceduri privind retragerea accesului utilizatorilor de îndată ce aceștia nu mai sunt autorizați să folosească anumite resurse IT / la încetarea contractului
c) Elaborarea și implementarea unei proceduri privind efectuarea unei analize anuale a drepturilor de acces
7.2. Autentificarea utilizatorilor
a) Definirea pentru fiecare utilizator a unui identificator unic
b) Elaborarea și implementarea măsurilor în legătură cu parolele necesare pentru autentificare (stocarea acestora într-un mod securizat, alegerea unei parole care să respecte cerințele cu privire la complexitate)
7.3. Monitorizarea accesului şi managementul incidentelor de securitate
a) Configurarea jurnalelor (de exemplu, va stoca evenimente în fișiere jurnal) pentru a înregistra activitățile utilizatorilor, anomaliile și evenimentele legate de securitate
b) Informarea utilizatorilor privind instalarea unui sistem care să permită verificarea accesului în rețeaua IT
c) Segregarea accesului în sisteme – stabilirea nivelurilor de acces și a zonelor pe fiecare utilizator şi fiecare administrator, drepturile „admin”
d) Protejarea sistemelor și a informațiilor ce rezultă din utilizarea acestora împotriva accesului neautorizat
e) Elaborarea de proceduri care să detalieze monitorizarea utilizării sistemelor și efectuarea periodică a unei analize a informațiilor din jurnal pentru a detecta anomalii
7.4. Protejarea stațiilor de lucru
a) Implementarea unei proceduri pentru deconectarea automată a stațiilor de lucru care nu au fost utilizate o anumită perioadă de timp
b) Instalarea unui firewall și limitarea porturilor de comunicații autorizate la cele strict necesare pentru buna funcționare a aplicațiilor instalate pe o stație de lucru

c) Utilizarea unui software antivirus actualizat în mod regulat
d) Păstrarea datelor pe un suport de stocare căruia i se efectuează copii de siguranță în mod regulat și accesibil prin intermediul rețelei instituției/societății
e) Limitarea conexiunii la anumite dispozitive mobile, precum stick-uri USB, hard disk-uri externe etc. la ceea ce este esențial
f) Elaborarea și implementarea unei proceduri pentru dezactivarea adreselor de e-mail la plecarea angajaților şi la schimbarea locului de activitate; predarea staţiilor de lucru şi formatarea acestora după anonimizarea arhivei
g) Dezactivarea redării automate (autorun) în cazul dispozitivelor mobile
h) Obținerea consimțământului utilizatorului în cazul intervenției de la distanță asupra stației de lucru pe care acesta lucrează (de exemplu prin răspunsul la o întrebare afișată pe ecranul stației de lucru) și informarea utilizatorului cu privire la intervenție
7.5. Protejarea prelucrării prin dispozitive mobile
a) Informarea utilizatorilor cu privire la riscurile specifice asociate cu utilizarea dispozitivelor mobile - Prin instrucțiunile dispozitivului date de producător/distribuitor
b) Implementarea măsurilor de sincronizare și de efectuare a copiilor de siguranță pentru stațiile de lucru
c) Furnizarea măsurilor de criptare care să protejeze stațiile de lucru mobile și dispozitivele de stocare
d) Utilizarea de către utilizatori în afară de codul PIN al cartelei SIM al smartphone-urilor, a altor măsuri pentru deblocarea acestuia - Cod PIN, amprentă, cod pattern
e) Informare utilizatori
f) Backup zilnic
g) Actualizare programe
7.6. Protejarea rețelei interne
a) Limitarea accesului la serviciile neesențiale (VoIP, peer to peer, etc.)
b) Gestionarea rețelelor Wi-Fi prin utilizarea celor mai noi tehnologii de criptare (WPA2 sau WPA2-PSK cu parole complexe)

c) Implementarea unui VPN pentru acces la distanță, precum și, dacă este posibil, o metodă de autentificare complexă a utilizatorului (cartelă inteligentă, parolă unică generată de fiecare dată etc.).
d) Parolă unică, dublă autentificare, filtre trafic
e) Asigurarea că nicio interfață de administrare nu este direct accesibilă de pe Internet, iar întreținerea la distanță este realizată printr-o rețea VPN
7.7. Protejarea serverelor
a) Acordarea de acces la intrumentele și interfețele de administrare doar persoanelor calificate.
b) Adoptarea de politici specifice cu privire la parolele atribuite administratorilor
c) Actualizarea sistemelor de operarare și a aplicațiilor și programarea săptămânală a unei verificări automate
d) Actualizarea contractelor cu furnizorul serviciilor de stocare date şi cu ceilalţi furnizori de produse software
e) Implementare politică parole
7.8. Protejarea website-urilor
a) Implementarea unui protocol TLS (înlocuind SSL) pe toate website-urile și utilizarea acestuia pe toate paginile
b) Limitarea porturilor de comunicație la cele strict necesare pentru buna funcționare a aplicațiilor instalate
c) Acordarea de acces doar persoanelor calificate la instrumentele și interfețele de administrare
d) Obținerea consimțământului utilizatorilor web după ce au fost informați că se utilizează cookie-uri care nu sunt necesare pentru furnizarea serviciului
e) Limitarea accesului şi desfiinţarea porturilor nealocate personal
f) Implementarea modulelor cookie
7.9. Asigurarea continuității activității
a) Efectuarea de copii de siguranță, periodic, protejarea acestora asigurând același nivel de securitate ca și cel pentru datele stocate pe serverele operaționale
b) Proceduri backup, implementare sisteme securitate backup: firewall.

c) Testare periodică (anual) vulnerabilităţi şi punerea în aplicare a Planului de Conducere Instituție al continuităţii activităţii
d) Cumpărarea de generatoare/baterii pentru serverele locale, din România; contractarea şi impunerea asigurării continuităţii furnizării energiei electrice la serverele de stocare. Utilizarea unei surse de alimentare continuă pentru a proteja echipamentul utilizat
e) Asigurarea continuității activității prin crearea unui plan IT de management al continuității activității/afacerii și testarea periodică a modalității de restaurare a copiilor de siguranță și de aplicare a acestuia
7.10. Arhivarea securizată / stocarea electronică a documentelor
a) Elaborarea și implementarea unei proceduri de gestionare a arhivei, incluzând metode specifice de acces la datele arhivate
b) Măsuri de asigurare back-up la toate stocurile de documente care conţin date
c) Aplicarea de măsuri care să garanteze distrugerea arhivei în întregimea sa, inclusiv din stocarea electronică şi back-up – server IT
7.11. Supravegherea mentenanței și distrugerii datelor
a) Înregistrarea activităților de mentenanță într-un registru
b) Includerea unei clauze de securitate în contractele de mentenanță cu furnizorii de servicii
c) Desemnarea unei persoane responsabile care să supravegheze modul de exercitare a atribuțiilor de către terți
d) Elaborarea și implementarea unei proceduri de ștergere a datelor
7.12. Protejarea transferurilor cu alte entități
a) Implementarea de măsuri de criptare înainte de a transmite datele către terți prin dispozitive portabile (DVD, stick US, hard drive extern); Fişiere cu parolă, iar parola transmisă prin alte mijloace de comunicare; Parolare dispozitive; criptare cu cheie
b) Implementarea de măsuri de criptare pentru documentele sensibile înainte de a le trimite, dacă această transmisie se realizează prin mesagerie electronică

c) Utilizarea unui protocol care să garanteze confidențialitatea și autentificarea serverului destinatar pentru transferurile de fișiere, de exemplu SFTP sau HTTPS, utilizând cea mai recentă versiune de protocol;
7.13. Asigurarea siguranței fizice
a) Instalarea de alarme anti-efracție și verificarea acestora periodică
b) Menținerea unei liste actualizate cu persoanele sau categoriile de persoane autorizate să acceseze fiecare zonă a arhivelor fizice
c) Paza umană la punctele de acces în incinte, Plan de pază, sisteme CCTV; (redactarea si implementarea de note de informare cu privire la prelucrarea datelor cu caracter personal prin sistemul de supraveghere CCTV – la intrarea în incintele supravegheate),
d) Limitarea accesului doar la persoanele care au dreptul să fie în acel loc
e) Utilizarea unei surse de alimentare continuă pentru a proteja echipamentul utilizat pentru prelucrarea datelor cu caracter personal
f) Verificarea accesului fizic în cadrul Instituției (vizitatori, angajați)
7.14. Aplicarea privacy by design / privacy by default
a) Integrarea regulilor privind protecția datelor cu caracter personal, inclusiv din perspectiva confidențialității și a măsurilor de securitate, de la momentul conceperii aplicațiilor sau de la momentul contractării furnizării serviciilor
b) Implementarea unei politici privacy by design, de respectare a securității și a vieții private în mediul on-line încă din momentul proiectării sau implementării noilor tehnologii
7.15. Supravegherea dezvoltării programelor software
a) Introducerea în contractele cu furnizorii de aplicaţii şi IT a clauzelor specifice;
b) Modificarea şi configurarea aplicaţiilor existente astfel încât să furnizeze jurnale;
c) Programe antivirus implementate
7.16. Protejarea aplicațiilor și programelor software
a) Identificarea măsurilor de securitate ale aplicaţiilor şi programelor software

b) Identificarea posibilităţilor de acces şi intervenţie în aplicaţii şi programe software la solicitarea persoanelor vizate (pentru drepturi)
c) Programare: acordare posibilitate acces, ştergere, restricţionare, opoziţie, portabilitate
d) Aplicarea procedurii user - admin
e) Testare periodică vulnerabilităţi
f) Înregistrarea rapoartelor şi verificarea periodică a vulnerabilităţilor rezolvate
8.Gestionarea persoanelor împuternicite de operator
8.1.Evaluarea furnizorilor
a) Elaborarea chestionarului de evaluare, transmiterea anuală a chestionarului persoanelor împuternicite
b) Evaluarea garanţiilor oferite suficiente și adecvate (în special din punctul de vedere al cunoștințelor, fiabilității și resurselor); Selectarea și utilizarea numai a unor persoane împuternicite care sunt în măsură să ofere garanții
c) Negocierea acordului de prelucrare cu furnizorul (persoana împuternicită) în cazul în care apar chestiuni noi ce nu au fost avute în vedere la negocierea inițială
d) Semnarea unui acord cu persoanele împuternicite, referitor la modalitatea de prelucrare a datelor cu caracter personal
e) Auditarea persoanelor împuternicite la sediul acestora direct sau printr-un auditor extern.
8.2. Evaluarea operatorilor asociați
a) Identificarea, calificare şi semnarea contractelor operatori asociați
9. Aplicarea principiului responsabilității
9.1. Evaluarea documentelor
a) Analiza fiecărui canal de colectare pentru evaluarea posibilității de a demonstra conformitatea RGPD;
b) Analiza posibilității de a demonstra măsurile tehnice şi organizatorice luate;
c) Implementarea suplimentară: presupune conștientizarea, instruirea, monitorizarea și auditul – toate sarcinile pe care responsabilul cu protecția datelor le poate întreprinde.

d) Inventarierea registrelor necesare, evaluarea evidențelor: încălcări ale datelor cu caracter personal, notele de informare (pe versiuni), politici și proceduri implementate.
10. Social-media şi cloud
10.1 Facebook
a) Analiză furnizori de date din perspectiva RGPD
b) Încheiere acord de protecția datelor/aderare la politica de protecția datelor impusă de furnizor
10.2 Instagram
10.3 Twitter
11. Evenimente (diverse evenimente organizate)
11.1 Evaluarea furnizorilor
a) Elaborarea chestionarului de evaluare a persoanelor împuternicite, dacă este cazul
b) Evaluarea garanțiilor oferite suficiente și adecvate (în special din punctul de vedere al cunoștințelor, fiabilității și resurselor)
c) Selectarea şi utilizarea numai a unor persoane împuternicite care sunt în măsură să ofere garanții adecvate
d) Semnarea unui acord cu persoanele împuternicite sau operator asociat, referitor la modalitatea de prelucrare a datelor cu caracter personal
11.2. Informarea persoanelor vizate
a) Stabilirea modului în care sunt prelucrate datele cu caracter personal, a categoriilor de persoane vizate și a categoriilor de date cu caracter personal
b) Elaborarea anexei privind protecția datelor în cazul evenimentelor organizate
c) Redactarea și implementarea notelor de informare a persoanelor vizate (prin paginile de social media, pe invitații, la locația desfasurării evenimentului, etc.)
d) Redactarea și implementarea formularelor de obținere a consimțământului persoanelor vizate pentru acele prelucrări întemeiate pe consimțământul acestora

Concluzii

Potrivit unui sondaj privind drepturile fundamentale[19], 69% din populația UE în vârstă de peste 16 ani a auzit de RGPD, iar 71 % din cetățenii UE știu despre existența autorității lor naționale pentru protecția datelor.

Persoanele fizice sunt din ce în ce mai conștiente de drepturile lor: drepturile de acces, de rectificare, de ștergere și de portabilitate a datelor lor cu caracter personal, dreptul de a se opune prelucrării, precum și de necesitatea asigurării transparenței din partea operatorilor în ceea ce privește datele cu caracter personal prelucrate. RGPD a consolidat drepturile procedurale, incluzând dreptul de a depune o plângere la o autoritate pentru protecția datelor, inclusiv prin acțiuni de reprezentare, precum și dreptul la o cale de atac judiciară.

Ca atare, este imperios necesar ca autoritățile implicate în gestionarea FESI să pregătească proceduri/politici detaliate pentru toate operațiunile de prelucrare a datelor cu caracter personal. Însă, în egală măsură, este important să se implementeze sisteme de securitate capabile să protejeze datele cu caracter personal iar personalul care are acces la date cu caracter personal de orice natură să primească instruire corespunzatoare.

Pentru a beneficia de întregul potențial al RGPD, este important să existe o abordare armonizată și o cultură europeană comună de protecție a datelor, dar și să fie promovată o gestiune eficientă a cazurilor de transfer de date în sistem transfrontalier.

[19] Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA) (2020): Sondaj privind drepturile fundamentale 2019. Protecția datelor și tehnologia: https://fra.europa.eu/en/publication/2020/fundamental-rights-survey-data-protection

În concluzie este important să se garanteze că toate instrumentele disponibile în RGPD sunt utilizate pe deplin pentru a se asigura o aplicare eficientă, iar instruirea personalizată referitoare la normele RGPD şi confidențialitatea datelor vor fi de mare folos în conformarea cadrului operațional FESI, proiectul cod 3.1.107 implementat de ANFP reprezentând un un pas important în acest sens.

Colectiv de redactare, experţi asociere

PUBLIC RESEARCH SRL şi BOCASOFT SRL

(experţi şi personal suport)

Cătălin Giulescu

Cristina Maria Manda

Ioana Lefterescu

Carmen Mariana Dăscălescu

Celia Beşciu