UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

Modul 1: Noţiuni introductive cu privire la domeniul protecţiei datelor cu caracter personal

- Cadrul legislativ actual aplicabil protecţiei datelor cu caracter personal din perspectiva naţională şi europeană;
- GDPR – Elemente cu caracter de noutate introduse prin noul cadru legislativ – comparaţie cu dispoziţiile legale actuale, ghiduri şi opinii emise în domeniul protecţiei datelor cu caracter personal – art. 29 Working Group;
- Noţiuni aplicabile în domeniul protecţiei datelor cu caracter personal – definiţia datelor cu caracter personal, categorii speciale de date cu caracter personal (date sensibile), persoanele implicate în prelucrarea datelor cu caracter personal (persoane vizate, operator, împuternicit);
- Domeniul de aplicare al GDPR din punct de vedere material şi teritorial;
- Principiile prelucrării datelor cu caracter personal;
- Noţiunea de responsabil cu protecţia datelor cu caracter personal.

LEGISLAȚIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

DIRECTIVE

- Directiva (UE) 2016/680 - DIRECTIVA (UE) 2016/680 A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului.
- Directiva (UE) 2016/681 - DIRECTIVA (UE) 2016/681 A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea şi urmărirea penală a infracţiunilor de terorism şi a infracţiunilor grave.
- Directiva 95/46/CE - DIRECTIVA 95/46/CE a PARLAMENTULUI EUROPEAN I A CONSILIULUI din 24 octombrie 1995 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date - ABROGATĂ DE Regulamentul (UE) 2016/679 GDPR
- Directiva 2002/58/CE - DIRECTIVA 2002/58 / CE A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI din 12 iulie 2002 privind prelucrarea datelor cu caracter personal şi protejarea confidenţialităţii în sectorul comunicaţiilor publice (Directiva privind confidenţialitatea şi comunicaţiile electronice).
- Directiva 31/2000 - DIRECTIVA 2000/31/CE A PARLAMENTULUI EUROPEAN Ş I A CONSILIULUI din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societăţii informaţionale, în special ale comerţului electronic, pe piaţa internă (directiva privind comerţul electronic).

LEGISLAȚIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

DECIZII

- 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 ţări terţe în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului.
- Decizia 2010/365/UE din 29 iunie 2010 privind aplicarea dispoziţiilor acquis-ului Schengen referitoare la Sistemul de Informaţii Schengen în Republica Bulgaria şi în România.
- Decizia Comisiei din 5 februarie 2010 privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în ţări terţe în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului (2010/87/UE).
- Decizia 2009/371/JAI din 6 aprilie 2009 privind înfiinţarea Oficiului European de Poliţie (Europol), CONSILIUL UNIUNII EUROPENE.
- Decizia 2008/633/JAI a Consiliului din 23 iunie 2008 privind accesul la Sistemul de Informaţii privind vizele (VIS) în vederea consultării de către autorităţile desemnate ale statelor membre şi de către Europol în scopul prevenirii, depistării şi cercetării infracţiunilor de terorism şi a altor infracţiuni grave.

LEGISLAŢIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

DECIZII

- Decizie cadru 2008/977/JAI privind protecţia datelor cu caracter personal prelucrate în cadrul cooperării poliţieneşti şi judiciare în materie penală.
- Decizia Comisiei din 4 martie 2008 de adoptare a Manualului SIRENE şi a altor dispoziţii de aplicare a Sistemului de Informaţii Schengen din a doua generaţie (SIS II).
- Decizia 2007/533/JAI din 27 iunie 2007 privind instituirea, funcţionarea şi utilizarea Sistemului de Informţii Schengen din a doua generaţie.
- Decizia 2004/915/CE din 27 decembrie 2004 de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentru transferul de date cu caracter personal către ţări terţe.
- Decizia 2001/497/CE din 15 iunie 2001 privind clauzele contractuale standard pentru transferul de date cu caracter personal către ţările terţe în temeiul Directivei 95/46/CE.

LEGISLAȚIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

CONVENŢII

Convenţie din 19 iunie 1990 de aplicare a acordului de la Schengen din 14 iunie 1985 privind eliminarea graduala a controalelor la frontierele comune, Schengen, 19 iunie 1990.

Convenţie privind înfiinţarea Oficiului European de Poliţie, în temeiul art. K.3 din Tratatul privind Uniunea Europeană (Convenţia Europol).

Convenţia de la Prum - Schengen III.

LEGISLAŢIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

REGULAMENTE

- 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 (Regulamentul general privind protecţia datelor).
- Regulamentul (CE) nr. 810/2009 al Parlamentului European şi al Consiliului privind instituirea unui Cod comunitar de vize.
- Regulamentul (CE) nr. 767/2008 al Parlamentului European şi al Consiliului privind Sistemul de Informaşii privind vizele (VIS) şi schimbul de date între statele membre cu privire la vizele de scurtă şedere.
- Regulamentul (CE) nr. 1987/2006 al Parlamentului European şi al Consiliului privind instituirea, funcţionarea şi utilizarea Sistemului de Informaţii Schengen din a doua generaţie (SIS II).
- Regulamentul (CE) nr. 1986/2006 al Parlamentului European şi al Consiliului privind accesul la Sistemul de Informaţii Schengen din a doua generaţie (SIS II) al serviciilor competente, în statele membre, pentru eliberarea certificatelor de înmatriculare a vehiculelor.

LEGISLAȚIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

RECOMANDĂRI

- Recomandarea 2009/387/CE din 12 mai 2009 privind aplicarea principiilor de respectare a vieţii private şi protecţie a datelor în aplicaţiile bazate pe identificarea prin radiofrecvenţă.
- Recomandarea NR. R (87) 15 a comitetului de ministri ai statelor membre ce reglementează utilizarea datelor personale în sectorul poliţienesc.

LEGISLAȚIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

GRUPUL DE LUCRU ART. 29/ DIRECTIVA 95/46/CE a PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI

Articolul 29 Grupul de lucru pentru protecţia persoanelor în ceea ce privete prelucrarea datelor cu caracter personal

1. Se instituie un grup de lucru pentru protecţia persoanelor în ceea ce priveşte prelucrarea datelor cu caracter personal, denumit în continuare „grup de lucru". Grupul de lucru are caracter consultativ şi acţionează independent.

2. Grupul de lucru este compus dintr-un reprezentant al autorităţii sau al autorităţilor de supraveghere desemnate de fiecare stat membru, dintr-un reprezentant al autorităţii sau al autorităţilor create pentru instituţiile şi organismele comunitare şi dintr-un reprezentant al Comisiei. Fiecare membru al grupului de lucru este desemnat de instituţia, autoritatea sau autorităţile pe care le reprezintă. Dacă un stat membru a desemnat mai multe autorităţi de supraveghere, acestea procedează la nominalizarea unui reprezentant comun. Acelaşi lucru se aplică autorităţilor create pentru instituţiile şi organismele comunitare.

3. Grupul de lucru decide cu majoritatea simplă a reprezentanţilor autorităţilor de supraveghere.

4. Grupul de lucru îşi alege preşedintele. Durata mandatului preşedintelui este doi ani. Mandatul poate fi reînnoit.

5. Secretariatul grupului de lucru este asigurat de Comisie.

6. Grupul de lucru îşi adoptă regulamentul de procedură.

7. Grupul de lucru ia în discuţie subiectele înscrise pe ordinea de zi de către preşedinte, fie din iniţiativa acestuia, fie la cererea unui reprezentant al autorităţilor de supraveghere sau la cererea Comisiei.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

LEGISLAŢIE EXISTENTĂ LA NIVELUL UNIUNII EUROPENE

OPINII GRUPUL DE LUCRU ART. 29

- Opinia nr. 1/2014 - 27.02.2014 Avizul 01/2014 privind aplicarea necesităţii şi proporţionalităţii conceptelor şi protecţiei datelor în cadrul sectorului de aplicare a legii.
- Opinia nr. 2/2014 - 27.02.2014 referitor la un referenţial privind cerinţele pentru regulile corporatiste obligatorii prezentate autorităţilor naţionale de protecţie a datelor din UE şi pentru regulile transfrontaliere privind protecţia vieţii private prezentate agenţilor APEC cu responsabilităţi în materie de CBPR.
- Opinia nr. 3/2014 - 25.03.2014 privind notificarea încălcărilor securităţii datelor cu caracter personal.
- Opinia nr. 4/2014 - 10.04.2014 privind supravegherea comunicaţiilor electronice în scopul colectării de date operative şi al asigurării securităţii naţionale.
- Opinia nr. 5/2014 - 10.04.2014 privind tehnicile de anonimizare.
- Opinia nr. 6/2014 - 09.04.2014 privind noţiunea de interese legitime ale operatorului de date în temeiul articolului 7 din Directiva 95/46 / CE.
- Opinia nr. 7/2014 - 04.06.2014 privind protecţia datelor cu caracter personal în Quebec.
- Opinia nr. 8/2014 - 16.09.2014 privind evoluţiile recente pe internet ale lucrurilor.
- Opinia nr. 9/2014 - 25.11.2014 privind aplicarea Directivei 2002/58 / CE în cazul dispozitivului de amprentare.
- Ghid de implementare a Deciziei CJUE in cazul Google - 26.11.2014.

LEGISLAȚIE EXISTENTĂ LA NIVEL NAȚIONAL

- Legea nr. 677 din 21 noiembrie 2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date - A FOST ABROGATĂ prin Legea nr. 129/2018.
- Legea nr. 102 din 3 mai 2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, cu modificările şi completările ulterioare.
- Legea nr. 129 din 15 iunie 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.
- LEGE nr. 190 din 18 iulie 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).

LEGISLAȚIE EXISTENTĂ LA NIVEL NAȚIONAL

- Regulamentul de Organizare şi Funcţionare al ANSPDCP din 11 Noiembrie 2005, cu modificările şi completările ulterioare.
- Ordonanţa de Urgenţă nr. 131 din 22 septembrie 2005 pentru prorogarea termenului prevăzut la art. 19 alin. (1) din Legea nr. **102/2005**privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal.
- Legea nr. 278 din 15 octombrie 2007 privind aprobarea Ordonanţei de urgenţă a Guvernului nr. **36/2007** pentru abrogarea Legii nr. **476/2003** privind aprobarea taxei de notificare a prelucrărilor de date cu caracter personal, care cad sub incidenţa Legii nr. **677/2001**pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.
- Legea nr. 682 din 28 noiembrie 2001 privind ratificarea Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981.
- Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.
- Ordonanţa de Urgenţă nr. 13 din 24 aprilie 2012 pentru modificarea şi completarea Legii nr. **506/2004** privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.

LEGISLAȚIE EXISTENTĂ LA NIVEL NAȚIONAL

- Legea nr. 272 din 29 iunie 2006 pentru completarea art. 7 din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice.
- Legea nr. 365 din 7 iunie 2002 privind comerţul electronic*) - Republicare
- Norme metodologice din 20 noiembrie 2002 pentru aplicarea Legii nr. **365/2002** privind comertul electronic.
- Legea nr. 146 din 10 iulie 2008 pentru aderarea României la Tratatul dintre Regatul Belgiei, Republica Federală Germania, Regatul Spaniei, Republica Franceză, Marele Ducat de Luxemburg, Regatul Ţărilor de Jos şi Republica Austria privind aprofundarea cooperării transfrontaliere, în special în vederea combaterii terorismului, criminalităţii transfrontaliere şi migraţiei ilegale, semnat la Prum la 27 mai 2005.
- Legea nr. 238 din 10 iunie 2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice - REPUBLICARE*).

LEGISLAȚIE EXISTENTĂ LA NIVEL NAȚIONAL

Decizie nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal pentru furnizorii de servicii publice de reţele sau servicii de comunicaţii electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securităţii datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European şi a Consiliului privind confidenţialitatea şi comunicaţiile electronice (publicată în Monitorul Oficial 964 din 30.12.2014)Legea nr. 365 din 7 iunie 2002 privind comerţul electronic*) – Republicare.

Decizie nr. 99 din 18 mai 2018 privind încetarea aplicabilităţii unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

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.

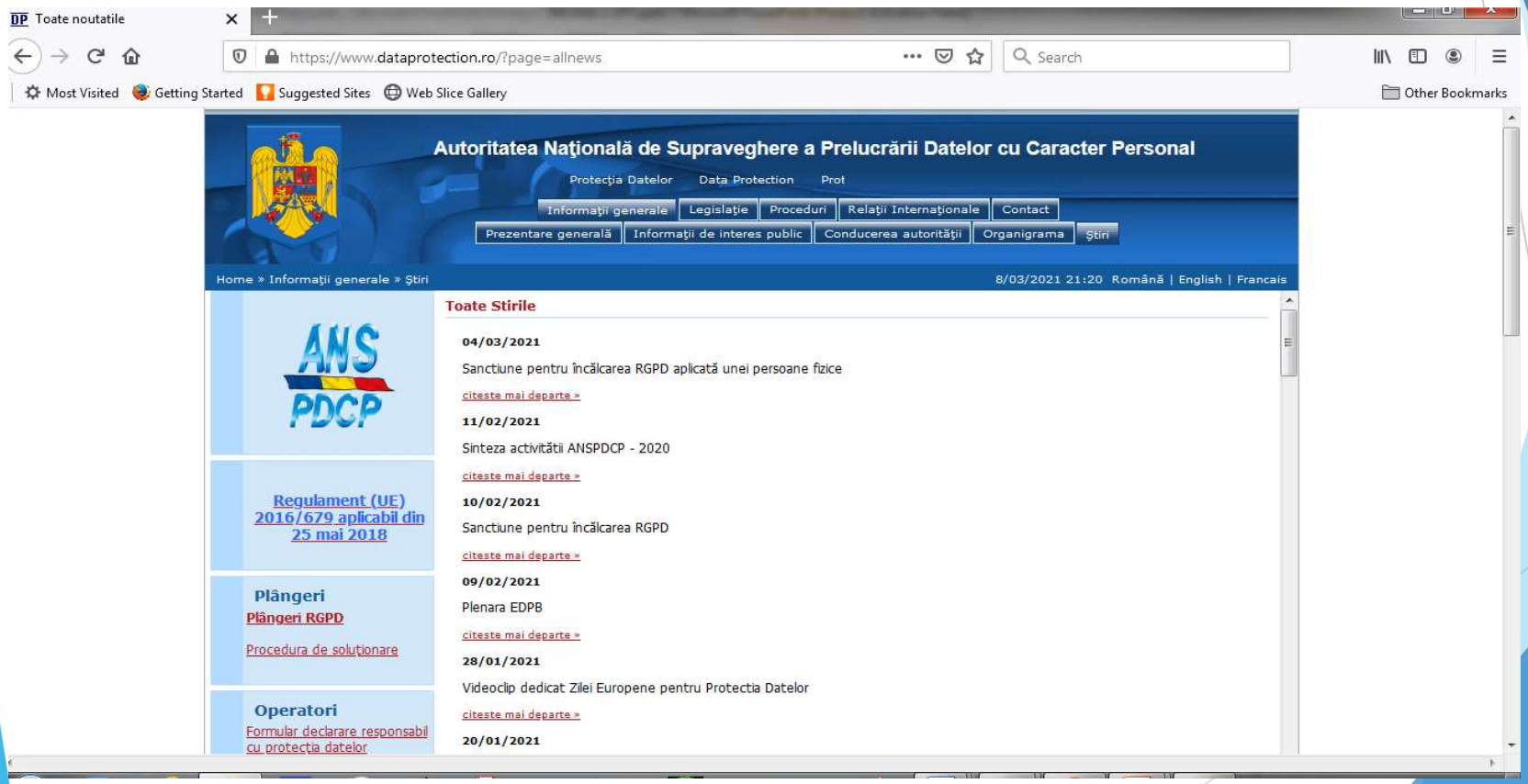
Decizia nr. 133 din 3 iulie 2018 privind aprobarea Procedurii de primire și soluționare a plângerilor.

Decizia nr. 161 din 09 Octombrie 2018 privind aprobarea Procedurii de efectuare a investigațiilor.

Decizia nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020



UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Ing. POPESCU ION

0733.333.333

CNP: 1731212190190

CI: RK 111111

CASATORIT

CLINIC SĂNĂTOS

ionpopescu@yahoo.com

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DATELE CU CARACTER PERSONAL

"Orice informație" - care este colectată sau destinată a fi colectată

- "Referitoare la" - cu conținut, scop sau impact asupra unei persoane
- "Identificat" - se poate efectua identificarea directă a persoanei
- "Sau identificabil" - se poate efectua identificare indirectă
- "Persoana naturală" - date de identificare de la naștere până la moarte

- **CARE POT FI DATELE CU CARACTER PERSONAL?**

DATE GENERALE

- Nume şi prenume
- Gen
- Vârsta
- Data naşterii
- Starea civilă
- Cetăţenie
- Situaţia militară
- Situaţia activităţii – angajat sau pensionar
- Adresa IP

CARE POT FI DATELE CU CARACTER PERSONAL?

NUMĂR DE IDENTIFICARE NAȚIONAL (art. 2, L190/2018)

- Cod numeric Personal (CNP)
- Serie şi număr acte de identitate emis de stat (CI, paşaport)
- Serie şi număr permis de conducere
- Număr asigurare socială de sănătate

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DIRECTOR GENERAL
SC GDPR SRL
Ing. POPESCU ION

0733.333.333
ionpopescu@gdpr.com

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

CARE POT FI DATELE CU CARACTER PERSONAL?

INFORMAȚII DE AFACERI

- Adresă de sediu social/punct de lucru
- Numărul de telefon de afaceri
- Adresa de e-mail de afaceri

- Numărul intern de identificare/serie legitimație de acces
- Alte informații de verificare a identității (date biometrice pentru acces)

CARE POT FI DATELE CU CARACTER PERSONAL?
CATEGORII SPECIALE DE DATE CU CARACTER PERSONAL

- Originea rasială/etnică
- Opiniile politice
- Religii sau credinţe filosofice
- Apartenenţa la un partid sau sindicat
- Datele biometrice
- Datele privind:
  - Sănătatea
  - Orientarea sexuală
  - Viaţa sexuală
  - Date genetice
- Date referitoare la:
  - Condamnari penale
  - Infractiuni
  - Interdicţii
- Date privind copiii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

CE ESTE RGPD/GDPR?

Regulamentul (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) **se aplica din 25 mai 2018.**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

CE FACE?

„ (1) *Prezentul regulament* ***stabileşte normele*** *referitoare la* ***protecţia persoanelor fizice*** *în ceea ce priveşte* ***prelucrarea datelor cu caracter personal****, precum şi* ***normele*** *referitoare la* ***libera circulaţie*** *a datelor cu caracter personal.*

(2) *Prezentul regulament asigură* ***protecţia drepturilor şi libertăţilor fundamentale ale persoanelor fizice*** *şi în special a dreptului acestora la* ***protecţia datelor cu caracter personal****.*

(3) ***Libera circulaţie*** *a datelor cu caracter personal în interiorul Uniunii* ***nu poate fi restricţionată sau interzisă*** *din motive legate de protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.* ” art. 1 /RGPD

CE FACE?

- Normele stabilite prin Regulament au **forţă juridică superioară** reglementărilor naţionale.

- Regulamentul priveşte **exclusiv** protecţia persoanelor fizice.

- Regulamentul **stabileşte norme** nu doar cu privire la **prelucrarea** datelor cu caracter personal şi **libera circulaţie** a acestor date, ci şi cu privire la **colectarea, stocarea şi utilizarea** datelor cu caracter personal.

CUI SE APLICĂ?
Domeniul de aplicare material

(1) Prezentul regulament se aplică **prelucrării datelor cu caracter personal**, efectuată total sau parțial prin **mijloace automatizate**, precum și **prelucrării prin alte mijloace** decât cele automatizate a datelor cu caracter personal care **fac parte** dintr-un **sistem de evidență a datelor** sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

CUI NU SE APLICĂ?

Domeniul de aplicare material

Prezentul regulament **nu se aplică** prelucrării datelor cu caracter personal:
(a) în cadrul unei activităţi care nu intră sub incidenţa dreptului Uniunii;
(b) de către statele membre atunci când desfăşoară activităţi care intră sub incidenţa capitolului 2 al titlului V din Tratatul UE (siguranţă naţională);
(c) de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice;
(d) de către autorităţile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracţiunilor, sau al executării sancţiunilor penale, inclusiv al protejării împotriva ameninţărilor la adresa siguranţei publice şi al prevenirii acestora.

CUI SE APLICĂ?

Domeniul de aplicare teritorial

(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

(2) Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activităţile de prelucrare sunt legate de:

(a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată;

sau

(b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

(3) Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internaţional public.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

PRINCIPII

CARE STAU LA BAZA PRELUCRĂRII DATELOR

PRINCIPII

Legalitatea prelucrării – precizează condiţiile în care este legal să se prelucreze date cu caracter personal

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

PRINCIPII

Legalitatea prelucrării – precizează condiţiile în care este legal să se prelucreze date cu caracter personal

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

PRINCIPII

Legalitatea prelucrării – precizează condiţiile în care este legal să se prelucreze date cu caracter personal

- Dacă scopul prelucrării este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcţii publice atribuite operatorului acesta este stabilit pe baza dreptului UE sau cel intern.
- Acesta va conţine dispoziţii specifice privind adaptarea aplicării normelor prezentului regulament, printre altele:
  - condiţiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate;
  - entităţile cărora le pot fi divulgate datele şi scopul pentru care respectivele date cu caracter personal pot fi divulgate;
  - limitările legate de scop;
  - perioadele de stocare;
  - operaţiunile şi procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale şi echitabile.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

PRINCIPII

- **Consimţământul (dacă prelucrarea se bazează pe consimţământ)–** obligativitatea ca operatorul să demonstreze că persoana vizată şi-a dat consimţământul ca datele sale cu caracter personal să fie prelucrate.
- **Prelucrarea de categorii speciale de date cu caracter personal –** este interzisă în general dar se poate efectua în anumite condiţii exprese.

STRUCTURA RGPD - CAPITOLUL II PRINCIPII

- **Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni -** se efectuează, numai sub controlul unei autorităţi de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate.

- **Prelucrarea care nu necesită identificare -** dacă nu este necesară identificarea unei persoane prin prelucrarea datelor operatorul nu va efectua nicio operaţiune de prelucrare în scopul identificării acelei persoane.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

Desemnarea responsabilului cu protecţia datelor

Operatorul şi persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

- prelucrarea este efectuată de o autoritate sau un organism public, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;
- activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă; sau
- activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale şi infracţiuni;
- prelucrează un număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, în scopul prevăzut la art. 6, alin. (1), lit. f) din Regulamentul general privind protecţia datelor, respectiv al realizării intereselor legitime urmărite de operator sau de o parte terţă. (pct. (2), art. 4, L190/2018).

Funcţia responsabilului cu protecţia datelor

Sarcinile responsabilului cu protecţia datelor

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Modul 2: Drepturile şi obligaţiile organizaţiei în prelucrarea datelor cu caracter personal. Instrumente de informare

- Drepturile şi obligaţiile împuternicitului în prelucrarea datelor cu caracter personal. Aspecte particulare cu privire la prelucrarea datelor sensibile
- Relaţia operator – împuternicit. Drepturi, responsabilităţi, prevederi contractuale obligatorii
- Drepturile şi obligaţiile operatorului în prelucrarea datelor cu caracter personal. Aspecte particulare cu privire la prelucrarea datelor sensibile
- Temeiurile de prelucrare a datelor cu caracter personal
- Prelucrarea datelor cu caracter personal în temeiul consimţământului persoanei vizate. Condiţii speciale aplicabile în ceea ce priveşte consimţământul minorilor

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă

DATE CU CARACTER PERSONAL - orice informaţii 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale

DATE GENETICE - datele cu caracter personal referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză

DATE BIOMETRICE - date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice

DATE PRIVIND SĂNĂTATEA - date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi 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

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregis trarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea

SISTEM DE EVIDENŢĂ A DATELOR - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice

CREARE DE PROFILURI - 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 performanţa la locul de muncă, situaţia economică, sănătatea, preferinţele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia

PRINCIPIILE PRELUCRĂRII

datele cu caracter personal sunt:

- prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată („legalitate, echitate şi transparenţă”);

- colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale, în conformitate cu articolul 89 alineatul (1) („limitări legate de scop”);

- adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);

- exacte şi, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere („exactitate”);

- păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic şi organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor şi libertăţilor persoanei vizate („limitări legate de stocare”);

- prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate şi confidenţialitate”).

Operatorul este **responsabil de respectarea principiilor prelucrării** şi **poate demonstra** această respectare.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Ing. POPESCU ION

0733.333.333

CNP: 1731212190190

CI: RK 111111

CASATORIT

CLINIC SĂNĂTOS

ionpopescu@yahoo.com

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DIRECTOR GENERAL
SC GDPR SRL
Ing. POPESCU ION

0733.333.333
ionpopescu@gdpr.com

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Responsabilitatea operatorului

ANALIZEAZĂ ŞI EVALUEAZĂ

- natura
- domeniul de aplicare
- contextul
- scopurile prelucrării
- riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice

IMPLEMENTEAZĂ

- măsuri tehnice şi organizatorice adecvate pentru a garanta şi demonstra că prelucrarea se efectuează în conformitate cu R.G.P.D.

Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Securitatea prelucrării datelor cu caracter personal

Operatorul şi persoana împuternicită de acesta trebuie să implementeze **măsuri tehnice şi organizatorice** adecvate în vederea asigurării unui nivel de securitate datelor cu caracter personal (transmise, stocate sau prelucrate într-un alt mod) care să includă cel puţin:

- pseudonimizarea şi criptarea datelor cu caracter personal;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

La evaluarea nivelului adecvat de securitate, se ţine seama în special de riscurile prezentate de prelucrare, generate în special, în mod **accidental sau ilegal**, de:

- distrugerea;
- pierderea;
- modificarea;
- divulgarea neautorizată;
- accesul neautorizat.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

ATENŢIE!

Măsurile minime de protecţie a datelor cu caracter personal sunt:

- măsuri de securitate fizică;

- măsuri de securitate a personalului;

- măsuri de securitate informatică.

Măsurile aplicate sunt constituite dintr-un cumul de acţiuni şi proceduri menite să asigure scopul enunţat.

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Operatori asociaţi - doi sau mai mulţi operatori stabilesc în comun scopurile şi mijloacele de prelucrare

Ei stabilesc într-un mod transparent responsabilităţile fiecăruia în ceea ce priveşte îndeplinirea obligaţiilor care le revin în temeiul R.G.P.D., în special în ceea ce priveşte exercitarea drepturilor persoanelor vizate şi îndatoririle fiecăruia de furnizare a informaţiilor, prin intermediul unui acord între ei, cu excepţia cazului şi în măsura în care responsabilităţile operatorilor sunt stabilite în dreptul Uniunii sau în dreptul intern care se aplică acestora.
Acordul poate să desemneze un punct de contact pentru persoanele vizate.

Reprezentanţii operatorilor sau ai persoanelor împuternicite de operatori care nu îşi au sediul în Uniune

Operatorul sau persoana împuternicită de operator desemnează în scris un reprezentant în Uniune.

Obligaţia nu se aplică:

- prelucrării care are un caracter ocazional, care nu include, pe scară largă, prelucrarea unor categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau prelucrarea unor date cu caracter personal referitoare la condamnări penale şi infracţiuni menţionată la articolul 10, şi care este puţin susceptibilă de a genera un risc pentru drepturile şi libertăţile persoanelor, ţinând cont de natura, contextul, domeniul de aplicare şi scopurile prelucrării; sau
- unei autorităţi sau unui organism public.

Reprezentanţii operatorilor sau ai persoanelor împuternicite de operatori care nu îşi au sediul în Uniune

Reprezentantul îşi are sediul în unul dintre statele membre în care se află persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri şi servicii sau al căror comportament este monitorizat.

Reprezentantul primeşte din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autorităţile de supraveghere şi persoanele vizate, în special, se pot adresa reprezentantului, în plus faţă de operator sau persoana împuternicită de operator sau în locul acestora, cu privire la toate chestiunile legate de prelucrarea, în scopul asigurării respectării prezentului regulament.

Desemnarea unui reprezentant de către operator sau persoana împuternicită de operator nu aduce atingere acţiunilor în justiţie care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator înseşi.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Persoana împuternicită de operator

În cazul în care prelucrarea urmează să fie realizată în numele unui operator, persoanele împuternicite oferă garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să respecte cerintele de securitate a datelor şi să asigure protecţia drepturilor persoanei vizate.

Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizaţie scrisă, specifică sau generală, din partea operatorului.

Persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecţii faţă de aceste modificări.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

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

Contractul sau acul juridic prevede în special că persoană împuternicită de operator:

- prelucrează datele cu caracter personal numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;
- se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;
- adoptă toate măsurile necesare în vederea asigurării securităţii datelor;
- oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea drepturilo de către persoana vizată;
- ajută operatorul să asigure respectarea obligaţiilor de asigurare a securităţii datelor;
- la alegerea operatorului, şterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;
- pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditurilor, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Desfăşurarea activităţii de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de operator – PERSOANA AUTORIZATĂ

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

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Prelucrarea unui număr de identificare naţional

Statele membre pot detalia în continuare condiţiile specifice de prelucrare a unui număr de identificare naţional sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare naţional sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanţii corespunzătoare pentru drepturile şi libertăţile persoanei vizate în temeiul prezentului regulament.

Prelucrarea în contextul ocupării unui loc de muncă

Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecţia drepturilor şi a libertăţilor cu privire la prelucrarea datelor cu caracter personal ale angajaţilor în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligaţiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării şi organizării muncii, al egalităţii şi diversităţii la locul de muncă, al asigurării sănătăţii şi securităţii la locul de muncă, al protejării proprietăţii angajatorului sau a clientului, precum şi în scopul exercitării şi beneficierii, în mod individual sau colectiv, de drepturile şi beneficiile legate de ocuparea unui loc de muncă, precum şi pentru încetarea raporturilor de muncă.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Garanţii şi derogări privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice

Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice are loc cu condiţia existenţei unor garanţii corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile şi libertăţile persoanelor vizate. Respectivele garanţii asigură faptul că au fost instituite măsuri tehnice şi organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivele măsuri pot include pseudonimizarea, cu condiţia ca respectivele scopuri să fie îndeplinite în acest mod. Atunci când respectivele scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.

Normele existente în domeniul protecţiei datelor pentru biserici şi asociaţii religioase

În cazul în care, într-un stat membru, bisericile şi asociaţiile sau comunităţile religioase aplică, la data intrării în vigoare a RGPD, un set cuprinzător de norme de protecţie a persoanelor fizice cu privire la prelucrare, aceste norme pot continua să se aplice, cu condiţia să fie aliniate la RGPD.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

În legislaţia naţională armonizată, respectiv, la Art. 2 din Legea 190/2018 se particularizează termenii:

AUTORITĂŢI ŞI ORGANISME PUBLICE - Camera Deputaţilor şi Senatul, Administraţia Prezidenţială, Guvernul, ministerele, celelalte organe de specialitate ale administraţiei publice centrale, autorităţile şi instituţiile publice autonome, autorităţile administraţiei publice locale şi deja nivel judeţean, alte autorităţi publice, precum şi instituţiile din subordinea/coordonarea acestora. În sensul prezentei legi, sunt asimilate autorităţilor/organismelor publice şi unităţile de cult şi asociaţiile şi fundaţiile de utilitate publică;"

ÎNDEPLINIREA UNEI SARCINI CARE SERVEŞTE UNUI INTERES PUBLIC - include acele activităţi ale partidelor politice sau ale organizaţiilor cetăţenilor aparţinând minorităţilor naţionale, ale organizaţiilor neguvernamentale, care servesc realizării obiectivelor prevăzute de dreptul constituţional sau de dreptul internaţional public ori funcţionării sistemului democratic, incluzând încurajarea participării cetăţenilor în procesul de luare a deciziilor şi a pregătirii politicilor publice, respectiv promovarea principiilor şi valorilor democraţiei.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

NUMĂR DE IDENTIFICARE NAŢIONAL - numărul prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care are aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul paşaportului, al permisului de conducere, numărul de asigurare socială de sănătate.

Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, în scopul prevăzut la art. 6 alin. (1) lit. f) din Regulamentul general privind protecţia datelor, respectiv al realizării intereselor legitime urmărite de operator sau de o parte terţă, se efectuează cu instituirea de către operator a următoarelor garanţii:

- punerea în aplicare de măsuri tehnice şi organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum şi pentru asigurarea securităţii şi confidenţialităţii prelucrărilor de date cu caracter personal, conform dispoziţiilor art. 32 din Regulamentul general privind protecţia datelor;
- numirea unui responsabil pentru protecţia datelor, în conformitate cu prevederile art. 10 din prezenta lege;
- stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii;
- instruirea periodică cu privire la obligaţiile ce le revin a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

PRELUCRAREA UNUI NUMĂR DE IDENTIFICARE NAŢIONAL

Art. 6 alin. (1) din Regulamentul general privind protecţia datelor.

Articolul 6/GDPR **Legalitatea prelucrării**

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

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

(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

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

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

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este 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.

Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Prelucrarea datelor cu caracter personal în contextul relaţiilor de muncă

În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de uncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

- interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;
- angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;
- angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor;
- înainte de introducerea sistemelor de monitorizare;
- alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa;
- durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Prelucrarea datelor cu caracter personal şi de categorii speciale de date cu caracter personal, în contextul îndeplinirii unei sarcini care serveşte unui interes public se efectuează cu instituirea de către operator sau de către partea terţă a următoarelor garanţii:

- punerea în aplicare a măsurilor tehnice şi organizatorice adecvate pentru respectarea principiilor enumerate la art. 5 din Regulamentul general privind protecţia datelor, în special a reducerii la minimum a datelor, respectiv a principiului integrităţii şi confidenţialităţii;
- numirea unui responsabil pentru protecţia datelor, dacă aceasta este necesară în conformitate cu art. 10 din L190/2018;
- stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Garanţii:

- informarea persoanei vizate despre prelucrarea datelor cu caracter personal;
- garantarea transparenţei informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate;
- garantarea dreptului de rectificare şi ştergere.

OBS: Prelucrarea se poate efectua fără consimţământul expres al persoanei vizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Modul 3: Drepturile şi obligaţiile persoanelor implicate în prelucrarea datelor cu caracter personal. Instrumente de informare

Drepturile şi obligaţiile persoanei vizate cu privire la prelucrarea datelor cu caracter personal;

Categorii de drepturi, informaţii care se furnizează persoanei vizate, modalitatea de exercitare a acestor drepturi;

Aspecte particulare cu privire la prelucrarea datelor sensibile.

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

- un nume,
- un număr de identificare
- date de localizare
- un identificator online
- sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate:

- **colectarea,**
- **înregistrarea,**
- **organizarea,**
- **structurarea,**
- **stocarea,**
- **adaptarea sau modificarea,**
- **extragerea,**
- **consultarea,**
- **utilizarea,**
- **divulgarea prin transmitere,**
- **diseminarea sau punerea la dispoziţie în orice alt mod,**
- **alinierea sau combinarea,**
- **restricţionarea,**
- **ştergerea**
- **distrugerea**

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

ACT ADITIONAL - MODEL

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

SISTEM DE EVIDENȚĂ A DATELOR - orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice

CREARE DE PROFILURI - 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:

- **performanţa la locul de muncă**
- **situaţia economică**
- **sănătatea**
- **preferinţele personale**
- **interesele**
- **fiabilitatea**
- **comportamentul**
- **locul în care se află persoana fizică respectivă**
- **deplasările acesteia**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

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

INFORMARE CU PRIVIRE LA PRELUCRAREA DATELOR CU CARACTER PERSONAL
ANGAJAŢI
CLIENȚI

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Ing. POPESCU ION

0733.333.333

CNP: 1731212190190

CI: RK 111111

CASATORIT

CLINIC SĂNĂTOS

ionpopescu@yahoo.com

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL III DREPTURILE PERSOANEI VIZATE

- ***Secţiunea 1 - Transparenţă şi modalităţi***
- ***Secţiunea 2 - Informare şi acces la date cu caracter personal***
- ***Secţiunea 3 - Rectificare şi ştergere***
- ***Secţiunea 4 - Dreptul la opoziţie şi procesul decizional individual automatizat***
- ***Secţiunea 5 - Restricţii***

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Informare şi acces la date cu caracter personal

Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate

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

- identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
- datele de contact ale responsabilului cu protecţia datelor;
- scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
- în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terţă;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Informare şi acces la date cu caracter personal

informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă:

- perioada pentru care vor fi stocate datele cu caracter personal;
- existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;
- dacă prelucrarea se bazează pe consimţământul persoanei vizate, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
- dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
- dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;
- existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Informare şi acces la date cu caracter personal - MODEL

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

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

În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informaţii:

- identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
- datele de contact ale responsabilului cu protecţia datelor, după caz;
- scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
- categoriile de date cu caracter personal vizate;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Dreptul de acces al persoanei vizate

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

- scopurile prelucrării;
- categoriile de date cu caracter personal vizate;
- destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţări terţe sau organizaţii internaţionale;
- acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- existenţa drepturilor persoanei vizate în ceea ce priveşte datele sale personale;
- în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;
- existenţa unui proces decizional automatizat incluzând crearea de profiluri, şi informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

- MODEL -

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

- **Dreptul la rectificare**

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

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

- **Dreptul la ştergerea datelor („dreptul de a fi uitat”)**

Persoana vizată are dreptul de a solicita şi obţine din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligaţia de a şterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

- datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- persoana vizată îşi retrage consimţământul pe baza căruia are loc prelucrarea;
- persoana vizată se opune prelucrării şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau persoana vizată se opune prelucrării scopuri de marketing;
- datele cu caracter personal au fost prelucrate ilegal;
- datele cu caracter personal trebuie şterse pentru respectarea unei obligaţii legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidenţa căruia se af lă operatorul;
- datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societăţii informaţionale direct unui copil.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

- **Dreptul la ştergerea datelor („dreptul de a fi uitat”)**

Dacă operatorul care a făcut publice datele cu caracter personal este obligat să le şteargă, ţinând seama de tehnologia disponibilă şi de costul implementării. Va lua măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii cu care colaborează că persoana vizată a solicitat ştergerea de către aceşti operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

Aceste prevederi nu se aplică dacă prelucrarea este necesară:

- pentru exercitarea dreptului la liberă exprimare şi la informare;
- pentru respectarea unei obligaţii legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este învestit operatorul;
- din motive de interes public în domeniul sănătăţii publice;
- în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice;
- pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Dreptul la restricţionarea prelucrării

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

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

În cazul în care prelucrarea a fost restricţionată, datele cu caracter personal pot, cu excepţia stocării, să fie prelucrate numai cu consimţământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau pentru protecţia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

❖Dreptul la portabilitatea datelor

Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc dacă acestea au fost furnizate operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, dacă prelucrarea se bazează pe consimţământul persoanei vizate sau pe un contract precum şi în situaţia în care prelucrarea este efectuată prin mijloace automate.

Persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

❖ **Dreptul la opoziţie**

În orice moment, persoana vizată are dreptul de a se opune, din motive legate de situaţia particulară în care se află, prelucrării datelor cu caracter personal care o privesc, inclusiv creării de profiluri.

Operatorul nu va mai prelucra acele datele, cu excepţia cazului în care poate să demonstreze că are motive legitime şi imperioase care prevalează asupra intereselor, drepturilor şi libertăţilor persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţă.

Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct sau crearea de profiluri, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor care o privesc, situaţie în care datele cu caracter personal nu mai sunt prelucrate în acele scopuri.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Procesul decizional individual automatizat, inclusiv crearea de profiluri

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

Excepţii:

- este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date;
- este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate; sau
- are la bază consimţământul explicit al persoanei vizate.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Restricţii

Dreptul UE sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricţiona printr-o măsură legislativă domeniul de aplicare al obligaţiilor şi al drepturilor pentru a asigura:

- securitatea naţională;
- apărarea;
- securitatea publică;
- prevenirea, investigarea, depistarea sau urmărirea penală a infracţiunilor sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa securităţii publice şi prevenirea acestora;
- alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;
- protejarea independenţei judiciare şi a procedurilor judiciare;
- prevenirea, investigarea, depistarea şi urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
- funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii oficiale;
- protecţia persoanei vizate sau a drepturilor şi libertăţilor altora;
- punerea în aplicare a pretenţiilor de drept civil.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Modul 3: Drepturile şi obligaţiile persoanelor implicate în prelucrarea datelor cu caracter personal. Instrumente de informare

Drepturile şi obligaţiile persoanei vizate cu privire la prelucrarea datelor cu caracter personal;

Categorii de drepturi, informaţii care se furnizează persoanei vizate, modalitatea de exercitare a acestor drepturi;

Aspecte particulare cu privire la prelucrarea datelor sensibile.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL III DREPTURILE PERSOANEI VIZATE

- ***Secţiunea 1 - Transparenţă şi modalităţi***
- ***Secţiunea 2 - Informare şi acces la date cu caracter personal***
- ***Secţiunea 3 - Rectificare şi ştergere***
- ***Secţiunea 4 - Dreptul la opoziţie şi procesul decizional individual automatizat***
- ***Secţiunea 5 - Restricţii***

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate:

- **colectarea,**
- **înregistrarea,**
- **organizarea,**
- **structurarea,**
- **stocarea,**
- **adaptarea sau modificarea,**
- **extragerea,**
- **consultarea,**
- **utilizarea,**
- **divulgarea prin transmitere,**
- **diseminarea sau punerea la dispoziţie în orice alt mod,**
- **alinierea sau combinarea,**
- **restricţionarea,**
- **ştergerea**
- **distrugerea**

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Ing. POPESCU ION

0733.333.333

CNP: 1731212190190

CI: RK 111111

CASATORIT

CLINIC SĂNĂTOS

ionpopescu@yahoo.com

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Informare şi acces la date cu caracter personal

Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate

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

- identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
- datele de contact ale responsabilului cu protecţia datelor;
- scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
- în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terţă;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Informare şi acces la date cu caracter personal

informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă:

- perioada pentru care vor fi stocate datele cu caracter personal;
- existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;
- dacă prelucrarea se bazează pe consimţământul persoanei vizate, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
- dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
- dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;
- existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

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

În cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informaţii:

- identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia;
- datele de contact ale responsabilului cu protecţia datelor, după caz;
- scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
- categoriile de date cu caracter personal vizate;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Procesul decizional individual automatizat, inclusiv crearea de profiluri

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

Excepţii:

- este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date;
- este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate; sau
- are la bază consimţământul explicit al persoanei vizate.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Restricţii

Dreptul UE sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricţiona printr-o măsură legislativă domeniul de aplicare al obligaţiilor şi al drepturilor pentru a asigura:

- securitatea naţională;
- apărarea;
- securitatea publică;
- prevenirea, investigarea, depistarea sau urmărirea penală a infracţiunilor sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa securităţii publice şi prevenirea acestora;
- alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, inclusiv în domeniile monetar, bugetar şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;
- protejarea independenţei judiciare şi a procedurilor judiciare;
- prevenirea, investigarea, depistarea şi urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
- funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii oficiale;
- protecţia persoanei vizate sau a drepturilor şi libertăţilor altora;
- punerea în aplicare a pretenţiilor de drept civil.

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Condiţii aplicabile în ceea ce priveşte consimţământul copiilor în legătură cu serviciile societăţii informaţionale

În cazul în care se aplică articolul 6 alineatul (1) litera (a) - persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale - în ceea ce priveşte oferirea de servicii ale societăţii informaţionale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puţin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă şi în măsura în care consimţământul respectiv este acordat sau autorizat de titularul răspunderii părinteşti asupra copilului.

Statele membre pot prevedea prin lege o vârstă inferioară în aceste scopuri, cu condiţia ca acea vârstă inferioară să nu fie mai mică de 13 ani.

Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părinteşti a acordat sau a autorizat consimţământul, ţinând seama de tehnologiile disponibile.

Condiţiile prelucrării DCP nu afectează dreptul general al contractelor aplicabil în statele membre, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

Prelucrarea de categorii speciale de date cu caracter personal

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

Prelucrarea de categorii speciale de date cu caracter personal

- persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepţia cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicţia prevăzută la alineatul (1) să nu poată fi ridicată prin consimţământul persoanei vizate;
- prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forţei de muncă şi al securităţii sociale şi protecţiei sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanţii adecvate pentru drepturile fundamentale şi interesele persoanei vizate;
- prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-şi da consimţământul;
- prelucrarea este efectuată în cadrul activităţilor lor legitime şi cu garanţii adecvate de către o fundaţie, o asociaţie sau orice alt organism fără scop lucrativ şi cu specific politic, filozofic, religios sau sindical, cu condiţia ca prelucrarea să se refere numai la membrii sau la foştii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale şi ca datele cu caracter personal să nu fie comunicate terţilor fără consimţământul persoanelor vizate;
- prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare; (g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate;
- prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate;
- prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării condiţiilor şi garanţiilor prevăzute la alineatul (3);
- prelucrarea este necesară din motive de interes public în domeniul sănătăţii publice, cum ar fi protecţia împotriva ameninţărilor transfrontaliere grave la adresa sănătăţii sau asigurarea de standarde ridicate de calitate şi siguranţă a asistenţei medicale şi a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, în special a secretului profesional; sau
- prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în baza dreptului Uniunii sau a dreptului intern, care este proporţional cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor şi prevede măsuri corespun zătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate.
- Datele cu caracter personal pot fi prelucrate în scopuri medicale doar de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naţionale competente sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naţionale competente.
- Statele membre pot menţine sau introduce condiţii suplimentare, inclusiv restricţii, în ceea ce priveşte prelucrarea de date genetice, date biometrice sau date privind sănătatea.

Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni

Prelucrarea de date cu caracter personal referitoare la condamnări penale şi infracţiuni sau la măsuri de securitate conexe în temeiul articolului 6 alineatul (1) se efectuează numai sub controlul unei autorităţi de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern care prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ţine numai sub controlul unei autorităţi de stat.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

SCOPUL

Colectarea, utilizarea, prelucrarea si furnizarea datelor cu caracter personal se face exclusiv in vederea realizarii scopului pentru care au fost colectate si anume: incheierea contractelor de munca, acordarea unor bonusuri sau a altor drepturi salariale, recrutare forta de munca, imputernicirea privind utilizarea mijloacelor de transport auto ale organizatiei, executarea in bune conditii a contratelor comerciale incheiate de operator ,etc. si numai in numele si pentru client, respectand prevederile RGPD, dreptul UE si a legislatiei romane in domeniu.

PERSONELE VIZATE

Persoane fizice: angajaţi.

CATEGORIILE DE DATE PERSONALE COLECTATE

- **date de identificare**: nume, prenume, sex, data nasterii, CNP, serie si numar act de identitate, nationalitatea, starea civila, adresa de domiciliu sau de resedinta, locul si data nasterii;
- **date de contact:** adresa, email, tel/mobil;
- **date privind sănătatea;**
- **date privind pregătirea profesională**: educaţie, studii, training uri, calificări, certificări
- **date antropometrice si fizionomice:** imagini obţinute în urma activităţii de supraveghere.

Prelucrarea datelor cu caracter personal, se face in urma obtinerii consimtamantului persoanei vizate.

BAZA LEGALĂ A PRELUCRĂRII

Legea nr. 53/2003, HG 500/2011

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

METODELOR TEHNICE DE PRELUCRARE

- manual – preluarea documentelor fizice care conţin DCP - suport hârtie (tipărit sau scris de mană);
- automat/informatic - introducerea datelor în format digital în aplicaţii sau tipizate pe sisteme de calcul
  - suport informatic – dispozitiv de transport (stick);
  - suport informatic - sistemul informatic al organizatiei (calculatoare, servere, etc.).

TERŢI CARORA LI SE TRANSMIT PRELUCRĂRILE/DATELE

- Instituţii de stat (ITM, ANAF, etc.)
- Instituţii bancare (plată salarii, etc.)
- Colaboratori (servicii externe de SSM, PSI-SU, Med. Mun, etc.)

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie) Neintomirea sau intocmirea defectuoasa de documente Acces neautorizat la baza de date sau documente Furtul de documente de catre terte persoane Distrugerea de documente de catre terte persoane Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

MĂSURI TEHNICE ŞI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT DE HARTIE

- Spaţiile de stocare (încăperile unde sunt amplasate seifurile de păstrare /stocare) sunt identificate şi protejate, şi se aflate în posesia operatorului;
- documentele ce conţin date cu caracter personal (DCP), sunt păstrate în fişete speciale, dotate cu încuietori pentru a asigura securitatea acestora;
- imprimarea datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru aceasta operaţiune de către operator şi pentru scopul pentru care aceste date au fost furnizate;
- reziduurile în format de hârtie care conţin date şi documente vor fi distruse într-un mod securizat cu dispozitive de tocat hârtii;
- la părăsirea locului de muncă, utilizatorii trebuie sa închidă în fişete documentele ce conţin DCP, dacă în aceeaşi incintă mai au acces şi alte persoane care nu au legătură cu DCP prelucrate sau alte persoane străine;
- limitarea accesului persoanelor străine, neînsoţite în spaţiile unde se prelucrează/păstrează DCP;
- documentelor ce conţin DCP, care au depăşit termenul de arhivare/păstrare în conformitate cu prevederile legale şi/sau procedurilor interne, sunt distruse. La momentul distrugerii se va încheia un Proces Verbal in care vor fi menţionate numerele de dosare ce au fost distruse şi modalitatea de distrugere.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

MĂSURI TEHNICE ŞI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT ELECTRONIC

- Tehnica de calcul care stochează date cu caracter personal, va fi amplasata în spatii identificate ăi protejate, aflate în posesia operatorului, la care au acces doar persoanele împuternicite.
- Datele cu caracter personal vor putea fi înregistrate pe suport mobil (stick USB/memorie externă, disc optic) numai dacă respectivul suport a fost securizat, astfel încât datele pe care le conţine sa nu poată fi citite/recuperate/copiate/extrase de pe suport, decat dupa introducerea unui/unor coduri speciale de securitate şi doar cu acordul conducătorului operatorului.
- Operatorul de date cu caracter personal va întocmi o evidenta a tehnicii de calcul utilizata si a persoanelor autorizate sa o foloseasca, la care poate atasa fisele care atesta instruirea personalului angajat in acest scop. Acestea trebuie sa aiba incheiate raporturi de munca cu operatorul (contracte de munca, contracte de colaborare, contracte de prestari servicii)
- Mentenanţa, modernizările Şi orice intervenţie asupra sistemului informatic prin intermediul cărora se sunt accesate DCP sunt făcute doar de către persoane autorizate în acest sens de către operator.

DURATA DE PRELUCRARE/PĂSTRARE/DISTRUGERE

MEF 3512/2008 şi Anexa 6 a Legii Arhivelor Naţionale stabilesc următoarele termene de păstrare:

50 de ani – statele de plată
75 de ani – dosarele de personal
contractele de muncă
convenţiile civile de prestări servicii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

Modul 4: Identificarea instrumentelor de monitorizare a modului în care organizaţia respectă prevederile legislaţiei privind protecţia datelor cu caracter personal, organizarea şi utilizarea acestora în cadrul organizaţiei

Politici şi instrumente care pot fi aplicate în vederea monitorizării modului în care organizaţia respectă prevederile legislaţiei privind protecţia datelor cu caracter personal

Activităţi periodice sau ad-hoc care pot fi desfăşurate pentru verificarea modului în care sunt implementate cerinţele tehnice şi organizatorice adecvate prelucrării datelor cu caracter personal

Identificarea cazurilor în care este necesară externalizarea activităţii de verificare

Evidenţa activităţilor de prelucrare a datelor cu caracter personal

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

SCOPUL

Colectarea, utilizarea, prelucrarea si furnizarea datelor cu caracter personal se face exclusiv in vederea realizarii scopului pentru care au fost colectate si anume: incheierea contractelor de munca, acordarea unor bonusuri sau a altor drepturi salariale, recrutare forta de munca, imputernicirea privind utilizarea mijloacelor de transport auto ale organizatiei, executarea in bune conditii a contratelor comerciale incheiate de operator ,etc. si numai in numele si pentru client, respectand prevederile RGPD, dreptul UE si a legislatiei romane in domeniu.

PERSONELE VIZATE

Persoane fizice: angajaţi.

CATEGORIILE DE DATE PERSONALE COLECTATE

- **date de identificare**: nume, prenume, sex, data nasterii, CNP, serie si numar act de identitate, nationalitatea, starea civila, adresa de domiciliu sau de resedinta, locul si data nasterii;
- **date de contact:** adresa, email, tel/mobil;
- **date privind sănătatea;**
- **date privind pregătirea profesională**: educaţie, studii, training uri, calificări, certificări
- **date antropometrice si fizionomice:** imagini obţinute în urma activităţii de supraveghere.

Prelucrarea datelor cu caracter personal, se face in urma obtinerii consimtamantului persoanei vizate.

BAZA LEGALĂ A PRELUCRĂRII

Legea nr. 53/2003, HG 500/2011

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

METODELOR TEHNICE DE PRELUCRARE

- manual – preluarea documentelor fizice care conţin DCP - suport hârtie (tipărit sau scris de mană);
- automat/informatic - introducerea datelor în format digital în aplicaţii sau tipizate pe sisteme de calcul
  - suport informatic – dispozitiv de transport (stick);
  - suport informatic - sistemul informatic al organizatiei (calculatoare, servere, etc.).

TERŢI CARORA LI SE TRANSMIT PRELUCRĂRILE/DATELE

- Instituţii de stat (ITM, ANAF, etc.)
- Instituţii bancare (plată salarii, etc.)
- Colaboratori (servicii externe de SSM, PSI-SU, Med. Mun, etc.)

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie) Neintomirea sau intocmirea defectuoasa de documente Acces neautorizat la baza de date sau documente Furtul de documente de catre terte persoane Distrugerea de documente de catre terte persoane Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

MĂSURI TEHNICE ŞI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT DE HARTIE

- Spaţiile de stocare (încăperile unde sunt amplasate seifurile de păstrare /stocare) sunt identificate şi protejate, şi se aflate în posesia operatorului;
- documentele ce conţin date cu caracter personal (DCP), sunt păstrate în fişete speciale, dotate cu încuietori pentru a asigura securitatea acestora;
- imprimarea datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru aceasta operaţiune de către operator şi pentru scopul pentru care aceste date au fost furnizate;
- reziduurile în format de hârtie care conţin date şi documente vor fi distruse într-un mod securizat cu dispozitive de tocat hârtii;
- la părăsirea locului de muncă, utilizatorii trebuie sa închidă în fişete documentele ce conţin DCP, dacă în aceeaşi incintă mai au acces şi alte persoane care nu au legătură cu DCP prelucrate sau alte persoane străine;
- limitarea accesului persoanelor străine, neînsoţite în spaţiile unde se prelucrează/păstrează DCP;
- documentelor ce conţin DCP, care au depăşit termenul de arhivare/păstrare în conformitate cu prevederile legale şi/sau procedurilor interne, sunt distruse. La momentul distrugerii se va încheia un Proces Verbal in care vor fi menţionate numerele de dosare ce au fost distruse şi modalitatea de distrugere.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

MĂSURI TEHNICE ŞI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT ELECTRONIC

- Tehnica de calcul care stochează date cu caracter personal, va fi amplasata în spatii identificate ăi protejate, aflate în posesia operatorului, la care au acces doar persoanele împuternicite.
- Datele cu caracter personal vor putea fi înregistrate pe suport mobil (stick USB/memorie externă, disc optic) numai dacă respectivul suport a fost securizat, astfel încât datele pe care le conţine sa nu poată fi citite/recuperate/copiate/extrase de pe suport, decat dupa introducerea unui/unor coduri speciale de securitate şi doar cu acordul conducătorului operatorului.
- Operatorul de date cu caracter personal va întocmi o evidenta a tehnicii de calcul utilizata si a persoanelor autorizate sa o foloseasca, la care poate atasa fisele care atesta instruirea personalului angajat in acest scop. Acestea trebuie sa aiba incheiate raporturi de munca cu operatorul (contracte de munca, contracte de colaborare, contracte de prestari servicii)
- Mentenanţa, modernizările Şi orice intervenţie asupra sistemului informatic prin intermediul cărora se sunt accesate DCP sunt făcute doar de către persoane autorizate în acest sens de către operator.

DURATA DE PRELUCRARE/PĂSTRARE/DISTRUGERE

MEF 3512/2008 şi Anexa 6 a Legii Arhivelor Naţionale stabilesc următoarele termene de păstrare:

50 de ani – statele de plată
75 de ani – dosarele de personal
contractele de muncă
convenţiile civile de prestări servicii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Evidenţele activităţilor de prelucrare

Fiecare operator sau reprezentantul acestuia trebuie să păstreaze **evidenţa activităţilor de prelucrare** desfăşurate care cuprinde **cel puţin**:

- numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Evidenţele activităţilor de prelucrare

Fiecare operator sau persoana împuternicită de operator păstrează o **evidenţă a tuturor categoriilor de activităţi de prelucrare** desfăşurate **în numele operatorului,** care cuprind:

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

Evidenţele pot fi formulate în scris (inclusiv în format electronic).

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Evidenţele activităţilor de prelucrare

Aceste evidenţe **nu sunt obligatorii** în cazul întreprinderilor sau organizaţiilor cu **mai puţin de 250 de angajaţi**, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze **un risc pentru drepturile şi libertăţile persoanelor vizate**, prelucrarea **nu este ocazională** sau prelucrarea **include categorii speciale de date** sau date cu caracter personal referitoare la **condamnări penale şi infracţiuni**.

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

CARTOGRAFIEREA PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

CINE ?

Se înscriu în evidenţa numele şi coordonatele operatorului (şi ale reprezentantului sau legal) şi, dupa caz, ale responsabilului cu protecţia datelor;
Se întocmeşte 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 infracţiunile).

DE CE ?

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

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

CARTOGRAFIEREA PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

CUM?
Se precizează modalitatea/modalităţile tehnice în care sunt colectate şi/sau prelucrate datele cu caracter personal.
CÂT?
Se specifică durata de păstrare a datelor cu caracter personal.
UNDE?
Se menţionează formatul şi locul în care se pastrează datele cu caracter personal.

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI GENERALE	
PG – ALFABETA - 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL
PG – ALFABETA - 02	POLITICA PRIVIND RGPD
PG – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL IN ACTIVITATEA ORGANIZATIEI
PG – ALFABETA - 04	DATELE CU CARACTER PERSONAL CARE TREBUIE PROTEJATE
PG – ALFABETA - 05	MASURI TEHNICE SI ORGANIZATORICE
PG - ALFABETA - 06	PROCEDURA DE ACTIUNE IN SITUATIA UNUI INCIDENT DE SECURITATE
PG - ALFABETA - 07	PROCEDURA DE INTOCMIRE RASPUNS PERSOANA VIZATA

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI INTERNE	
PI – ALFABETA – 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIVIND ACTIVITATEA DE RESURSE UMANE RU
PI – ALFABETA – 02	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CURSURI/FORMARE PROFESIONALA A ADULTILOR
PI – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CONTRACTARI
PI – ALFABETA – 04	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) AFERENTA SERVICIILOR EXTERNALIZATE.
PI – ALFABETA – 05	PASTRAREA DATELOR CU CARACTER PERSONAL
PI – ALFABETA - 06	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) MONITORIZARE VIDEO

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

Modul 4: Identificarea instrumentelor de monitorizare a modului în care organizaţia respectă prevederile legislaţiei privind protecţia datelor cu caracter personal, organizarea şi utilizarea acestora în cadrul organizaţiei

Politici şi instrumente care pot fi aplicate în vederea monitorizării modului în care organizaţia respectă prevederile legislaţiei privind protecţia datelor cu caracter personal

Activităţi periodice sau ad-hoc care pot fi desfăşurate pentru verificarea modului în care sunt implementate cerinţele tehnice şi organizatorice adecvate prelucrării datelor cu caracter personal

Identificarea cazurilor în care este necesară externalizarea activităţii de verificare

Evidenţa activităţilor de prelucrare a datelor cu caracter personal

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie) Neintomirea sau intocmirea defectuoasa de documente Acces neautorizat la baza de date sau documente Furtul de documente de catre terte persoane Distrugerea de documente de catre terte persoane Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

MĂSURI TEHNICE ŞI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT DE HARTIE

- Spaţiile de stocare (încăperile unde sunt amplasate seifurile de păstrare /stocare) sunt identificate şi protejate, şi se aflate în posesia operatorului;
- documentele ce conţin date cu caracter personal (DCP), sunt păstrate în fişete speciale, dotate cu încuietori pentru a asigura securitatea acestora;
- imprimarea datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru aceasta operaţiune de către operator şi pentru scopul pentru care aceste date au fost furnizate;
- reziduurile în format de hârtie care conţin date şi documente vor fi distruse într-un mod securizat cu dispozitive de tocat hârtii;
- la părăsirea locului de muncă, utilizatorii trebuie sa închidă în fişete documentele ce conţin DCP, dacă în aceeaşi incintă mai au acces şi alte persoane care nu au legătură cu DCP prelucrate sau alte persoane străine;
- limitarea accesului persoanelor străine, neînsoţite în spaţiile unde se prelucrează/păstrează DCP;
- documentelor ce conţin DCP, care au depăşit termenul de arhivare/păstrare în conformitate cu prevederile legale şi/sau procedurilor interne, sunt distruse. La momentul distrugerii se va încheia un Proces Verbal in care vor fi menţionate numerele de dosare ce au fost distruse şi modalitatea de distrugere.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

MĂSURI TEHNICE ŞI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT ELECTRONIC

- Tehnica de calcul care stochează date cu caracter personal, va fi amplasata în spatii identificate ăi protejate, aflate în posesia operatorului, la care au acces doar persoanele împuternicite.
- Datele cu caracter personal vor putea fi înregistrate pe suport mobil (stick USB/memorie externă, disc optic) numai dacă respectivul suport a fost securizat, astfel încât datele pe care le conţine sa nu poată fi citite/recuperate/copiate/extrase de pe suport, decat dupa introducerea unui/unor coduri speciale de securitate şi doar cu acordul conducătorului operatorului.
- Operatorul de date cu caracter personal va întocmi o evidenta a tehnicii de calcul utilizata si a persoanelor autorizate sa o foloseasca, la care poate atasa fisele care atesta instruirea personalului angajat in acest scop. Acestea trebuie sa aiba incheiate raporturi de munca cu operatorul (contracte de munca, contracte de colaborare, contracte de prestari servicii)
- Mentenanţa, modernizările Şi orice intervenţie asupra sistemului informatic prin intermediul cărora se sunt accesate DCP sunt făcute doar de către persoane autorizate în acest sens de către operator.

DURATA DE PRELUCRARE/PĂSTRARE/DISTRUGERE

MEF 3512/2008 şi Anexa 6 a Legii Arhivelor Naţionale stabilesc următoarele termene de păstrare:

50 de ani – statele de plată
75 de ani – dosarele de personal
contractele de muncă
convenţiile civile de prestări servicii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Evidenţele activităţilor de prelucrare

Fiecare operator sau reprezentantul acestuia trebuie să păstreaze **evidenţa activităţilor de prelucrare** desfăşurate care cuprinde **cel puţin**:

- numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Evidenţele activităţilor de prelucrare

Fiecare operator sau persoana împuternicită de operator păstrează o **evidenţă a tuturor categoriilor de activităţi de prelucrare** desfăşurate **în numele operatorului,** care cuprind:

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

Evidenţele pot fi formulate în scris (inclusiv în format electronic).

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Evidenţele activităţilor de prelucrare

Aceste evidenţe **nu sunt obligatorii** în cazul întreprinderilor sau organizaţiilor cu **mai puţin de 250 de angajaţi**, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze **un risc pentru drepturile şi libertăţile persoanelor vizate**, prelucrarea **nu este ocazională** sau prelucrarea **include categorii speciale de date** sau date cu caracter personal referitoare la **condamnări penale şi infracţiuni**.

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

CARTOGRAFIEREA PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

CINE ?

Se înscriu în evidenţa numele şi coordonatele operatorului (şi ale reprezentantului sau legal) şi, dupa caz, ale responsabilului cu protecţia datelor;
Se întocmeşte 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 infracţiunile).

DE CE ?

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

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

CARTOGRAFIEREA PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

CUM?
Se precizează modalitatea/modalităţile tehnice în care sunt colectate şi/sau prelucrate datele cu caracter personal.
CÂT?
Se specifică durata de păstrare a datelor cu caracter personal.
UNDE?
Se menţionează formatul şi locul în care se pastrează datele cu caracter personal.

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI GENERALE	
PG – ALFABETA - 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL
PG – ALFABETA - 02	POLITICA PRIVIND RGPD
PG – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL IN ACTIVITATEA ORGANIZATIEI
PG – ALFABETA - 04	DATELE CU CARACTER PERSONAL CARE TREBUIE PROTEJATE
PG – ALFABETA - 05	MASURI TEHNICE SI ORGANIZATORICE
PG - ALFABETA - 06	PROCEDURA DE ACTIUNE IN SITUATIA UNUI INCIDENT DE SECURITATE
PG - ALFABETA - 07	PROCEDURA DE INTOCMIRE RASPUNS PERSOANA VIZATA

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI INTERNE	
PI – ALFABETA – 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIVIND ACTIVITATEA DE RESURSE UMANE RU
PI – ALFABETA – 02	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CURSURI/FORMARE PROFESIONALA A ADULTILOR
PI – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CONTRACTARI
PI – ALFABETA – 04	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) AFERENTA SERVICIILOR EXTERNALIZATE.
PI – ALFABETA – 05	PASTRAREA DATELOR CU CARACTER PERSONAL
PI – ALFABETA - 06	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) MONITORIZARE VIDEO

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Modul 5: Sfera activităţilor aferente asistenţei de specialitate acordate de responsabilul cu protecţia datelor cu caracter personal.

Elaborarea planului de lucru al responsabilului cu protecţia datelor cu caracter personal

Principiul responsabilităţii în domeniul protecţiei datelor cu caracter personal;

Evaluarea impactului asupra protecţiei datelor;

Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit (conceptul de *data protection by design and by default*);

Transferul de date cu caracter personal – regim juridic aplicabil, drepturi şi obligaţii în funcţie de natura destinatarului (inclusiv transferul către ţări terţe);

Conceptul de securitate al prelucrării datelor cu caracter personal. Încălcarea securităţii datelor cu caracter personal;

Răspunderea şi sancţiunile aplicabile în cazul nerespectării legislaţiei în domeniul protecţiei datelor cu caracter personal.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Securitatea prelucrării

Operatorul şi persoana împuternicită de acesta trebuie să implementeze **măsuri tehnice şi organizatorice** adecvate în vederea asigurării unui nivel de securitate care să includă cel puţin:

- pseudonimizarea şi criptarea datelor cu caracter personal;
- asigurarea confidenţialităţii, integrităţii, disponibilităţii şi rezistenţei continue ale sistemelor şi serviciilor de prelucrare;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

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

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Evaluarea impactului asupra protecţiei datelor - înainte de începerea prelucrării, prin analiza tuturor caracteristicilor: natura, domeniul de aplicare, contextul şi scopurile prelucrării, pentru a identifica posibilele riscuri pentru drepturile şi libertăţile persoanelor fizice.

Evaluarea efectuată va conţine minim:

- o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
- o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;
- o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate;
- măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal.

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Cooperarea cu autoritatea de supraveghere

Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal

În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, operatorul notifică acest lucru autorităţii de supraveghere competente în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoţită de o explicaţie motivată din partea operatorului.

Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal

În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal

Informarea persoanei vizate afectate nu este necesară în cazul în care oricare dintre următoarele condiţii este îndeplinită:

- operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
- operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor vizate afectate nu mai este susceptibil să se materializeze;
- ar necesita un efort disproporţionat. Acţiuni alternativr: se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

În cazul în care operatorul nu a comunicat deja încălcarea securităţii datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile de protecţie sunt îndeplinite.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL IV

OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Desemnarea responsabilului cu protecţia datelor

Operatorul şi persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

- prelucrarea este efectuată de o autoritate sau un organism public, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;
- activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară largă; sau
- activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale şi infracţiuni;
- prelucrează un număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, în scopul prevăzut la art. 6, alin. (1), lit. f) din Regulamentul general privind protecţia datelor, respectiv al realizării intereselor legitime urmărite de operator sau de o parte terţă. (pct. (2), art. 4, L190/2018).

Funcţia responsabilului cu protecţia datelor

Sarcinile responsabilului cu protecţia datelor

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

Evidenţele activităţilor de prelucrare

Aceste evidenţe **nu sunt obligatorii** în cazul întreprinderilor sau organizaţiilor cu **mai puţin de 250 de angajaţi**, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze **un risc pentru drepturile şi libertăţile persoanelor vizate**, prelucrarea **nu este ocazională** sau prelucrarea **include categorii speciale de date** sau date cu caracter personal referitoare la **condamnări penale şi infracţiuni**.

Modul 5: Sfera activităţilor aferente asistenţei de specialitate acordate de responsabilul cu protecţia datelor cu caracter personal. Elaborarea planului de lucru al responsabilului cu protecţia datelor cu caracter personal

- Principiul responsabilităţii în domeniul protecţiei datelor cu caracter personal;
- Evaluarea impactului asupra protecţiei datelor;
- Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit (conceptul de *data protection by design and by default*);
- Transferul de date cu caracter personal – regim juridic aplicabil, drepturi şi obligaţii în funcţie de natura destinatarului (inclusiv transferul către ţări terţe);
- Conceptul de securitate al prelucrării datelor cu caracter personal. Încălcarea securităţii datelor cu caracter personal;
- Răspunderea şi sancţiunile aplicabile în cazul nerespectării legislaţiei în domeniul protecţiei datelor cu caracter personal.

Securitatea prelucrării

Operatorul şi persoana împuternicită de acesta trebuie să implementeze **măsuri tehnice şi organizatorice** adecvate în vederea asigurării unui nivel de securitate care să includă cel puţin:

- pseudonimizarea şi criptarea datelor cu caracter personal;
- asigurarea confidenţialităţii, integrităţii, disponibilităţii şi rezistenţei continue ale sistemelor şi serviciilor de prelucrare;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

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

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

Evaluarea impactului asupra protecţiei datelor - înainte de începerea prelucrării, prin analiza tuturor caracteristicilor: natura, domeniul de aplicare, contextul şi scopurile prelucrării, pentru a identifica posibilele riscuri pentru drepturile şi libertăţile persoanelor fizice.

Evaluarea efectuată va conţine minim:

- o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
- o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;
- o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate;
- măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal.

Articolul 35 **Evaluarea impactului asupra protecţiei datelor**

(3) Evaluarea impactului asupra protecţiei datelor se impune mai ales în cazul:

(a) unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date sau a unor date cu caracter personal privind condamnări penale şi infracţiuni, menţionată la articolul 10;

sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Autoritatea de supraveghere întocmeşte şi publică o listă a tipurilor de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor, în conformitate cu alineatul (1). Autoritatea de supraveghere comunică aceste liste comitetului menţionat la articolul 68.

(5) Autoritatea de supraveghere poate, de asemenea, să stabilească şi să pună la dispoziţia publicului o listă a tipurilor de operaţiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecţiei datelor. Autoritatea de supraveghere comunică aceste liste comitetului.

DECIZIE nr. 174 din 18 octombrie 2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal

Evaluarea impactului asupra protecţiei datelor cu caracter personal de către operatori este obligatorie în special în următoarele cazuri:

a)prelucrarea datelor cu caracter personal în vederea realizării unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

b)prelucrarea pe scară largă a datelor cu caracter personal privind originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la sindicate, a datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor privind sănătatea, viaţa sexuală sau orientarea sexuală ale unei persoane fizice sau a datelor cu caracter personal referitoare la condamnări penale şi infracţiuni;

c)prelucrarea datelor cu caracter personal având ca scop monitorizarea sistematică pe scară largă a unei zone accesibile publicului, cum ar fi supravegherea video în centre comerciale, stadioane, pieţe, parcuri sau alte asemenea spaţii;

d)prelucrarea pe scară largă a datelor cu caracter personal ale persoanelor vulnerabile, în special ale minorilor şi ale angajaţilor, prin mijloace automate de monitorizare şi/sau înregistrare sistematică a comportamentului, inclusiv în vederea desfăşurării activităţilor de reclamă, marketing şi publicitate;

e)prelucrarea pe scară largă a datelor cu caracter personal prin utilizarea inovatoare sau implementarea unor tehnologii noi, în special în cazul în care operaţiunile respective limitează capacitatea persoanelor vizate de a-şi exercita drepturile, cum ar fi utilizarea tehnicilor de recunoaştere facială în vederea facilitării accesului în diferite spaţii;

f)prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicaţii "Internetul lucrurilor", cum ar fi smart TV, vehicule conectate, contoare inteligente, jucării inteligente, oraşe inteligente sau alte asemenea aplicaţii);

g)prelucrarea pe scară largă şi/sau sistematică a datelor de trafic şi/sau de localizare a persoanelor fizice (cum ar fi monitorizarea prin Wi-Fi, prelucrarea datelor de localizare geografică a pasagerilor în transportul public sau alte asemenea situaţii) atunci când prelucrarea nu este necesară pentru prestarea unui serviciu solicitat de persoana vizată.

(2) Prin excepţie de la alin. (1), evaluarea impactului asupra protecţiei datelor nu este obligatorie atunci când prelucrarea efectuată în temeiul art. 6 alin. (1) lit. (c) sau (e) din Regulamentul general privind protecţia datelor are un temei juridic în dreptul Uniunii sau în dreptul intern şi deja s-a efectuat o evaluare a impactului asupra protecţiei datelor ca parte a unei evaluări generale a impactului în contextul adoptării actelor normative respective.

Evaluarea de risc privind protecţia datelor cu caracter personal, are la bază metoda “MATRICE CONSECINţE/PROBABILITATE” (conform SR EN 31010), completată cu cuantificarea acestuia.

Aplicarea metodei permite ierarhizarea riscurilor în funcţie de valoarea lor, şi alocarea eficientă a resurselor aferente (necesare).

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie) Neintomirea sau intocmirea defectuoasa de documente Acces neautorizat la baza de date sau documente Furtul de documente de catre terte persoane Distrugerea de documente de catre terte persoane Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

A. SCALA DE COTATIE A GRAVITATII IMPACTULUI (CONSECINTELOR) SI A PROBABILITATII ACTIUNII FACTORILOR DE RISC (PRODUCERII DE EVENIMENTE), ASUPRA PROTECTIEI DATELOR CU CARACTER PERSONAL.

CLASE DE GRAVITATE	IMPACT (CONSECINTE)	GRAVITATEA IMPACTULUI (GRAVITATEA CONSECINTELOR)
1	NEGLIJABIL	impactul (consecintele) este neglijabil, existand totusi riscul producerii unui incidente de securitate
2	MIC	impactul (consecintele) este mici, aparitia unui incident de securitate este redus
3	MEDIU	impactul (consecintele) este mediu, aparitia unui incident de securitate este posibil
4	GRAV	impactul (consecintele) este grav ,aparitia unui incident de securitate este probabil
5	FOARTE GRAV	impactul (consecintele) este foarte grav, aparitia unui incident de securitate este iminent

CLASE DE PROBABILITATE	PRODUCEREA DE EVENIMENTE	PROBABILITATEA CONSECINTELOR
1	EXTRE DE RARE	probabilitatea de producere a consecintelor este extrem de rara; p > de 5 ani.
2	FOARTE RARE	probabilitatea de producere a consecintelor este foarte rara; 1 ani > p < 5 ani
3	RAR	probabilitatea de producere a consecintelor este rara; 6 luni > p > 1 an
4	RIDICATA	probabilitatea de producere a consecintelor este probabila; 15 zile > p > 6 luni
5	SIGURE	probabilitatea de producere a consecintelor este sigura (certa) p < 15 zile

B. GRILA PRIVIND CATEGORIILE DE RISC, PRIN COMBINAREA GRAVITATII CONSECINTELOR CU PROBABILITATEA DE PRODUCERE A ACESTUIA.

CLASA DE GRAVITATE / CLASA DE PROBABILITATE		1	2	3	4	5
		IMPACT (CONSECINTE)				
		NEGLIJABIL	MIC	MEDIU	GRAV	FOARTE GRAV
5	SIGUR	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)
4	PROBABIL	(4,1)	(4,2)	4,3)	(4,4)	(4,5)
3	RAR	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)
2	FOARTE RAR	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
1	EXTREM DE RARE	(1,1)	(1.2)	(1,3)	(1,4)	(1,5)

C. SCALA DE INCADRARE A: NIVEL DE RISC /NIVEL DE SECURITATE

NIVEL DE RISC	CUPLUL GRAVITATE - PROBABILITATE	NIVEL DE SECURITATE
1. MINIM	(1,1)(1,2)(1,3)(1,4) (1,5)(2,1)(2,2)(2,3)(3,1)(4,1)(5,1)	5. RIDICAT
2. MIC	(2,4)(2,5)(3,2) (3,3) (4,2)(5,2)	4. MARE
3. MEDIU	(3,4) (3,5) (4,3)(5,3)	3. MEDIU
4. MARE	(4,4) (4,5) (5,4)	2. MIC
5. FOARTE MARE	(5,5)	1. MINIM

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

Evidenţele activităţilor de prelucrare

Fiecare operator sau reprezentantul acestuia trebuie să păstreze **evidenţa activităţilor de prelucrare** desfăşurate care cuprinde **cel puţin**:

- numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

MĂSURI TEHNICE şI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT DE HARTIE

- Spaţiile de stocare (încăperile unde sunt amplasate seifurile de păstrare /stocare) sunt identificate şi protejate, şi se aflate în posesia operatorului;
- documentele ce conţin date cu caracter personal (DCP), sunt păstrate în fişete speciale, dotate cu încuietori pentru a asigura securitatea acestora;
- imprimarea datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru aceasta operaţiune de către operator şi pentru scopul pentru care aceste date au fost furnizate;
- reziduurile în format de hârtie care conţin date şi documente vor fi distruse într-un mod securizat cu dispozitive de tocat hârtii;
- la părăsirea locului de muncă, utilizatorii trebuie sa închidă în fişete documentele ce conţin DCP, dacă în aceeaşi incintă mai au acces şi alte persoane care nu au legătură cu DCP prelucrate sau alte persoane străine;
- limitarea accesului persoanelor străine, neînsoţite în spaţiile unde se prelucrează/păstrează DCP;
- documentelor ce conţin DCP, care au depăşit termenul de arhivare/păstrare în conformitate cu prevederile legale şi/sau procedurilor interne, sunt distruse. La momentul distrugerii se va încheia un Proces Verbal in care vor fi menţionate numerele de dosare ce au fost distruse şi modalitatea de distrugere.

MĂSURI TEHNICE şI ORGANIZATORICE IMPLEMENTATE/NECESARE

PRELUCRAREA DCP PE SUPORT ELECTRONIC

- Tehnica de calcul care stochează date cu caracter personal, va fi amplasata în spatii identificate ăi protejate, aflate în posesia operatorului, la care au acces doar persoanele împuternicite.
- Datele cu caracter personal vor putea fi înregistrate pe suport mobil (stick USB/memorie externă, disc optic) numai dacă respectivul suport a fost securizat, astfel încât datele pe care le conţine sa nu poată fi citite/recuperate/copiate/extrase de pe suport, decat dupa introducerea unui/unor coduri speciale de securitate şi doar cu acordul conducătorului operatorului.
- Operatorul de date cu caracter personal va întocmi o evidenta a tehnicii de calcul utilizata si a persoanelor autorizate sa o foloseasca, la care poate atasa fisele care atesta instruirea personalului angajat in acest scop. Acestea trebuie sa aiba incheiate raporturi de munca cu operatorul (contracte de munca, contracte de colaborare, contracte de prestari servicii)
- Mentenanţa, modernizările şi orice intervenţie asupra sistemului informatic prin intermediul cărora se sunt accesate DCP sunt făcute doar de către persoane autorizate în acest sens de către operator.

DURATA DE PRELUCRARE/PĂSTRARE/DISTRUGERE

MEF 3512/2008 şi Anexa 6 a Legii Arhivelor Naţionale stabilesc următoarele termene de păstrare:

50 de ani – statele de plată

75 de ani – dosarele de personal

contractele de muncă

convenţiile civile de prestări servicii

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI GENERALE	
PG – ALFABETA - 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL
PG – ALFABETA - 02	POLITICA PRIVIND RGPD
PG – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL IN ACTIVITATEA ORGANIZATIEI
PG – ALFABETA - 04	DATELE CU CARACTER PERSONAL CARE TREBUIE PROTEJATE
PG – ALFABETA - 05	MASURI TEHNICE SI ORGANIZATORICE
PG - ALFABETA - 06	PROCEDURA DE ACTIUNE IN SITUATIA UNUI INCIDENT DE SECURITATE
PG - ALFABETA - 07	PROCEDURA DE INTOCMIRE RASPUNS PERSOANA VIZATA

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI INTERNE	
PI – ALFABETA – 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIVIND ACTIVITATEA DE RESURSE UMANE RU
PI – ALFABETA – 02	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CURSURI/FORMARE PROFESIONALA A ADULTILOR
PI – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CONTRACTARI
PI – ALFABETA – 04	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) AFERENTA SERVICIILOR EXTERNALIZATE.
PI – ALFABETA – 05	PASTRAREA DATELOR CU CARACTER PERSONAL
PI – ALFABETA - 06	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) MONITORIZARE VIDEO

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

Modul 5: Sfera activităţilor aferente asistenţei de specialitate acordate de responsabilul cu protecţia datelor cu caracter personal. Elaborarea planului de lucru al responsabilului cu protecţia datelor cu caracter personal

- Principiul responsabilităţii în domeniul protecţiei datelor cu caracter personal;
- Evaluarea impactului asupra protecţiei datelor;
- Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit (conceptul de *data protection by design and by default*);
- Transferul de date cu caracter personal – regim juridic aplicabil, drepturi şi obligaţii în funcţie de natura destinatarului (inclusiv transferul către ţări terţe);
- Conceptul de securitate al prelucrării datelor cu caracter personal. Încălcarea securităţii datelor cu caracter personal;
- Răspunderea şi sancţiunile aplicabile în cazul nerespectării legislaţiei în domeniul protecţiei datelor cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

Securitatea prelucrării

Operatorul şi persoana împuternicită de acesta trebuie să implementeze **măsuri tehnice şi organizatorice** adecvate în vederea asigurării unui nivel de securitate care să includă cel puţin:

- pseudonimizarea şi criptarea datelor cu caracter personal;
- asigurarea confidenţialităţii, integrităţii, disponibilităţii şi rezistenţei continue ale sistemelor şi serviciilor de prelucrare;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

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

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie)
	Neintomirea sau intocmirea defectuoasa de documente
	Acces neautorizat la baza de date sau documente
	Furtul de documente de catre terte persoane
	Distrugerea de documente de catre terte persoane
	Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

Evaluarea impactului asupra protecţiei datelor - înainte de începerea prelucrării, prin analiza tuturor caracteristicilor: natura, domeniul de aplicare, contextul şi scopurile prelucrării, pentru a identifica posibilele riscuri pentru drepturile şi libertăţile persoanelor fizice.

Evaluarea efectuată va conţine minim:

- o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
- o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;
- o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate;
- măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Evidenţele activităţilor de prelucrare

Fiecare operator sau reprezentantul acestuia trebuie să păstreaze **evidenţa activităţilor de prelucrare** desfăşurate care cuprinde **cel puţin**:

- numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI GENERALE	
PG – ALFABETA - 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL
PG – ALFABETA - 02	POLITICA PRIVIND RGPD
PG – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL IN ACTIVITATEA ORGANIZATIEI
PG – ALFABETA - 04	DATELE CU CARACTER PERSONAL CARE TREBUIE PROTEJATE
PG – ALFABETA - 05	MASURI TEHNICE SI ORGANIZATORICE
PG - ALFABETA - 06	PROCEDURA DE ACTIUNE IN SITUATIA UNUI INCIDENT DE SECURITATE
PG - ALFABETA - 07	PROCEDURA DE INTOCMIRE RASPUNS PERSOANA VIZATA

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI INTERNE	
PI – ALFABETA – 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIVIND ACTIVITATEA DE RESURSE UMANE RU
PI – ALFABETA – 02	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CURSURI/FORMARE PROFESIONALA A ADULTILOR
PI – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CONTRACTARI
PI – ALFABETA – 04	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) AFERENTA SERVICIILOR EXTERNALIZATE.
PI – ALFABETA – 05	PASTRAREA DATELOR CU CARACTER PERSONAL
PI – ALFABETA - 06	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) MONITORIZARE VIDEO

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecţie

Transferul de date cu caracter personal către o ţară terţă sau o organizaţie internaţională se poate realiza atunci când Comisia a decis că ţara terţă, un teritoriu ori unul sau mai multe sectoare specificate din acea ţară terţă sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. Transferurile realizate în aceste condiţii nu necesită autorizări speciale.

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Evaluarea caracterul adecvat al nivelului de protecţie:

- respectarea drepturilor omului şi a libertăţilor fundamentale
- existenţa şi funcţionarea eficientă a uneia sau mai multor autorităţi de supraveghere independente
- angajamentele internaţionale la care a aderat ţara terţă sau organizaţia internaţională

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Evaluarea caracterul adecvat al nivelului de protecţie:

- respectarea drepturilor omului şi a libertăţilor fundamentale;
- accesul autorităţilor publice la datele cu caracter personal;
- normele de protecţie a datelor, normele profesionale şi măsuri de securitate, inclusiv norme privind transferul ulterior de date cu caracter personal către o altă ţară terţă sau organizaţie internaţională;
- existenţa şi funcţionarea eficientă a uneia sau mai multor autorităţi de supraveghere independente;
- angajamentele internaţionale la care a aderat ţara terţă sau organizaţia internaţională.

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Transferuri în baza unor garanţii adecvate

În absenţa unei decizii a Comitetului european operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională numai dacă operatorul sau persoana împuternicită de operator a oferit garanţii adecvate şi cu condiţia să existe drepturi opozabile şi căi de atac eficiente pentru persoanele vizate.

Garanţiile adecvate pot fi furnizate prin:

- un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice;
- reguli corporatiste obligatorii;
- clauze standard de protecţie a datelor adoptate de Comisie în conformitate cu procedura de examinare menţionată la articolul 93 alineatul (2);
- clauze standard de protecţie a datelor adoptate de o autoritate de supraveghere şi aprobate de Comisie;
- un cod de conduită însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau
- un mecanism de certificare însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din ţara terţă de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Transferuri în baza unor garanţii adecvate

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

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

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Reguli corporatiste obligatorii

În conformitate cu mecanismul pentru asigurarea coerenţei, autoritatea de supraveghere competentă aprobă reguli corporatiste obligatorii, cu condiţia ca acestea:

(a) să fie obligatorii din punct de vedere juridic şi să se aplice fiecărui membru vizat al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, inclusiv angajaţilor acestuia, precum şi să fie puse în aplicare de membrii în cauză;

(b) să confere, în mod expres, drepturi opozabile persoanelor vizate în ceea ce privește prelucrarea datelor lor cu caracter personal;

şi

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

(c) să îndeplinească cerinţele de mai jos:

Regulile corporatiste obligatorii :

- structura şi datele de contact ale grupului de întreprinderi sau ale grupului de întreprinderi implicate într-o activitate economică comună şi ale fiecăruia dintre membrii săi;
- transferurile de date sau setul de transferuri, inclusiv categoriile de date cu caracter personal, tipul prelucrării şi scopurile prelucrării, tipurile de persoane vizate afectate şi identificarea ţării terţe sau a ţărilor terţe în cauză;
- caracterul lor juridic obligatoriu, atât pe plan intern, cât şi extern;
- aplicarea principiilor generale în materie de protecţie a datelor, în special limitarea scopului, reducerea la minimum a datelor, perioadele de stocare limitate, calitatea datelor, protecţia datelor începând cu momentul conceperii şi protecţia implicită, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date cu caracter personal, măsurile de asigurare a securităţii datelor, precum şi cerinţele referitoare la transferurile ulterioare către organisme care nu fac obiectul regulilor corporatiste obligatorii;

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Regulile corporatiste obligatorii :

- drepturile persoanelor vizate în ceea ce privește prelucrarea și mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, dreptul de a depune o plângere în fața autorității de supraveghere competente și în fața instanțelor competente ale statelor membre, în conformitate cu articolul 79, precum și dreptul de a obține reparații și, după caz, despăgubiri pentru încălcarea regulilor corporatiste obligatorii;
- acceptarea de către operator sau de persoana împuternicită de operator, care își are sediul pe teritoriul unui stat membru, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru în cauză care nu își are sediul în Uniune; operatorul sau persoana împuternicită de operator este exonerat(ă) de această răspundere, integral sau parțial, numai dacă dovedește că membrul respectiv nu a fost răspunzător de evenimentul care a cauzat prejudiciul;
- modul în care informațiile privind regulile corporatiste obligatorii, sunt furnizate persoanelor vizate;

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Regulile corporatiste obligatorii :

- sarcinile oricărui responsabil cu protecţia datelor sau ale oricărei alte persoane sau entităţi însărcinate cu monitorizarea respectării regulilor corporatiste obligatorii în cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, a activităţilor de formare şi a gestionării plângerilor;
- procedurile de formulare a plângerilor;
- mecanismele din cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, menite să asigure verificarea conformităţii cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protecţia datelor şi metodele de asigurare a acţiunilor corective menite să protejeze drepturile persoanei vizate. Rezultatele acestor verificări ar trebui să fie puse la dispoziţia autorităţii de supraveghere competente, la cerere;
- mecanismele de raportare şi înregistrare a modificărilor aduse regulilor şi de raportare a acestor modificări autorităţii de supraveghere;

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Regulile corporatiste obligatorii :

- mecanismul de cooperare cu autoritatea de supraveghere în vederea asigurării respectării regulilor de către orice membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, în special prin punerea la dispoziţia autorităţii de supraveghere a rezultatelor verificărilor cu privire la măsurile menţionate la punctul (j);
- mecanismele de raportare către autoritatea de supraveghere competentă a oricăror cerinţe legale impuse unui membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună într-o ţară terţă care pot avea un efect advers considerabil asupra garanţiilor furnizate prin regulile corporatiste obligatorii; şi
- formarea corespunzătoare în domeniul protecţiei datelor a personalului care are un acces permanent sau periodic la date cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Transferurile sau divulgările de informaţii neautorizate de dreptul Uniunii

Orice hotărâre a unei instanţe sau a unui tribunal şi orice decizie a unei autorităţi administrative a unei ţări terţe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internaţional, cum ar fi un tratat de asistenţă judiciară reciprocă în vigoare între ţara terţă solicitantă şi Uniune sau un stat membru, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol.

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Derogări pentru situaţii specifice

În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie sau a unor garanţii adecvate, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o ţară terţă sau o organizaţie internaţională poate avea loc numai în una dintre condiţiile următoare:

- persoana vizată şi-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecţie şi a unor garanţii adecvate;
- transferul este necesar pentru executarea unui contract între persoana vizată şi operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
- transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator şi o altă persoană fizică sau juridică;
- transferul este necesar din considerente importante de interes public;
- transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanţă;
- transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-şi exprima acordul;
- transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informaţii publicului şi care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condiţiile cu privire la consultare prevăzute de dreptul Uniunii sau de dreptul intern în acel caz specific.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL V TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRI TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

În cazul în care un transfer nu ar putea să se întemeieze pe o dispoziţie **unei decizii privind caracterul adecvat al nivelului de protecţie sau în baza unor garanţii adecvate**, inclusiv dispoziţii privind reguli corporatiste obligatorii, şi nu este aplicabilă niciuna dintre derogările pentru situaţii specifice prevăzute pentru **situaţii specifice**, un transfer către o ţară terţă sau o organizaţie internaţională poate avea loc numai în cazul în care transferul nu este repetitiv, se referă doar la un număr limitat de persoane vizate, este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile şi libertăţile persoanei vizate şi operatorul a evaluat toate circumstanţele aferente transferului de date şi, pe baza acestei evaluări, a prezentat garanţii corespunzătoare în ceea ce priveşte protecţia datelor cu caracter personal. Operatorul informează autoritatea de supraveghere cu privire la transfer.

Operatorul, în plus informează persoana vizată cu privire la transfer şi la interesele legitime majore pe care le urmăreşte.

Cooperarea cu autoritatea de supraveghere

Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

În cazul în care are loc o încălcare a securităţii datelor cu caracter personal, operatorul notifică acest lucru autorităţii de supraveghere competente în termen de cel mult 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoţită de o explicaţie motivată din partea operatorului.

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

În cazul în care încălcarea securităţii datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

STRUCTURA RGPD - CAPITOLUL IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal

Informarea persoanei vizate afectate nu este necesară în cazul în care oricare dintre următoarele condiţii este îndeplinită:

- operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
- operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor vizate afectate nu mai este susceptibil să se materializeze;
- ar necesita un efort disproporţionat. Acţiuni alternativr: se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

În cazul în care operatorul nu a comunicat deja încălcarea securităţii datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile de protecţie sunt îndeplinite.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie)
	Neintomirea sau intocmirea defectuoasa de documente
	Acces neautorizat la baza de date sau documente
	Furtul de documente de catre terte persoane
	Distrugerea de documente de catre terte persoane
	Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

Evaluarea impactului asupra protecţiei datelor - înainte de începerea prelucrării, prin analiza tuturor caracteristicilor: natura, domeniul de aplicare, contextul şi scopurile prelucrării, pentru a identifica posibilele riscuri pentru drepturile şi libertăţile persoanelor fizice.

Evaluarea efectuată va conţine minim:

- o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
- o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;
- o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate;
- măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Evidenţele activităţilor de prelucrare

Fiecare operator sau reprezentantul acestuia trebuie să păstreaze **evidenţa activităţilor de prelucrare** desfăşurate care cuprinde **cel puţin**:

- numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI GENERALE	
PG – ALFABETA - 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL
PG – ALFABETA - 02	POLITICA PRIVIND RGPD
PG – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL IN ACTIVITATEA ORGANIZATIEI
PG – ALFABETA - 04	DATELE CU CARACTER PERSONAL CARE TREBUIE PROTEJATE
PG – ALFABETA - 05	MASURI TEHNICE SI ORGANIZATORICE
PG - ALFABETA - 06	PROCEDURA DE ACTIUNE IN SITUATIA UNUI INCIDENT DE SECURITATE
PG - ALFABETA - 07	PROCEDURA DE INTOCMIRE RASPUNS PERSOANA VIZATA

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI INTERNE	
PI – ALFABETA – 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIVIND ACTIVITATEA DE RESURSE UMANE RU
PI – ALFABETA – 02	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CURSURI/FORMARE PROFESIONALA A ADULTILOR
PI – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CONTRACTARI
PI – ALFABETA – 04	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) AFERENTA SERVICIILOR EXTERNALIZATE.
PI – ALFABETA – 05	PASTRAREA DATELOR CU CARACTER PERSONAL
PI – ALFABETA - 06	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) MONITORIZARE VIDEO

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

Modul 6: Relaţia cu autoritatea de supraveghere în domeniul protecţiei datelor cu caracter personal. Instrumente şi situaţii specifice

Consultarea şi/sau aprobarea autorităţii de supraveghere cu privire la efectuarea anumitor operaţiuni de prelucrare în cazurile prevăzute de legislaţia aplicabilă;

Competenţele autorităţii de supraveghere. Conceptul de autoritate de supraveghere principală conform GDPR;

Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal. Modalitate de lucru şi instrumente.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL VI AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL VI AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

Secțiunea 1 Statutul independent

Fiecare stat membru se asigură că una sau mai multe autorităţi publice independente sunt responsabile de monitorizarea aplicării prezentului regulament, în vederea protejării drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea şi în vederea facilitării liberei circulaţii a datelor cu caracter personal în cadrul Uniunii („autoritatea de supraveghere”)

Secțiunea 2 Abilitări, sarcini și competențe

Competența

Fiecare autoritate de supraveghere are competența să îndeplinească sarcinile şi să exercite competenţele care îi sunt conferite în conformitate cu prezentul regulament pe teritoriul statului membru de care aparţine.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL VI AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

Sarcini

(a) monitorizează şi asigură aplicarea prezentului regulament;

(b) promovează acţiuni de sensibilizare şi de înţelegere în rândul publicului a riscurilor, normelor, garanţiilor şi drepturilor în materie de prelucrare. Se acordă atenţie specială activităţilor care se adresează în mod specific copiilor;

(c) oferă consiliere, în conformitate cu dreptul intern, parlamentului naţional, guvernului şi altor instituţii şi organisme cu privire la măsurile legislative şi administrative referitoare la protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea;

(d) promovează acţiuni de sensibilizare a operatorilor şi a persoanelor împuternicite de aceştia cu privire la obligaţiile care le revin în temeiul prezentului regulament;

(e) la cerere, furnizează informaţii oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu prezentul regulament şi, dacă este cazul, cooperează cu autorităţile de supraveghere din alte state membre în acest scop;

(f) tratează plângerile depuse de o persoană vizată, un organism, o organizaţie sau o asociaţie şi investighează într-o măsură adecvată obiectul plângerii şi informează reclamantul cu privire la evoluţia şi rezultatul investigaţiei, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigaţii mai amănunţite sau coordonarea cu o altă autoritate de supraveghere;

(g) cooperează, inclusiv prin schimb de informaţii, cu alte autorităţi de supraveghere şi îşi oferă asistenţă reciprocă pentru a asigura coerenţa aplicării şi respectării prezentului regulament;

(h) desfăşoară investigaţii privind aplicarea prezentului regulament, inclusiv pe baza unor informaţii primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;

(i) monitorizează evoluţiile relevante, în măsura în care acestea au impact asupra protecţiei datelor cu caracter personal, în special evoluţia tehnologiilor informaţiei şi comunicaţiilor şi a practicilor comerciale;

STRUCTURA RGPD - CAPITOLUL VI AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

Sarcini

(j) adoptă clauze contractuale standard;

(k) întocmeşte şi menţine la zi o listă în legătură cu cerinţa privind evaluarea impactului asupra protecţiei datelor;

(l) oferă consiliere cu privire la operaţiunile de prelucrare

(m) încurajează elaborarea de coduri de conduită, îşi dă avizul cu privire la acestea şi le aprobă pe cele care oferă suficiente garanţii;

(n) încurajează stabilirea unor mecanisme de certificare, precum şi a unor sigilii şi mărci în domeniul protecţiei datelor;

(o) acolo unde este cazul, efectuează o revizuire periodică a certificărilor acordate;

(p) elaborează şi publică criteriile de acreditare a unui organism de monitorizare a codurilor de conduită şi a unui organism de certificare ;

(q) coordonează procedura de acreditare a unui organism de monitorizare a codurilor de conduită;

(r) autorizează clauzele şi dispoziţiile contractuale;

(s) aprobă regulile corporatiste obligatorii;

(t) contribuie la activităţile comitetului;

(u) menţine la zi evidenţe interne privind încălcările prezentului regulament şi măsurile luate, în special avertismentele emise şi sancţiunile impuse;

(v) îndeplineşte orice alte sarcini legate de protecţia datelor cu caracter personal.

STRUCTURA RGPD - CAPITOLUL VI AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

Sarcini

Fiecare autoritate de supraveghere facilitează depunerea plângerilor menţionate prin măsuri precum punerea la dispoziţie a unui formular de depunere a plângerii care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

Îndeplinirea sarcinilor fiecărei autorităţi de supraveghere este gratuită pentru persoana vizată şi, după caz, pentru responsabilul cu protecţia datelor.

În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate percepe o taxă rezonabilă, bazată pe costurile administrative, sau poate refuza să le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autorităţii de supraveghere.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL VII COOPERARE ŞI COERENȚĂ

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL VII COOPERARE ŞI COERENŢĂ

Secţiunea 1 Cooperare

Cooperarea dintre autoritatea de supraveghere principală şi celelalte autorităţi de supraveghere vizate

Autoritatea de supraveghere principală cooperează cu celelalte autorităţi de supraveghere vizate în încercarea de a ajunge la un consens. Autoritatea de supraveghere principală şi autorităţile de supraveghere vizate îşi comunică reciproc toate informaţiile relevante.

Secţiunea 2 Asigurarea coerenţei

Pentru a contribui la aplicarea coerentă a RGPD în întreaga Uniune, autorităţile de supraveghere cooperează între ele şi, după caz, cu Comisia prin mecanismul pentru asigurarea coerenţei.

Secţiunea 3 Comitetul european pentru protecţia datelor

Comitetul european pentru protecţia datelor („comitetul”) este instituit ca organ al Uniunii şi are personalitate juridică.

Comitetul este alcătuit din şeful unei autorităţi de supraveghere din fiecare stat membru şi din Autoritatea Europeană pentru Protecţia Datelor sau reprezentanţii respectivi ai acestora.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL IX DISPOZIȚII REFERITOARE LA SITUAȚII SPECIFICE DE PRELUCRARE

Prelucrarea şi libertatea de exprimare şi de informare

Prin intermediul dreptului intern, statele membre asigură un echilibru între dreptul la protecţia datelor cu caracter personal în temeiul prezentului regulament şi dreptul la libertatea de exprimare şi de informare, inclusiv prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare.

Prelucrarea şi accesul public la documente oficiale

Datele cu caracter personal din documentele oficiale deţinute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei sarcini care serveşte interesului public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu dreptul Uniunii sau cu dreptul intern sub incidenţa căruia intră autoritatea sau organismul, pentru a stabili un echilibru între accesul public la documente oficiale şi dreptul la protecţia datelor cu caracter personal în temeiul RGPD.

STRUCTURA RGPD - CAPITOLUL IX DISPOZIȚII REFERITOARE LA SITUAȚII SPECIFICE DE PRELUCRARE

Prelucrarea unui număr de identificare național

Statele membre pot detalia în continuare condițiile specifice de prelucrare a unui număr de identificare național sau a oricărui alt identificator cu aplicabilitate generală. În acest caz, numărul de identificare național sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate în temeiul prezentului regulament.

Prelucrarea în contextul ocupării unui loc de muncă

Prin lege sau prin acorduri colective, statele membre pot prevedea norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, al protejării proprietății angajatorului sau a clientului, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă.

Garanţii şi derogări privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice

Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice are loc cu condiţia existenţei unor garanţii corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile şi libertăţile persoanelor vizate. Respectivele garanţii asigură faptul că au fost instituite măsuri tehnice şi organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivele măsuri pot include pseudonimizarea, cu condiţia ca respectivele scopuri să fie îndeplinite în acest mod. Atunci când respectivele scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.

Normele existente în domeniul protecţiei datelor pentru biserici şi asociaţii religioase

În cazul în care, într-un stat membru, bisericile şi asociaţiile sau comunităţile religioase aplică, la data intrării în vigoare a RGPD, un set cuprinzător de norme de protecţie a persoanelor fizice cu privire la prelucrare, aceste norme pot continua să se aplice, cu condiţia să fie aliniate la RGPD.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL X ACTE DELEGATE ŞI ACTE DE PUNERE ÎN APLICARE

STRUCTURA RGPD - CAPITOLUL X ACTE DELEGATE ŞI ACTE DE PUNERE ÎN APLICARE

Exercitarea delegării

Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute de prezentul articol.

Procedura comitetului

Comisia este asistată de un comitet. Comitetul respectiv este un comitet în înțelesul Regulamentului (UE) nr. 182/2011.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL XI DISPOZIȚII FINALE

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL XI DISPOZIŢII FINALE

- **Abrogarea Directivei 95/46/C**
- **Relaţia cu Directiva 2002/58/CE**
- **Relaţia cu acordurile încheiate anterior**
- **Rapoartele Comisiei**
- **Revizuirea altor acte juridice ale Uniunii în materie de protecţie a datelor**
- **Intrare în vigoare şi aplicare**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPLETĂRI INTRODUSE DE

LEGEA 190 din 18 iulie 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)

DEFINIŢII

- autorităţi şi organisme publice - Camera Deputaţilor şi Senatul, Administraţia Prezidenţială, Guvernul, ministerele, celelalte organe de specialitate ale administraţiei publice centrale, autorităţile şi instituţiile publice autonome, autorităţile administraţiei publice locale şi deja nivel judeţean, alte autorităţi publice, precum şi instituţiile din subordinea/coordonarea acestora. În sensul prezentei legi, sunt asimilate autorităţilor/organismelor publice şi unităţile de cult şi asociaţiile şi fundaţiile de utilitate publică;

- număr de identificare naţional - numărul prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care are aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul paşaportului, al permisului de conducere, numărul de asigurare socială de sănătate;

- plan de remediere - anexă la procesul-verbal de constatare şi sancţionare a contravenţiei, întocmit în condiţiile prevăzute la art. 11, prin care Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea naţională de supraveghere, stabileşte măsuri şi un termen de remediere;

DEFINIȚII

- măsură de remediere - soluţie dispusă de Autoritatea naţională de supraveghere în planul de remediere în vederea îndeplinirii de către autoritatea/organismul public a obligaţiilor prevăzute de lege;

- termen de remediere - perioada de timp de cel mult 90 de zile de la data comunicării procesului-verbal de constatare şi sancţionare a contravenţiei, în care autoritatea/organismul public are posibilitatea remedierii neregulilor constatate şi îndeplinirii obligaţiilor legale;

- îndeplinirea unei sarcini care serveşte unui interes public - include acele activităţi ale partidelor politice sau ale organizaţiilor cetăţenilor aparţinând minorităţilor naţionale, ale organizaţiilor neguvernamentale, care servesc realizării obiectivelor prevăzute de dreptul constituţional sau de dreptul internaţional public ori funcţionării sistemului democratic, incluzând încurajarea participării cetăţenilor în procesul de luare a deciziilor şi a pregătirii politicilor publice, respectiv promovarea principiilor şi valorilor democraţiei.

PRELUCRAREA DATELOR GENETICE, A DATELOR BIOMETRICE SAU A DATELOR PRIVIND SĂNĂTATEA

Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri, este permisă cu consimţământul explicit al persoanei vizate sau dacă prelucrarea este efectuată în temeiul unor dispoziţii legale exprese, cu instituirea unor măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate.

PRELUCRAREA UNUI NUMĂR DE IDENTIFICARE NAŢIONAL

Prelucrarea unui număr de identificare naţional (art. 4, L190/2018)

(1) Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, se poate efectua în situaţiile prevăzute de art. 6 alin. (1) din Regulamentul general privind protecţia datelor.

Articolul 6/GDPR **Legalitatea prelucrării**

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

(a) persoana vizată şi-a dat consimţământul 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 obligaţii 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 serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul;

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorităţi publice în îndeplinirea atribuţiilor lor.

PRELUCRAREA UNUI NUMĂR DE IDENTIFICARE NAŢIONAL

Prelucrarea, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, **în scopul realizării intereselor legitime urmărite de operator sau de o parte** terţă se efectuează cu instituirea de către operator a următoarelor garanţii:

- punerea în aplicare de măsuri tehnice şi organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum şi pentru asigurarea securităţii şi confidenţialităţii prelucrărilor de date cu caracter personal, conform dispoziţiilor art. 32 din Regulamentul general privind protecţia datelor;

- numirea unui responsabil pentru protecţia datelor, în conformitate cu prevederile art. 10 din prezenta lege;

- stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii;

- instruirea periodică cu privire la obligaţiile ce le revin a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN CONTEXTUL RELAŢIILOR DE MUNCĂ

În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

- interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate; angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;
- angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;
- alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa;

şi

- durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

PRELUCRAREA DATELOR CU CARACTER PERSONAL ŞI DE CATEGORII SPECIALE DE DATE CU CARACTER PERSONAL, ÎN CONTEXTUL ÎNDEPLINIRII UNEI SARCINI CARE SERVEŞTE UNUI INTERES PUBLIC

În cazul în care prelucrarea datelor personale şi speciale este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public se efectuează cu instituirea de către operator sau de către partea terţă a următoarelor garanţii:

- punerea în aplicare a măsurilor tehnice şi organizatorice adecvate pentru respectarea principiilor legalităţii prelucrării datelor cu caracter personal, în special a reducerii la minimum a datelor, respectiv a principiului integrităţii şi confidenţialităţii;
- numirea unui responsabil pentru protecţia datelor, dacă aceasta este necesară;
- stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.

PRELUCRAREA DATELOR CU CARACTER PERSONAL ŞI DE CATEGORII SPECIALE DE DATE CU CARACTER PERSONAL DE CĂTRE PARTIDELE POLITICE ŞI ORGANIZAŢIILE CETĂŢENILOR APARŢINÂND MINORITĂŢILOR NAŢIONALE, ORGANIZAŢIILOR NEGUVERNAMENTALE

Garanţii:

- informarea persoanei vizate despre prelucrarea datelor cu caracter personal;
- garantarea transparenţei informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor persoanei vizate;
- garantarea dreptului de rectificare şi ştergere.

OBS: Prelucrarea se poate efectua fără consimţământul expres al persoanei vizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD

CAPITOLUL VIII CĂI DE ATAC, RĂSPUNDERE ŞI SANCŢIUNI

STRUCTURA RGPD - CAPITOLUL VIII CĂI DE ATAC, RĂSPUNDERE ŞI SANCȚIUNI

SANCȚIUNI

În funcţie de circumstanţele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor preventive, ţinând cont de următoarele aspecte:

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

dacă încălcarea a fost comisă intenţionat sau din neglijenţă;

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

gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia;

eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;

gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea şi a atenua posibilele efecte negative ale încălcării;

categoriile de date cu caracter personal afectate de încălcare;

modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, în special dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

în cazul în care măsurile preventive au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la acelaşi obiect, respectarea respectivelor măsuri;

aderarea la coduri de conduită aprobate sau la mecanisme de certificare aprobate;

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

STRUCTURA RGPD - CAPITOLUL VIII CĂI DE ATAC, RĂSPUNDERE ŞI SANCȚIUNI

SANCȚIUNI

Pentru încălcarea:

- obligaţiilor operatorului şi ale persoanei împuternicite de operator;
- obligaţiilor organismului de certificare;
- obligaţiilor organismului de monitorizare;

se aplică **amenzi administrative de până la 10 000 000 EUR** sau, în cazul unei întreprinderi, de până la **2 % din cifra de afaceri mondială totală anuală** corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

Pentru încălcărea:

- principiilor de bază pentru prelucrare, inclusiv condiţiile privind consimţământul;
- drepturilor persoanelor vizate;
- modului de efectuare a transferurilor de date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională;
- orice obligaţii în temeiul legislaţiei naţionale adoptate în temeiul capitolului IX;
- nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării f luxurilor de date, emisă de către autoritatea de supraveghere sau neacordarea accesului

se aplică amenzi **administrative de până la 20 000 000 EUR** sau, în cazul unei întreprinderi, de până la **4 % din cifra de afaceri mondială totală anuală** corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

Pentru încălcarea unui ordin emis de autoritatea de supraveghere se aplică **amenzi administrative de până la 20 000 000 EUR** sau, în cazul unei întreprinderi, de până la **4 % din cifra de afaceri mondială totală anuală** corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

STRUCTURA RGPD - CAPITOLUL VIII CĂI DE ATAC, RĂSPUNDERE ŞI SANCŢIUNI

SANCŢIUNI

În concepţia RGPD, sancţiunile civile (răspunderea civilă) pot coexista cu cele administrative. Sancţiunile administrative (amenzi) vor fi aplicate de către autoritatea naţională şi vor fi uriaşe, comparativ cu sancţiunile care pot fi aplicate astăzi de către Autoritate:

- ✓ Mustrare.
- ✓ Măsuri corective (ex. limitare temporară sau definitivă, suspendare, restricţionarea prelucrării).
- ✓ Acţiune judecătorească (despăgubiri).
- ✓ Amendă de până la 10 sau 20 mil. Euro.
- ✓ Amendă de până la 4% din cifra de afaceri mondială totală anuală.

MĂSURI CORECTIVE ŞI SANCŢIUNI

Sancţiunile contravenţionale principale sunt avertismentul şi amenda contravenţională.

Constatarea contravenţiilor prevăzute de prezenta lege şi aplicarea sancţiunilor contravenţionale, precum şi a celorlalte măsuri corective se fac de Autoritatea naţională de supraveghere.

MĂSURI CORECTIVE ŞI SANCŢIUNI

Aplicarea măsurilor corective autorităţilor şi organismelor publice

- La constatarea unei încălcări a RGPD Autoritatea naţională de supraveghere încheie un proces-verbal de constatare şi sancţionare a contravenţiei prin care se aplică sancţiunea avertismentului şi la care anexează un plan de remediere (Anexa la L190/2018).

- Termenul de remediere se stabileşte în funcţie de riscurile asociate prelucrării, precum şi demersurile necesar a fi îndeplinite pentru asigurarea conformităţi prelucrării iar în termen de 10 zile de la data expirării termenului de remediere, Autoritatea naţională de supraveghere poate relua controlul.

- Responsabilitatea îndeplinirii măsurilor de remediere revine autorităţii/organismului public care, potrivit legii, poartă răspunderea contravenţională pentru faptele constatate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare, cum ar fi:

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie)
	Neintomirea sau intocmirea defectuoasa de documente
	Acces neautorizat la baza de date sau documente
	Furtul de documente de catre terte persoane
	Distrugerea de documente de catre terte persoane
	Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

Evaluarea impactului asupra protecţiei datelor - înainte de începerea prelucrării, prin analiza tuturor caracteristicilor: natura, domeniul de aplicare, contextul şi scopurile prelucrării, pentru a identifica posibilele riscuri pentru drepturile şi libertăţile persoanelor fizice.

Evaluarea efectuată va conţine minim:

- o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
- o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;
- o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate;
- măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Evidenţele activităţilor de prelucrare

Fiecare operator sau reprezentantul acestuia trebuie să păstreaze **evidenţa activităţilor de prelucrare** desfăşurate care cuprinde **cel puţin**:

- numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI GENERALE	
PG – ALFABETA - 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL
PG – ALFABETA - 02	POLITICA PRIVIND RGPD
PG – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL IN ACTIVITATEA ORGANIZATIEI
PG – ALFABETA - 04	DATELE CU CARACTER PERSONAL CARE TREBUIE PROTEJATE
PG – ALFABETA - 05	MASURI TEHNICE SI ORGANIZATORICE
PG - ALFABETA - 06	PROCEDURA DE ACTIUNE IN SITUATIA UNUI INCIDENT DE SECURITATE
PG - ALFABETA - 07	PROCEDURA DE INTOCMIRE RASPUNS PERSOANA VIZATA

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI INTERNE	
PI – ALFABETA – 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIVIND ACTIVITATEA DE RESURSE UMANE RU
PI – ALFABETA – 02	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CURSURI/FORMARE PROFESIONALA A ADULTILOR
PI – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CONTRACTARI
PI – ALFABETA – 04	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) AFERENTA SERVICIILOR EXTERNALIZATE.
PI – ALFABETA – 05	PASTRAREA DATELOR CU CARACTER PERSONAL
PI – ALFABETA - 06	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) MONITORIZARE VIDEO

Modul 7: Aspecte specifice cu privire la rolul şi activitatea responsabilului cu protecţia datelor cu caracter personal

Responsabilul cu protecţia datelor cu caracter personal – rol, drepturi şi obligaţii, poziţie în cadrul organizaţiei;

Desemnarea responsabilului cu protecţia datelor cu caracter personal;

Rolul şi atribuţiile responsabilului cu protecţia datelor cu caracter personal în cadrul organizaţiei;

Poziţia responsabilului cu protecţia datelor cu caracter personal în cadrul organizaţiei;

Principiul obiectivităţii în desfăşurarea sarcinilor şi activităţilor responsabilului cu protecţia datelor cu caracter personal. Conflictul de interese cu alte structuri din cadrul organizţiei;

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RPD/DPO
RESPONSABILIL CU PROTECȚIA DATELOR / DATA PROTECTION OFFICER

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

- Ce organizaţii au nevoie de RPD/DPO?
- Care este rolul RPD/DPO în organizaţie?
- Responsabilităţile RPD/DPO .
- Drepturile RPD/DPO.
- Rolul RPD/DPO.
- Expertiza RPD/DPO.
- Calificările necesare RPD/DPO.
- Bune practici la angajarea RPD/DPO.

Desemnarea responsabilului cu protecţia datelor (art. 37 RGPD/GDPR)

Operatorul sau persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

- prelucrarea este efectuată de o **autoritate sau un organism public**, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;
- **activităţile principale** ale operatorului sau ale persoanei împuternicite de operator **constau în operaţiuni de prelucrare** care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o **monitorizare periodică şi sistematică a persoanelor vizate pe scară largă**;
- **activităţile principale** ale operatorului sau ale persoanei împuternicite de operator constau în **prelucrarea pe scară largă a unor categorii speciale de date**.

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

Autoritate publică sau un **organism public**

RGPD nu definește **exact** ce înseamnă „**autoritate publică sau organism public**”.

Așadar o astfel de încadrare va fi stabilită în conformitate cu dreptul intern. În consecință, autoritățile și organismele publice includ autoritățile naționale, regionale și locale, dar conceptul, în conformitate cu legislația națională aplicabilă, include, de asemenea, o serie de alte organisme guvernate de legislația în domeniul public. În astfel de cazuri, desemnarea unui DPO este obligatorie.

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

Activităţi principale

„**Activităţile principale ale operatorului sau ale persoanei împuternicite de operator**”, în sensul considerat de RGPD, se referă la *„activităţile de bază şi nu la prelucrarea datelor cu caracter personal drept activităţi auxiliare”, adică* acele **operaţiuni cheie** necesare pentru **îndeplinirea obiectivelor** operatorului sau persoanei împuternicite de operator.

Cu toate acestea, **activităţile principale** nu ar trebui interpretate ca excluzând activităţile în care prelucrarea datelor reprezintă o parte indisolubilă a activităţii operatorului sau persoanei împuternicite de operator.

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

Pe scară largă

RGPD impune ca în situaţia în care prelucrarea datelor cu caracter personal este efectuată pe scară largă se desemnează un DPO, însă nu definește ce anume constituie prelucarea pe scară largă.

Se recomandă ca următorii factori să fie luaţi în considerare atunci când se stabileşte dacă prelucarea este efectuată pe **scară largă**:

- numărul persoanelor vizate , ori un număr exact ori un procent din populaţia relevantă;
- volumul datelor şi/sau gama de elemente diferite de date în curs de prelucrare;
- durata sau permanenţa activităţii de prelucrare a datelor;
- suprafaţa geografică a activităţii de prelucrare.

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

Monitorizarea periodică şi sistematică

Conceptul de *„monitorizare a comportamentului persoanelor vizate”* include toate formele de urmărire şi profilare pe Internet, inclusiv în scop de publicitate comportamentală.

„periodic” ca însemnând una sau mai multe din următoarele:

- în curs de desfăşurare sau care apare la anumite intervale într-o anumită perioadă;
- recurente sau repetate la perioade fixe;
- constante sau care au loc periodic;

„sistematic” ca însemnând una sau mai multe din următoarele:

- apărut ca rezultat al implementarii sistemului;
- prearanjat, organizat sau metodic;
- ca parte a unui plan general de colectare a datelor;
- ca parte a unei strategii.

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

- orice **autoritate publică** sau un **organism public**, cu excepţia instanţelor în exercitarea funcţiei lor jurisdicţionale;

- organizaţiile care desfăşoară o **activitate principală** care conduce la realizarea unei **monitorizări constante şi sistematice pe scară largă** a persoanelor;

- organizaţiile care desfăşoară o activitate principală care constă în **prelucrarea pe scară largă** de date sensibile (cum ar fi : date privind originea rasială sau etnică, convingerile religioase, apartenenţa sindicală, date genetice, biometrice, privind starea de sănătate) sau referitoare la condamnări penale şi infracţiuni;

- **orice operator** care prelucrează **un număr de identificare naţional**, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, în scopul prevăzut la art. 6 alin. (1) lit. f) din Regulamentul general privind protecţia datelor, respectiv **al realizării intereselor legitime urmărite de operator sau de o parte terţă**. (pct. (2), art. 4, L190/2018).

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

Autoritate publică sau un **organism public (conform art. 2, legea 190/2018)**

„Camera Deputaţilor şi Senatul, Administraţia Prezidenţială, Guvernul, ministerele, celelalte organe de specialitate ale administraţiei publice centrale, autorităţile şi instituţiile publice autonome, autorităţile administraţiei publice locale şi deja nivel judeţean, alte autorităţi publice, precum şi instituţiile din subordinea/coordonarea acestora. În sensul prezentei legi, sunt asimilate autorităţilor/organismelor publice şi unităţile de cult şi asociaţiile şi fundaţiile de utilitate publică.”

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

Conform pct. (1), art. 10, Legea 190/2018:

”Desemnarea şi sarcinile responsabilului cu protecţia datelor Operatorii şi persoanele împuternicite de operator desemnează un responsabil cu protecţia datelor în situaţiile şi condiţiile prevăzute la art. 37-39 din Regulamentul general privind protecţia datelor.”

CINE TREBUIE SĂ NUMEASCĂ RPD/DPO?

Cu excepţia cazului în care este evident faptul că o organizaţie **nu este obligată** să desemneze un DPO, este recomandabil ca operatorii şi persoanele împuternicite de operator **să documenteze evaluările interne** efectuate pentru a determina dacă va fi numit un DPO, pentru a fi în măsură să demonstreze că au fost luaţi în considerare în mod corespunzător factorii relevanţi.

Această analiză poate fi solicitată de autoritatea de supraveghere şi ar trebui actualizată atunci când este necesar, atunci când întreprind activităţi noi sau furnizează servicii noi care intră sub incidenţa RGPD.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

NUMIREA D.P.O.

Ca regulă generală, funcţia de DPO trebuie reflectată în organigrama societăţii.

Ca atare, ar trebui să existe o decizie a organului societar competent prin care să se actualizeze structura organizatorică internă (fie în sensul că se creează o nouă poziţie, fie că se suplimentează atribuţiile unei poziţii deja existente, cu cele specifice DPO).

În plus, exerciţiul funcţiei de DPO trebuie să fie reglementată în raporturile contractuale cu persoana care va exercita funcţia de DPO.

Aceasta presupune încheierea unui contract de muncă (care să reglementeze atribuţiile specifice acestei funcţiei), dacă funcţia de DPO va fi ocupată de o persoană nou angajată.

NUMIREA D.P.O.

Dacă funcţia de DPO va fi ocupată de un angajat existent, societatea va trebui să semneze cu angajatul respectiv un act adiţional la contractul de muncă (prin care părţile vor agrea modificarea fişei postului, cu suplimentarea sarcinilor specifice unui DPO, precum şi eventualele ajustări privind remuneraţia cuvenită acestuia).

Dacă se modifică doar atribuţiile angajatului existent, părţile vor putea semna doar o fişă a postului actualizată, fără a fi necesară încheierea unui act adiţional la contractul de muncă.

Desigur, numirea unui DPO din rândul angajaţilor existenţi va putea fi făcută doar cu acordul respectivului angajat (i.e. desemnarea unui DPO nu poate fi făcută printr-o decizie unilaterală a angajatorului).

RESPONSABILITĂŢILE RPD/DPO

Definite în Articolul 39 al GDPR, **includ, dar nu sunt limitate** la următoarele:

❖**Educarea** companiilor şi a angajaţilor privind cerinţele importante de conformitate.

❖ **Pregătirea** personalului implicat în procesarea datelor personale.

❖**Efectuarea periodică de revizii de securitate** pentru a asigura conformitatea şi pentru a adresa în mod proactiv potenţialele probleme.

❖ Respectă secretul sau confidenţialitatea în ceea ce priveşte îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

❖Reprezentarea ca şi **punct de contact** între companii şi Autoritatea de Supraveghere.

RESPONSABILITATILE RPD/DPO

Definite în Articolul 39 al GDPR, **includ, dar nu sunt limitate** la următoarele:

❖**Monitorizarea performanţelor şi consilierea** cu privire la impactul efortului de protejare a datelor personale.

❖**Consiliere şi monitorizare** în legătură cu menţinerea de înregistrări complete ale tuturor activităţilor de procesare ale datelor personale efectuate de companii, incluzând scopul tuturor activităţilor de procesare care la cerere trebuie făcute publice.

❖**Urmărirea activităţilor de notificare către persoanele vizate** ale căror date sunt procesate pentru a-i informa cu privire la felul în care datele lor personale sunt folosite, la dreptul lor de a-şi avea datele personale şterse şi ce măsuri a luat compania pentru a le proteja informaţiile personale.

SARCINILE RPD/DPO

- **să informeze şi să consilieze** operatorul sau persoana împuternicită de operator, precum şi angajaţii acestora cu privire la obligaţiile existente în domeniul protecţiei datelor cu caracter personal;
- **să monitorizeze respectarea RGPD** şi a legislaţiei naţionale în domeniul protecţiei datelor;
- **să consilieze operatorul sau persoana împuternicită** în legătură cu realizarea de studii de impact privind protecţia datelor şi să verifice efectuarea acestora;
- **să reprezinte punctul de contact** în relaţia cu persoanele vizate în ceea ce priveşte exercitarea drepturilor lor;
- **să coopereze cu autoritatea pentru protecţia datelor** şi să reprezinte punctul de contact în relaţia cu aceasta.

DREPTURILE RPD/DPO

- Spijin activ al funcţiei DPO din partea managementului superior timp suficient pentru DPO în vederea îndeplinirii atribuţiilor sale.
- Sprijin corespunzător în ceea ce priveşte resursele financiare, infrastructură (sediu, facilităţi, echipament) şi personal, după caz.
- Comunicare oficială către toţi angajaţii cu privire la desemnarea DPO.
- Accesul necesar la alte servicii precum resurse umane, juridic, IT, securitate etc. astfel încât DPO să beneficieze de un sprijin esenţial, reacţii şi informaţii din partea altor servicii.

PROTECȚIA DREPTURILOR RPD/DPO

DPO-ul trebuie ***să beneficieze de separarea îndatoririlor față de alte departamente*** *și este necesar* ***să i se acorde independența și autoritate*** *pentru a-și îndeplini cu succes rolul.*

- Raportează celui mai înalt nivel ierarhic în organizaţie.
- Operează independent şi nu poate fi concediat sau penalizat în legatură cu activităţile pe care le execută.
- Aderând la codul de conduită şi obtinând certificare internațională, DPO va avea numeroase beneficii: credibilitate, expertiză, impunere.
- Oferă soluţii pentru a preveni sancţiunile aplicabile organizaţiei în legatură cu securitatea şi protecţia datelor personale.

GESTIONAREA CONFLICTELOR DE INTERESE

În general, se consideră că poate exista un conflict de interese dacă funcţia de DPO este ocupată de persoane care au funcţii executive (de decizie) cum ar fi:

- administrator/director general (în cazul acestora, în principiu, apare un conflict de interese general, având în vedere şi puterea decizională generală cu privire la activitatea unei societăţi),
- director financiar (acesta are putere de decizie cu privire la aspectele financiare şi, prin urmare, ar putea influenţa decizia de a aproba finanţarea unor/tuturor măsurilor specifice/necesare pentru conformarea cu cerinţele stabilite de legislaţia privind protecţia datelor),
- director de resurse umane (poate să influenţeze mecanismele de prelucrare a datelor angajaţilor, foştilor angajaţi, sau a potenţialilor angajaţi),
- directorul de marketing (poate să influenţeze mecanismele de prelucrare a datelor clienţilor în activitatea de marketing).

ATENŢIE!

- Un grup de întreprinderi poate numi un **responsabil cu protecţia datelor unic**, cu condiţia ca responsabilul cu protecţia datelor să fie **uşor accesibil** din fiecare întreprindere.

- Dacă operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat **un responsabil cu protecţia datelor unic** pentru **mai multe** dintre aceste **autorităţi sau organisme**, luând în considerare structura organizatorică şi dimensiunea acestora. (stipulat şi la pct. (2), art. 10, Legea 190/2018).

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ATENȚIE!

- În situaţia în care operatorul sau persoana împuternicită de operator **reprezintă categorii ori asociaţii şi alte organisme** de operatori sau de persoane împuternicite de operatori poate desemna **un singur responsabil cu protecţia datelor**.
- 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 online autorităţii de supraveghere – *formular_dpo_notificari_securizat*.

ASPECTE DE LUAT ÎN CALCUL LA NUMIREA RPD/DPO

- Monitorizarea respectării GDPR, a altor dispoziţii de drept referitoare la protecţia datelor şi a politicilor de protecţie a datelor cu caracter personal, prin folosirea optimî a resurselor puse la dispoziţie de operator. - *aptitudini manageriale, colegialitate, capacitatea de analiză şi sinteză, autodidact.*
- Desfăşurarea acţiunilor de sensibilizare şi de formare a personalului implicat în operaţiunile de procesare, precum şi evaluările aferente. – *aptitudini manageriale, colegialitate, capacitatea de a transmite informaţii, autodidact.*
- Furnizarea de consiliere, la cerere, în ceea ce priveste evaluarea impactului asupra protecţiei datelor şi monitorizarea funcţionării acestuia. – *aptitudini de comunicare în scris şi verbal, capacitate de analiză şi sinteză*.
- Punct de contact în ceea ce priveste exprimarea drepturilor de către persoanele vizate. - *aptitudini de comunicare în scris şi verbal,*
- Cooperarea cu autoritatea de supraveghere - punct de contact pentru autoritatea de supraveghere. (*practic e doar o chestiune de reprezentare, DPO acţionand ca persoana de contact).* - *aptitudini de comunicare în scris şi verbal, corectitudine, asumarea răspunderii.*

BUNE PRACTICI LA ANGAJAREA RPD/DPO

- să se identifice funcţiile care ar fi incompatibile cu funcţia de DPO;
- să se elaboreze norme interne în acest sens, care să includă o explicaţie mai generală cu privire la conflictele de interese, pentru a evita conflictele de interese;
- să se declare că DPO lor nu are niciun conflict de interese în ceea ce priveşte funcţia sa ca şi DPO, ca şi modalitate de creştere a gradului de conştientizare a acestei cerinţe;
- să se includă garanţii în normele interne ale organizaţiei şi să se asigure că anunţul de post vacant pentru funcţia de DPO sau contractul de prestări servicii este suficient de precis şi 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 funcţie de faptul dacă DPO este recrutat intern sau extern.

EXPERTIZA RPD/DPO

- Recomandabil a fi 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-şi îndeplini sarcinile specifice.

- Trebuie să fie **proporţională** cu **sensibilitatea, complexitatea şi volumul de date prelucrate** de organizaţie.

- DPO ar trebui ales cu atenţie, ţinând seama de **aspectele de protecţie a datelor** care apar în cadrul organizaţiei.

CALIFICĂRILE NECESARE RPD/DPO

- DPO să aibă **experienţă** în legislaţia şi practicile de protecţie a datelor la nivel naţional şi european, precum şi o înţelegere complexă a RGPD.
- **Cunoaşterea** sectorului de afaceri şi a organizării operatorului.
- DPO ar trebui, de asemenea, **să înţeleagă** operaţiunile de prelucrare efectuate, precum şi sistemele de informaţii şi necesităţile de securitate şi protecţie a datelor ale operatorului.
- În cazul unei **autorităţi publice** sau a unui **organism public**, DPO trebuie să aibă, de asemenea, cunoştinţă de regulile şi procedurile administrative ale organizaţiei.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

GESTIONAREA CONFLICTELOR DE INTERESE

Conflictul de interese este indisolubil legat de cerinţa independenţei DPO. Orice funcţii sau sarcini suplimentare încredinţate DPO care generează o presiune din zona de business (e.g. puteri de decizie sau chiar de execuţie în legătură cu scopurile şi mijloacele de prelucrare a datelor), contrară atribuţiilor legale ale DPO sunt surse ale conflictului de interese.

Nu există o listă a unor astfel de funcţii, ci acestea trebuie determinate de la caz la caz, întrucât structurile organizatorice şi procesele decizionale interne variază de la o societate la alta.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

GESTIONAREA CONFLICTELOR DE INTERESE

Ca principiu, GDPR nu instituie o interdicţie generală pentru un DPO de a exercita şi altă funcţie. Dimpotrivă, GDPR prevede că responsabilul cu protecţia datelor poate îndeplini şi alte sarcini şi atribuţii. Cu toate acestea, operatorul sau persoana împuternicită trebuie să se asigure că niciuna dintre aceste sarcini şi atribuţii nu generează un conflict de interese.

Conflictul de interese poate apărea în situaţia în care DPO-ul ar fi chemat să analizeze o chestiune în care el a decis sau pe care el a implementat-o în cadrul altei funcţii. Incompatibilităţile ar trebui să fie expres prevăzute de legislaţia în vigoare, ceea ce nu este cazul în acest moment.

GESTIONAREA CONFLICTELOR DE INTERESE

Conflicte de interese ar putea apărea și în legătură cu poziții care nu implică atribuții de conducere.

- consilierul juridic desemnat drept DPO care, totodată, ar fi autorizat să reprezinte societatea într-un litigiu privind legalitatea prelucrării datelor cu caracter personal.
- managerul IT care cumulează și poziția de DPO s-ar putea afla într-o poziție de conflict de interese întrucât acesta este răspunzător pentru calitatea măsurilor tehnice (de securitate IT) de conformare cu cerințele GDPR.


UNIUNEA EUROPEANĂ


GUVERNUL
ROMÂNIEI


POCU


Instrumente Structurale
2014-2020

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

EVALUAREA ACTIVITĂȚII UNUI DPO

GDPR nu reglementează mecanismele prin care activitatea DPO ar putea fi evaluată.

Ca atare, în scopul evaluării activității DPO-ului, ar putea fi implementate măsuri similare celor care sunt, în general, folosite pentru evaluarea activității angajaților.

Astfel, recomandăm redactarea unor politici interne clare, care să definească mecanismele de prelucrare a datelor, precum și procesele/măsurile corelative ce trebuie respectate/urmărite.

De asemenea, este necesară trasarea clară a sarcinilor și atribuțiilor DPO-ului prin politicile interne și fișa postului sau contractul încheiat cu DPO-ul, care să includă sarcini de raportare periodică către conducerea societății în care a fost desemnat.

Nu în ultimul rând, activitatea DPO-ului ar putea fi verificată în contextul auditării prin intermediul unor terți specialiști (consultanți în securitate cibernetică, avocați etc) a activității societății de prelucrare a datelor personale sau al unor controale din partea autorității pentru supravegherea prelucrării datelor cu caracter personal.

CONCLUZII:

- DPO **nu este** personal **responsabil** în caz de nerespectare a RGPD.

- Operatorul sau persoana împuternicită de operator **au în responsabilitate** să se asigure şi să fie în măsură **să demonstreze** că prelucrarea este efectuată în conformitate cu disponziţiile RGPD.

- Operatorului sau a persoanei împuternicite de operator îi revine sarcina de a asigura respectarea **normelor de protecţie a datelor** reprezintă responsabilitatea.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

COMPETIT – Formare și calificare pentru competitivitatea întreprinderilor

COD SMIS: 128223

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

RESPONSABIL CU PROTECȚIA DATELOR

PERSOANĂ VIZATĂ – orice persoană fizică identificată sau identificabilă direct sau indirect, în special prin referire la un element de identificare.

DATE CU CARACTER PERSONAL - orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată”)

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

OPERATOR - persoana fizică sau juridică, autoritatea publică, agenţia sau alt organism care, singur sau împreună cu altele, prelucrează date cu caracter personal când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern

Drepturile operatorului

- Dreptul de a prelucra date cu caracter personal cu respectarea principiilor legalităţii
- Dreptul de a numi persoane împuternicite
- Dreptul de a se asocia
- Dreptul de a-şi apăra interesele/bunurile

PRELUCRARE - orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

DREPTURILE PERSOANEI VIZATE

- **Dreptul de acces al persoanei vizate**
- **Dreptul la rectificare**
- **Dreptul la ștergerea datelor („dreptul de a fi uitat”)**
- **Dreptul la restricționarea prelucrării**
- **Dreptul la portabilitatea datelor**
- **Dreptul la opoziție**

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ASIGURARA PROTECȚIEI DATELOR

- "**privacy by design**"- dezvoltatorii de aplicaţii trebuie să se asigure, încă din stadiul dezvoltării, că aplicaţia lor va respecta regulile şi principiile stabilite de Regulament;
- "**privacy by default**".- furnizorii de aplicaţii care prelucrează date personale trebuie să se asigure că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/asupra a ceea ce postează sau împărtăşesc cu alţi utilizatori.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

Identificarea scopurilor prelucrării

Identificarea categoriilor de persoane vizate

Identificarea datelor cu caracter personal prelucrate

Identificarea bazei legale a prelucrării

Identificarea metodelor tehnice de prelucrare

Identificarea terţilor cărora li se transmit prelucrările/datele

Opţional – baza legală a transmiterii

Identificarea riscurilor prelucrării

Identificarea măsurilor tehnice şi organizatorice implementate/necesare

Identificarea duratei de prelucrare/păstrare/distrugere

Opţional – baza legală a păstrării/distrugerii

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL III DREPTURILE PERSOANEI VIZATE

IDENTIFICAREA FLUXURILOR DE PRELUCRARE A DATELOR

RISCURILE PRELUCRĂRII

FACTORI DE RISC SPECIFICI IDENTIFICATI	DESCRIEREA/ FORMA DE MANIFESTARE A RISCULUI
FACTORI DE RISC FIZICI	
Patrundere frauduloasa (patrundere prin efractie)	Patrunderea persoanelor neautorizate folosind diferite metode, in zonele protejate in scopul a sustragerii de bunuri, valori si documente ce contin DCP
Furt	Sustragerea de de bunuri, documente, ce contin DCP
Acte de vandalism, talharie, jaf, terorism.	Distrugerea de bunuri, valori, implicit documente ce contin DCP, prin violenta, intimidare, etc.
Defectiuni/ avarii ale instalatiilor electrice (pane de curent accidentale si/sau provocate, fluctuatii ale tensiunii in retea etc.)	Provoaca: - pierderea partiala si/sau totala a bazei de date; - avarierea/ distrugerea partiala si/sau totala a sistemului informatic (calculatoare, servere, etc.),
Defectiuni instalatii gaz	Explozii si incendii, si deci implicit distrugerea partiala sau totala a bazelor de date ce contin DCP atat pe suport hartie cat si pe suport electronic.
Defectiuni instalatii apa/ incalzire	Inundatii in incaperi, si deteriorarea sau distrugerea documentelor ce contin DCP, pe suport de hartie cat si cele pe suport electronic
Incendii	Distrugerea totala sau partiala a bazei de date atat pe suport fizic hartie cat si electronic
FACTORI DE RISC DEPENDENTI DE PERSONAL	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Sustragerea de documente si/sau fisiere ce contin DCP	Insusirea fara drept de documente si/sau fisiere ce contin DCP, in diferite scopuri personale (vanzare, instrainare, etc.)
Pierderea de DCP	Pierderea s-a petrecut in timpul transportuluI/transferului acestora de la sediu la terti
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Transmiterea (instrainarea) fara drept catre terti a DCP (cu sau fara intentie)
	Neintomirea sau intocmirea defectuoasa de documente
	Acces neautorizat la baza de date sau documente
	Furtul de documente de catre terte persoane
	Distrugerea de documente de catre terte persoane
	Transmiterea din gerseala catre terti neautorizati a DCP prelucrate in alta parte decat la serviciu
FACTORI DE RISC PRIVIND SISTEMUL INFORMATIC	
Sustragerea de documente si/sau fisiere ce contin DCP de catre terti	Provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa, virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Sustragerea de documente si/sau fisiere ce contin DCP	Virusarea sistemului informatic, copierea, distrugerea BD, introducere de date false.
Pierderea de DCP	Copierea, distrugerea BD, introducere de date false, provoaca disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.
Nerespectarea prevederilor privind procedurile specifice, a obligatiilor conform fisei de post si a regulamentului intern	Distrugerea partiala/totala a bazei de date ce contine DCP, si/sau a intregului sistem informatic, provoace disfunctionalitati ale sistemului infornatic din culpa sau cu rea vointa.

Evaluarea impactului asupra protecţiei datelor - înainte de începerea prelucrării, prin analiza tuturor caracteristicilor: natura, domeniul de aplicare, contextul şi scopurile prelucrării, pentru a identifica posibilele riscuri pentru drepturile şi libertăţile persoanelor fizice.

Evaluarea efectuată va conţine minim:

- o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
- o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;
- o evaluare a riscurilor pentru drepturile şi libertăţile persoanelor vizate;
- măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Evidenţele activităţilor de prelucrare

Fiecare operator sau reprezentantul acestuia trebuie să păstreaze **evidenţa activităţilor de prelucrare** desfăşurate care cuprinde **cel puţin**:

- numele şi datele de contact ale operatorului şi, după caz, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului cu protecţia datelor;
- scopurile prelucrării;
- o descriere a categoriilor de persoane vizate şi a categoriilor de date cu caracter personal;
- categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale;
- dacă este cazul, transferurile de date cu caracter personal către o ţară terţă sau o organizaţie internaţională, inclusiv identificarea ţării terţe sau a organizaţiei internaţionale respective şi, documentaţia care dovedeşte existenţa unor garanţii adecvate;
- acolo unde este posibil, termenele-limită preconizate pentru ştergerea diferitelor categorii de date;
- acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate.

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI GENERALE	
PG – ALFABETA - 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL
PG – ALFABETA - 02	POLITICA PRIVIND RGPD
PG – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL IN ACTIVITATEA ORGANIZATIEI
PG – ALFABETA - 04	DATELE CU CARACTER PERSONAL CARE TREBUIE PROTEJATE
PG – ALFABETA - 05	MASURI TEHNICE SI ORGANIZATORICE
PG - ALFABETA - 06	PROCEDURA DE ACTIUNE IN SITUATIA UNUI INCIDENT DE SECURITATE
PG - ALFABETA - 07	PROCEDURA DE INTOCMIRE RASPUNS PERSOANA VIZATA

COD PROCEDURA	DENUMIRE PROCEDURA
PROCEDURI INTERNE	
PI – ALFABETA – 01	PRELUCRAREA DATELOR CU CARACTER PERSONAL PRIVIND ACTIVITATEA DE RESURSE UMANE RU
PI – ALFABETA – 02	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CURSURI/FORMARE PROFESIONALA A ADULTILOR
PI – ALFABETA - 03	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) COMPARTIMENT CONTRACTARI
PI – ALFABETA – 04	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) AFERENTA SERVICIILOR EXTERNALIZATE.
PI – ALFABETA – 05	PASTRAREA DATELOR CU CARACTER PERSONAL
PI – ALFABETA - 06	PRELUCRAREA DATELOR CU CARACTER PERSONAL (PDCP) MONITORIZARE VIDEO

STRUCTURA RGPD - CAPITOLUL VIII CĂI DE ATAC, RĂSPUNDERE ŞI SANCŢIUNI

SANCŢIUNI

În concepţia RGPD, sancţiunile civile (răspunderea civilă) pot coexista cu cele administrative. Sancţiunile administrative (amenzi) vor fi aplicate de către autoritatea naţională şi vor fi uriaşe, comparativ cu sancţiunile care pot fi aplicate astăzi de către Autoritate:

- ✓ Mustrare.
- ✓ Măsuri corective (ex. limitare temporară sau definitivă, suspendare, restricţionarea prelucrării).
- ✓ Acţiune judecătorească (despăgubiri).
- ✓ Amendă de până la 10 sau 20 mil. Euro.
- ✓ Amendă de până la 4% din cifra de afaceri mondială totală anuală.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

STRUCTURA RGPD - CAPITOLUL VIII CĂI DE ATAC, RĂSPUNDERE ŞI SANCȚIUNI

SANCȚIUNI

Pentru încălcarea:

- obligaţiilor operatorului şi ale persoanei împuternicite de operator;
- obligaţiilor organismului de certificare;
- obligaţiilor organismului de monitorizare;

se aplică **amenzi administrative de până la 10 000 000 EUR** sau, în cazul unei întreprinderi, de până la **2 % din cifra de afaceri mondială totală anuală** corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

Pentru încălcarea:

- principiilor de bază pentru prelucrare, inclusiv condiţiile privind consimţământul;
- drepturilor persoanelor vizate;
- modului de efectuare a transferurilor de date cu caracter personal către un destinatar dintr-o ţară terţă sau o organizaţie internaţională;
- orice obligaţii în temeiul legislaţiei naţionale adoptate în temeiul capitolului IX;
- nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării f luxurilor de date, emisă de către autoritatea de supraveghere sau neacordarea accesului

se aplică amenzi **administrative de până la 20 000 000 EUR** sau, în cazul unei întreprinderi, de până la **4 % din cifra de afaceri mondială totală anuală** corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

Pentru încălcarea unui ordin emis de autoritatea de supraveghere se aplică **amenzi administrative de până la 20 000 000 EUR** sau, în cazul unei întreprinderi, de până la **4 % din cifra de afaceri mondială totală anuală** corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare.

Desemnarea responsabilului cu protecţia datelor (art. 37 RGPD/GDPR)

Operatorul sau persoana împuternicită de operator desemnează un responsabil cu protecţia datelor ori de câte ori:

- prelucrarea este efectuată de o **autoritate sau un organism public**, cu excepţia instanţelor care acţionează în exerciţiul funcţiei lor jurisdicţionale;
- **activităţile principale** ale operatorului sau ale persoanei împuternicite de operator **constau în operaţiuni de prelucrare** care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o **monitorizare periodică şi sistematică a persoanelor vizate pe scară largă**;
- **activităţile principale** ale operatorului sau ale persoanei împuternicite de operator constau în **prelucrarea pe scară largă a unor categorii speciale de date**.

Conform pct. (1), art. 10, Legea 190/2018:

”Desemnarea şi sarcinile responsabilului cu protecţia datelor

Operatorii şi persoanele împuternicite de operator desemnează un responsabil cu protecţie datelor în situaţiile şi condiţiile prevăzute la art. 37-39 din Regulamentul general privind protecţia datelor.”

Modul 8: Managementul riscului şi securitatea informaţiei

Sistemul de management al securităţii informaţiei în contextul prelucrării datelor cu caracter personal

Cerinţele în vigoare aplicabile în domeniul securităţii informaţionale – roluri, responsabilităţi şi autorităţi

Organizarea securităţii informaţiei, implementarea securităţii informaţiilor

Ciclul de viaţă al sistemelor informatice

Integrarea securităţii şi a vieţii private în ciclul de viaţă

Controlul calităţii sistemelor informatice

Securitatea administrării activelor

Securitatea de software şi proceduri

Securitatea aplicată tehnologiilor şi documentaţiei informatice

Cadrul general al evaluării şi gestionării riscurilor

Criterii de evaluare a riscului

Metodologii de analiză şi evaluare a riscurilor de securitate a informaţiilor

Evaluarea riscurilor

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

MANAGEMENTUL RISCULUI
ŞI
SECURITATEA INFOMAŢIEI

Există două categorii de date cu caracter personal pe care orice companie/instituţie/organism trebuie să le gestioneze:

- cele despre clienţi şi parteneri/furnizori;
- cele despre angajaţi.

ATENȚIE!

Datele cu caracter personal se pot regăsi în prelucrări cu format :

- **document tipărit;**

- **informaţie stocată pe un dispozitiv de transport al informaţiilor (stick, CD, DVD, hard-disk extern, etc.);**

- **informaţie procesată/stocată într-un sistem informatic de calcul.**

Securitatea prelucrării datelor cu caracter personal

Operatorul şi persoana împuternicită de acesta trebuie să implementeze **măsuri tehnice şi organizatorice** adecvate în vederea asigurării unui nivel de securitate datelor cu caracter personal (transmise, stocate sau prelucrate într-un alt mod) care să includă cel puţin:

- pseudonimizarea şi criptarea datelor cu caracter personal;
- capacitatea de a restabili disponibilitatea datelor cu caracter personal şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

La evaluarea nivelului adecvat de securitate, se ţine seama în special de riscurile prezentate de prelucrare, generate în special, în mod **accidental sau ilegal**, de:

- distrugerea;
- pierderea;
- modificarea;
- divulgarea neautorizată;
- accesul neautorizat.

MĂSURI TEHNICE ŞI ORGANIZATORICE

- Generarea automată a registrului de monitorizare a accesului la datele cu caracter personal şi a tuturor operaţiunilor asupra acestora prin mecanisme specifice.
- Posibilitatea de a oferi din câteva click-uri informaţiile deţinute despre o persoană conform cerinţelor GDPR având acces direct la fişa personală.
- Implementarea de mecanisme automate de atenţionare privind modalităţile de contactare acceptate de persoanele de contact din baza de date a companiei/instituţiei/entităţii.
- Crearea de log-uri la nivelul bazei de date pentru detectarea violării datelor cu caracter personal (identificarea breşelor de securitate).
- Centralizarea tuturor canalelor prin care se pot colecta date personale cu menţinerea informaţiei despre sursă şi data (pagina web, scanare cărţi de vizită, telefon, e-mail, etc).
- Controlul riguros al generării de duplicate ale fişierelor cu date.
- Implementarea procedurii de autorizare controlată şi procedurată a accesului la datele cu caracter personal.
- Controlul fluxurilor care implică prelucrarea datelor cu caracter personal.

ATENȚIE!

Obiectivele securității informației sunt:

- **confidențialitatea**: informația este accesibilă doar persoanelor autorizate;
- **integritatea** păstrarea informației și a metodelor de procesare în condiții cât mai sigure;
- **disponibilitatea**: doar utilizatorii autorizați au acces la informație și la resursele asociate atunci când este necesar.

OBSERVAȚIE: Pentru a concepe și implementa un sistem de management al securității informației (SMSI) trebuie să fie definite responsabilitățile și autoritatea necesare pentru toate funcțiile care sunt implicate în realizarea SMSI.

Securitatea informaţiei are eficacitate atunci când se implementează un set adecvat de politici, practici, proceduri, structuri organizaţionale şi măsuri software.

Uneltele aflate la dispoziţie sunt:

- **evaluarea riscurilor**: prin care se identifică ameninţările asupra resurselor, se evaluează vulnerabilitatea la aceste ameninţări, probabilitatea de producere a lor şi potenţialul impact asupra organizaţiei;
- **legislaţia în vigoare existentă** pe care orice organizaţie trebuie să o respecte;
- **analiza securităţii**: verificarea, actualizarea şi instruirea personalului în ceea ce priveşte setul specific de principii, obiective şi cerinţe adoptate pentru procesarea informaţiei în cadrul organizaţiei.

Analiza riscurilor într-o organizaţie presupune, în general, patru etape principale:

- identificarea resurselor care trebuie protejate;
- identificarea riscurilor/ameninţărilor specifice fiecărei resurse;
- ierarhizarea riscurilor;
- identificarea măsurilor prin care vor fi eliminate/diminuate riscurile.

Analiza a securităţii trebuie să cuprindă:

- selecţia soluţiilor viabile;
- stabilirea strategiei de asigurare a securităţii;
- compartimentarea şi controlul conexiunilor;
- compartimentarea comunicaţiilor;
- compartimentarea reţelelor;
- compartimentarea serviciilor şi aplicaţiilor folosite;
- apărarea pe nivele;
- strategia de răspuns la incidente;
- alocarea resurselor pentru securizare;
- stabilirea politicilor de securitate;
- realizarea şi implementarea mecanismelor şi procedurilor de securitate;
- auditul intern şi extern.

Pentru definirea politicii de securitate organizaţia trebuie să se decidă:

- care ameninţări trebuie eliminate şi care se pot tolera;
- care resurse trebuie protejate şi la ce nivel;
- cu ce mijloace poate fi implementată securitatea;
- care este preţul (financiar, uman, social etc.) măsurilor de securitate care poate fi acceptat.

ATENŢIE!

Un mecanism de control **nu trebuie să depăşească** valoarea bunului ce trebuie protejat.

Cerinţe privind sistemul de management al securităţii informaţiei.

Clasificarea informaţiei

Scopul urmărit: să asigure faptul că informaţia beneficiază de un nivel de protecţie adecvat. Informaţiile trebuie clasificate în funcţie de valoare, cerinţe legale, importantă şi criticalitate pentru organizaţie.

Organizaţia trebuie să elaboreze instrucţiuni pentru clasificarea informaţiilor, care sunt adecvate pentru nevoile organizaţiei, atât pentru controlul cât şi pentru partajarea informaţiilor.

Un set corespunzător de norme pentru etichetarea informaţiei şi manipularea informaţiei trebuie elaborat şi implementat în conformitate cu structura de clasificare adoptată de către organizaţie.

Cerinţe privind sistemul de management al securităţii informaţiei.

Securitatea fizică

Scopul urmărit: să prevină accesul fizic neautorizat, distrugerile şi pătrunderea în interiorul organizaţiei, precum şi accesul la informaţii.

Organizaţia trebuie să utilizeze perimetre de securitate pentru a proteja zonele care conţin informaţii şi facilităţi de prelucrare a informaţiilor.

Zonele de securitate trebuie protejate prin măsuri de control, de acces adecvate pentru a se asigura că numai personalului autorizat îi este permis accesul.

Trebuie realizată o evaluare a riscurilor, pentru a determina tipul de control al accesului care este necesar pentru siguranţa acestor zone de securitate.

Cerinţe privind sistemul de management al securităţii informaţiei.

Securitatea echipamentelor

Scopul urmărit: prevenirea pierderii, avarierii, furtului sau compromiterii resurselor şi întreruperii activităţii organizaţiei.

Echipamentele trebuie să fie:

amplasate şi protejate astfel încât să se reducă riscurile faţă de ameninţările, pericolele şi faţă de posibilităţile de acces neautorizat;

protejate împotriva efectelor penelor de curent şi a altor întreruperi cauzate de probleme ale utilităţilor suport;

corect întreţinuţi, pentru a se asigura disponibilitatea continuă şi integritatea acestora, prin mentenanţă preventivă.

Echipamentele, informaţiile nu trebuie scoase în afara spaţiului de lucru fără o autorizaţie prealabilă şi cu aplicarea unor măsuri de securitate adecvate.

Cerinţe privind sistemul de management al securităţii informaţiei.

Managementul comunicaţiilor

Scopul urmărit: să se asigure operarea corectă şi în condiţii de securitate a sistemelor de procesare a informaţiei.

Pentru protejarea schimbului de informaţii, folosind orice tip de dispozitiv de comunicare, trebuie implementate politici, proceduri şi măsuri de securitate specifice schimbului de informaţii.

Relaţiile de schimb pentru schimbul de informaţii între organizaţie şi alte părţi trebuie stabilite prin acorduri specifice.

Informaţia transmisă prin mesageria electronică trebuie protejată în mod corespunzător.

Cerinţe privind sistemul de management al securităţii informaţiei.

Politici şi proceduri

Scopul urmărit: să se asigure prelucrarea corectă şi în condiţii de securitate a informaţiilor corespunzătoare modului de interconectare a sistemelor informaţionale.

Politica organizaţiei ar trebui concepută în aşa fel încât informaţiile să aibă o clasificare de un nivel minim de confidenţialitate posibil, pentru a permite accesul tuturor celor care trebuie şi sunt abilitaţi să aibă acces la ea.

Stabilirea nivelului de confidenţialitate trebuie să aibă în vedere sensibilitatea şi faptul că informaţia, în orice formă şi pe ce suport se procesează, trebuie să fie protejată în conformitate cu clasificarea acesteia.

- **Cerinţe privind sistemul de management al securităţii informaţiei.**

Responsabilităţile pentru resurse

Regulile pentru utilizarea în mod acceptabil a informaţiilor şi resurselor asociate sistemelor de procesare a informaţiilor trebuie identificate, documentate şi implementate.

Obiectivul: prevenirea accesului neautorizat al utilizatorului, precum şi compromiterea sau furtul de informaţii şi sisteme de procesare a informaţiilor.

Utilizatorilor sistemelor informatice trebuie să:

- cunoască şi respecte bunele practici de securitate, în ceea ce priveşte selecţia şi utilizarea parolelor;
- cunoască şi respecte procedura de păstrare a ecranului protejat în cazul sistemelor de procesare a informaţiilor;
- cunoască şi respecte procedura de protecţie a echipamentul lăsat nesupravegheat;
- cunoască şi respecte modul de lucru cu documentele şi informaţiile din sistemele informatice şi mediile de stocare amovibile.

Cerinţe privind sistemul de management al securităţii informaţiei.

Tratarea incidentelor de securitate a informaţiei

Pentru ca răspunsul la un posibil incident de securitate a informaţiei să fie **rapid, eficient** şi să **limiteze daunele,** trebuie ca evenimentele de securitate a informaţiei şi punctele slabe asociate sistemelor informaţionale:

- să fie identificate şi comunicate de către angajaţi şi/sau celelalte părţi interesate;
- să fie raportate structurii/responsabilului cu Securitatea Informaţiei, cât mai curând posibil.
- să fie documentate şi implementate responsabilităţile şi regulile specifice pentru a asigura un răspuns rapid, eficace şi sistematic la incidentele de securitate ale informaţiei.
- structura/responsabilul cu Securitatea Informaţiei să măsoare şi să monitorizeze tipurile, volumul şi costurile incidentelor de securitate ale informaţiei şi să se informeze părţile interesate.

Cerinţe privind sistemul de management al securităţii informaţiei.

Cerinţe minime privind protecţia antivirus

- programul antivirus trebuie să fie instalat şi programat pentru pornire automată. Baza de date a acestui program trebuie menţinută la zi prin update-uri (actualizări) periodice;
- sistemele de calcul virusate trebuie scoase din reţea până când nu vor fi devirusate prin scanarea cu programul de antivirus;
- toate activităţile care au intenţia sau pot crea sau distribui programe ce conţin viruşi sau coduri maliţioase în reţea (ex: virus, trojan etc) trebuie interzise;
- la configurarea unui calculator nou, până la instalarea unui program de antivirus, se vor utiliza numai software-uri originale;
- orice software-uri comerciale trebuie scanate de antivirus înainte de a fi instalate;
- pentru a putea proteja datele în cazul virusării calculatorului, pentru fiecare sistem de calcul se face un back-up (salvare) periodic.

Cerinţe privind sistemul de management al securităţii informaţiei.

Cerinţe minime privind utilizarea corespondenţei electronice

- stabilite reguli clare şi reale pentru modul de transmitere a mesajelor de tip e-mail;
- transmiterea mesajelor ce conţin date confidenţiale să nu se efectueze înainte ca acestea să obţină acceptul pentru transmitere;
- informaţiile confidenţiale transmise prin e-mail să fie criptate în concordanţă cu politica de securitate a organizaţiei;
- e-mail-urile trebuie scanate automat de viruşi sau alte software-uri maliţioase;
- nu trebuie admisă folosirea contului de e-mail al organizaţiei în interese personale.

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

ÎNTREBĂRI?

VĂ MULȚUMESC.