					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P17					Titlul documentului: **Politica de protecție a datelor și a confidențialității**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 5.1, 6.1.3, 8.1, 10	Controale generale, tehnice și de îmbunătățire continuă relevante pentru protecția datelor
ISO/IEC 27002:2022	Controalele 5.34, 8.10, 8.11, 8.12	Controale pentru gestionarea PII, retenție, ștergere, anonimizare și drepturile persoanelor vizate
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Cerințe privind guvernanța, riscul, managementul accesului, jurnalizarea, răspunsul la încălcări și programul de confidențialitate
GDPR al UE	Articolele 5, 6, 12–23, 25, 28, 30, 32–34; Considerentul 78	Toate cerințele de bază privind confidențialitatea, responsabilitatea, drepturile persoanelor vizate, cererile persoanelor vizate, încălcările securității, precum și principiile de protecție a datelor încă din faza de proiectare și în mod implicit
Directiva NIS2 a UE	Articolul 21(2)(e), (f)	Controale de securitate bazate pe risc pentru entitățile esențiale și importante
Regulamentul DORA al UE	Articolele 6(2)(d), 11(1)(c), 15(1), 17	Guvernanță, risc asociat terților și termene pentru prelucrarea securizată
COBIT 2019	APO12, DSS01, DSS05, MEA	Managementul riscurilor, operațiuni securizate, monitorizarea conformității

1. Scop

1.1 Prezenta politică stabilește principiile organizaționale obligatorii și cerințele tehnice pentru protecția datelor cu caracter personal și aplicarea protecției datelor încă din faza de proiectare în toate mediile.

1.2 Aceasta formalizează responsabilitățile organizației în raport cu standardele internaționale și cadrele de reglementare, asigurând că datele cu caracter personal sunt colectate, prelucrate, păstrate, partajate și eliminate în mod legal, securizat și transparent.

1.3 Prezenta politică consolidează, de asemenea, conformitatea cu legislația și cadrele aplicabile în materie de confidențialitate, inclusiv GDPR al UE, Directiva NIS2 a UE, Regulamentul DORA al UE, ISO/IEC 27001:2022 și COBIT 2019.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor unităților organizaționale, întregului personal și tuturor sistemelor implicate în prelucrarea datelor cu caracter personal, inclusiv:

2.1.1 angajaților, contractanților, consultanților și furnizorilor terți de servicii.

2.1.2 datelor colectate din surse interne și externe în toate funcțiile organizației.

2.1.3 mediilor fizice și digitale, inclusiv serviciilor cloud, platformelor SaaS, dispozitivelor mobile și înregistrărilor pe suport hârtie.

2.1.4 tuturor mediilor, inclusiv sistemelor de producție, dezvoltare, testare și backup, în care pot exista date cu caracter personal.

2.2 Aceasta acoperă toate activitățile de prelucrare reglementate de legislația și standardele aplicabile privind confidențialitatea, inclusiv, fără a se limita la:

2.2.1 colectarea, stocarea, utilizarea, transmiterea și eliminarea datelor cu caracter personal.

2.2.2 exercitarea drepturilor persoanelor vizate, documentarea temeiului juridic și gestionarea consimțământului.

2.2.3 transferurile transfrontaliere, notificarea încălcărilor și partajarea datelor cu terți.

2.2.4 proiectarea securizată și aplicarea protecției datelor în mod implicit în sisteme și procese.

3. Obiective

3.1 Asigurarea unei prelucrări legale, transparente și responsabile a datelor cu caracter personal, în conformitate cu ISO/IEC 27001:2022 și cu obligațiile legale asociate.

3.2 Integrarea principiilor de protecție a datelor încă din faza de proiectare și în mod implicit în toate sistemele informatice, serviciile și procesele organizației.

3.3 Aplicarea măsurilor tehnice și organizatorice (TOMs) care protejează confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal pe întreg ciclul lor de viață.

3.4 Definirea rolurilor de guvernanță și a structurilor de responsabilizare pentru protecția datelor, inclusiv responsabilitățile Responsabilului cu protecția datelor (DPO), ale funcției de securitate a informațiilor, ale funcției juridice și ale proprietarilor datelor.

3.5 Asigurarea conformității depline cu articolele 5, 6, 25, 30 și 32 din GDPR, precum și cu cerințele de reducere a riscului și reziliență prevăzute de NIS2 și DORA.

3.6 Respectarea drepturilor persoanelor vizate, inclusiv accesul, rectificarea, ștergerea, restricționarea, portabilitatea, opoziția și protecția împotriva procesului decizional automatizat.

3.7 Atenuarea riscurilor de reglementare, reputaționale, juridice și operaționale generate de accesul neautorizat, utilizarea necorespunzătoare sau pierderea datelor cu caracter personal.

4. Roluri și responsabilități

4.1 Managementul executiv

4.1.1 Asigură supravegherea strategică și alocă resurse suficiente pentru susținerea programului de confidențialitate.

4.1.2 Aprobă prezenta politică și asigură aplicarea acesteia la nivelul întregii organizații.

4.2 Responsabilul cu protecția datelor (DPO)

4.2.1 Acționează independent pentru a supraveghea conformitatea cu reglementările privind protecția datelor.

4.2.2 Menține Registrul activităților de prelucrare (RoPA) în conformitate cu articolul 30 din GDPR.

4.2.3 Coordonează relația cu autoritățile de reglementare, realizează evaluări de impact asupra protecției datelor (DPIA) și gestionează procesele de notificare a încălcărilor.

4.2.4 Revizuiește excepțiile privind confidențialitatea și menține Registrul excepțiilor privind confidențialitatea.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Cerințe de revizuire și actualizare

9.1 Prezenta politică trebuie revizuită cel puțin anual sau mai devreme în următoarele condiții:

9.1.1 actualizări legale sau de reglementare semnificative (de exemplu, modificări ale GDPR, termene DORA)

9.1.2 sisteme noi sau activități noi de prelucrare care implică date cu caracter personal

9.1.3 constatări ale auditului intern care indică lacune la nivel de politică

9.1.4 incidente semnificative de încălcare sau feedback din partea autorităților de supraveghere

9.2 Responsabilități privind revizuirea

9.2.1 DPO trebuie să inițieze revizuirea politicii, în coordonare cu funcțiile juridic, risc, securitatea informațiilor și managementul executiv.

9.2.2 Toate actualizările trebuie înregistrate în Registrul de control al documentelor al SMSI și distribuite părților interesate afectate.

9.3 Controlul schimbărilor

9.3.1 Orice revizuire a prezentei politici trebuie aprobată formal de managementul executiv.

9.3.2 Versiunile perimate trebuie arhivate în condiții de securitate, iar versiunea actualizată trebuie să includă un istoric documentat al modificărilor.

10. Politici conexe și interdependențe

10.1 P1 – Politica de securitate a informațiilor. Stabilește principiile generale de guvernanță a securității care stau la baza prezentei politici de confidențialitate. P1 susține confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal în toate sistemele și serviciile.

10.2 P6 – Politica de management al riscurilor. Definește metodologia organizației pentru tratarea riscurilor, esențială pentru evaluarea riscurilor privind confidențialitatea, procesele DPIA și evaluările riscului rezidual impuse de GDPR și de clauza 6.1.3 din ISO/IEC 27001.

10.3 P13 – Politica de clasificare și etichetare a datelor. Ghidează clasificarea datelor cu caracter personal și a datelor sensibile, constituind baza pentru aplicarea controalelor adecvate de confidențialitate, inclusiv retenția, limitarea accesului și eliminarea securizată.

10.4 P14 – Politica de păstrare și eliminare a datelor. Susține în mod direct cerințele de confidențialitate prevăzute la articolele 5(1)(e) și 17 din GDPR, asigurând că datele cu caracter personal sunt păstrate doar atât timp cât este necesar și eliminate în condiții de securitate, în conformitate cu obligațiile legale.

10.5 P16 – Politica de mascare a datelor și pseudonimizare. Stabilește controale pentru reducerea posibilității de identificare a datelor cu caracter personal prin măsuri tehnice precum tokenizarea, mascarea dinamică și pseudonimizarea, asigurând astfel aplicarea articolului 32 din GDPR și a controlului 5.34 din ISO/IEC 27002.

10.6 P30 – Politica de răspuns la incidente. Prezintă protocoalele obligatorii de răspuns la încălcări, integrate cu gestionarea încălcărilor de confidențialitate și termenele de notificare prevăzute la articolele 33 și 34 din GDPR.

10.7 P33 – Politica de audit și monitorizare a conformității. Impune evaluări programate ale eficacității programului de confidențialitate, aplicării politicii și urmăririi acțiunilor corective la nivelul unităților organizaționale și al persoanelor împuternicite terțe.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 5.1 – Leadership și angajament: stabilește responsabilitatea la nivel executiv pentru protejarea datelor cu caracter personal și aplicarea principiilor de confidențialitate.

11.1.2 Clauza 6.1.3 – Managementul riscurilor de securitate a informațiilor: susține identificarea, evaluarea și tratarea riscurilor privind confidențialitatea prin DPIA și excepții.

11.1.3 Clauza 8.1 – Planificare și control operațional: impune măsuri tehnice și procedurale de protecție pentru a asigura prelucrarea securizată a datelor cu caracter personal.

11.1.4 Clauza 10.1 – Îmbunătățire continuă: impune evaluarea periodică și adaptarea programului de confidențialitate.

11.2 ISO/IEC 27002:2022 Controalele 5.34, 8.10, 8.11, 8.12: oferă îndrumări privind gestionarea PII, aplicarea retenției, ștergerea, anonimizarea și transparența privind drepturile persoanelor vizate.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: definesc responsabilitățile privind guvernanța, rolurile, responsabilizarea și instruirea în materie de confidențialitate.

11.3.2 PL-2, PL-8: impun integrarea controalelor de confidențialitate în ciclul de viață al sistemelor și în arhitectura organizației.

11.3.3 AC-2, AC-6: impun principiul privilegiului minim și managementul conturilor pentru protecția datelor cu caracter personal.

11.3.4 AU-2, AU-6, AU-9: impun jurnalizarea, trasabilitatea și integritatea auditului pentru accesul la date cu caracter personal.

11.3.5 IR-4, IR-5, IR-6: definesc procese structurate de detectare, analiză și raportare pentru încălcările de confidențialitate.

11.3.6 PM-1, PM-21, PM-23: stabilesc un program cuprinzător de confidențialitate, aliniat la obiectivele strategice privind riscul și guvernanța datelor.

11.4 GDPR al UE (2016/679)

11.4.1 Articolele 5, 6, 12–23, 25, 28, 30, 32–34: reglementează prelucrarea legală, limitarea scopului, drepturile persoanelor vizate, responsabilitatea, protecția datelor încă din faza de proiectare și în mod implicit, obligațiile terților și managementul încălcărilor.

11.4.2 Considerentul 78: consolidează principiile de protecție a datelor încă din faza de proiectare.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolul 21(2)(e) și (f): impune implementarea controalelor de securitate bazate pe risc și protecția datelor cu caracter personal în sfera entităților esențiale și importante.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 6(2)(d): impune guvernanța internă pentru riscul TIC aferent gestionării datelor.

11.6.2 Articolul 11(1)(c): impune supravegherea riscului asociat terților pentru serviciile legate de date.

11.6.3 Articolele 15(1) și 17: impun prelucrarea securizată a datelor de către furnizorii de servicii și notificări prompte către autoritățile de supraveghere ca urmare a incidentelor TIC.

11.7 COBIT 2019

11.7.1 APO12 – Managementul riscurilor: integrează riscul privind confidențialitatea în supravegherea mai amplă a riscurilor la nivelul organizației.

11.7.2 DSS01 – Operațiuni gestionate și DSS05 – Servicii de securitate: asigură operațiuni securizate, inclusiv controlul accesului, retenția și integritatea sistemelor.

11.7.3 MEA03 – Monitorizarea conformității: impune revizuirea continuă a stării de conformitate în raport cu obligațiile de confidențialitate de natură reglementară și cele prevăzute în politici.