					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P37					Titlul documentului: **Politica de conformitate juridică și de reglementare**							
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**

1. Scop

1.1 Prezenta politică stabilește cadrul obligatoriu pentru identificarea, gestionarea și respectarea tuturor obligațiilor juridice, de reglementare și contractuale relevante pentru securitatea informațiilor, protecția datelor și funcțiile operaționale ale organizației.

1.2 Scopul este prevenirea neconformității care ar putea conduce la amenzi, răspundere juridică, perturbarea activităților organizației, prejudicii de imagine sau măsuri de aplicare impuse de autoritățile de reglementare.

1.3 Prezenta politică sprijină integrarea obligațiilor de conformitate în structurile de guvernanță, procesele de management al riscurilor, fluxurile operaționale de lucru, ciclurile de viață ale proiectelor și arhitectura sistemelor.

1.4 Aceasta asigură că toate obligațiile relevante — la nivel de jurisdicții, sectoare de activitate și domenii de reglementare — sunt documentate clar, evaluate, monitorizate și aplicate în cadrul organizației.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică tuturor departamentelor, funcțiilor, unităților de afaceri și persoanelor care acționează în numele organizației, inclusiv:

2.1.1 angajaților permanenți și temporari;

2.1.2 contractorilor, consultanților și stagiarilor;

2.1.3 furnizorilor terți, persoanelor împuternicite de operator sau partenerilor care gestionează datele, sistemele sau responsabilitățile de reglementare ale organizației;

2.1.4 oricărui proces operațional, proiect sau inițiativă supus(ă) cerințelor juridice sau de reglementare.

2.2 Domeniile de conformitate reglementate prin prezenta politică includ, fără a se limita la:

2.2.1 obligațiile privind securitatea informațiilor și securitatea cibernetică (de exemplu, ISO/IEC 27001, NIS2, DORA);

2.2.2 legislația privind protecția datelor și viața privată (de exemplu, GDPR, legi sectoriale privind confidențialitatea);

2.2.3 reglementările sectoriale (de exemplu, financiar, medical, auto, apărare);

2.2.4 obligațiile contractuale care decurg din acorduri de confidențialitate (NDA), acorduri privind nivelul serviciilor (SLA) sau acorduri de prelucrare încheiate cu terți;

2.2.5 cerințele juridice privind raportarea incidentelor, interacțiunea cu organele de aplicare a legii și transferurile internaționale de date.

3. Obiective

3.1 Să asigure că toate legile, reglementările, standardele și obligațiile contractuale aplicabile sunt identificate, documentate, interpretate și implementate la nivelul întregii organizații.

3.2 Să integreze cerințele juridice și de reglementare în Sistemul de management al securității informației (SMSI), procesele de management al riscurilor, acordurile cu furnizorii și proiectarea produselor și serviciilor.

3.3 Să asigure un mecanism de monitorizare proactivă a modificărilor de reglementare și de actualizare corespunzătoare a controalelor și documentației.

3.4 Să definească responsabilități clare pentru supravegherea conformității, escaladarea încălcărilor, gestionarea excepțiilor și raportarea externă.

3.5 Să asigure caracterul verificabil și soliditatea poziției juridice și de reglementare a organizației în cadrul inspecțiilor, investigațiilor sau auditurilor de certificare.

4. Roluri și responsabilități

4.1 Conducerea executivă

4.1.1 Deține responsabilitatea strategică pentru alinierea juridică și de reglementare la nivelul întregii organizații.

4.1.2 Revizuiește și aprobă deciziile de conformitate cu risc ridicat, inclusiv acceptarea riscurilor și litigiile.

4.2 Responsabilul de conformitate / Directorul juridic / Consilierul juridic

4.2.1 Menține Registrul obligațiilor de conformitate, care include toate legile, standardele, certificările și clauzele contractuale aplicabile.

4.2.2 Efectuează evaluări ale impactului juridic pentru servicii noi, piețe noi sau fluxuri noi de date.

4.2.3 Oferă interpretarea autorizată a legilor și standardelor.

[... 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 Revizuirea anuală a politicii

9.1.1 Prezenta politică trebuie revizuită cel puțin o dată în fiecare an calendaristic pentru a:

9.1.1.1 asigura menținerea alinierii cu legislația actualizată, standardele din industrie și cadrele de reglementare;

9.1.1.2 valida eficacitatea operațională pe baza constatărilor de audit și a istoricului incidentelor;

9.1.1.3 reflecta modificările organizaționale (de exemplu, jurisdicții, sisteme sau linii de activitate noi).

9.2 Revizuiri declanșate de evenimente

9.2.1 Revizuirile intermediare trebuie inițiate atunci când:

9.2.2 intră în vigoare sau este actualizată o nouă cerință juridică sau de reglementare;

9.2.3 un incident de conformitate sau un audit evidențiază deficiențe ale politicii;

9.2.4 organizația intră pe o piață nouă sau într-o nouă linie de servicii guvernată de cadre de conformitate distincte;

9.2.5 tendințele de aplicare sau ghidurile autorităților de reglementare indică modificări ale profilului de risc.

9.3 Responsabilitate și aprobare

9.3.1 Departamentul juridic și responsabilul de conformitate răspund în comun de coordonarea procesului de revizuire.

9.3.2 Revizuirile finale ale politicii trebuie aprobate de conducerea executivă și înregistrate în registrul modificărilor de politici, împreună cu referințele aferente de control al modificărilor și planurile de comunicare.

9.4 Controlul versiunilor și comunicare

9.4.1 Orice versiune actualizată a prezentei politici trebuie:

9.4.1.1 să includă un rezumat al modificărilor-cheie;

9.4.1.2 să fie redistribuită prin canale oficiale (de exemplu, portalul de politici, LMS, buletine informative interne);

9.4.1.3 să necesite confirmarea luării la cunoștință din partea personalului afectat, în special din rolurile juridice, operaționale, de securitate și de management al furnizorilor.

10. Politici conexe și interdependențe

10.1 Prezenta politică funcționează împreună cu următoarele politici din cadrul SMSI al organizației și le consolidează:

10.1.1 P1 – Politica de securitate a informațiilor: stabilește principiile fundamentale de guvernanță care asigură că toate politicile de securitate a informațiilor — inclusiv cele de conformitate — sunt aliniate cu obiectivele strategice ale organizației și cu cerințele de reglementare.

10.1.2 P2 – Politica privind rolurile și responsabilitățile de guvernanță: definește autoritățile decizionale, inclusiv rolurile juridice și de conformitate responsabile de supravegherea de reglementare și de asumarea răspunderii.

10.1.3 P6 – Politica de management al riscurilor: sprijină evaluarea, asumarea și atenuarea riscurilor juridice și de conformitate cu reglementările la nivelul întregii organizații.

10.1.4 P8 – Politica privind conștientizarea și instruirea în domeniul securității informațiilor: asigură că întregul personal este informat cu privire la responsabilitățile de conformitate și primește instruire adecvată rolului.

10.1.5 P12 – Politica de management al activelor: consolidează obligațiile juridice privind gestionarea și protejarea activelor reglementate sau contractuale, inclusiv a celor care implică date cu caracter personal și infrastructuri critice.

10.1.6 P30 – Politica de răspuns la incidente: reglementează notificările juridice obligatorii (de exemplu, articolul 33 din GDPR) și procedurile de escaladare în cazul unei încălcări de conformitate sau al unui eveniment de reglementare.

10.1.7 P33 – Politica de audit și monitorizare a conformității: furnizează activități structurate de asigurare — inclusiv testarea și remedierea controalelor și colectarea dovezilor — necesare pentru verificarea internă și externă a conformității.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 4.2 – Înțelegerea nevoilor și așteptărilor părților interesate: impune identificarea și integrarea cerințelor juridice și de reglementare în SMSI.

11.1.2 Clauza 5.1 – Leadership și angajament: impune responsabilitatea executivă pentru stabilirea și menținerea conformității juridice la nivelul întregii organizații.

11.1.3 Clauza 5.3 – Roluri, responsabilități și autorități organizaționale: asigură claritatea rolurilor pentru supravegherea juridică și conformitatea cu reglementările.

11.1.4 Controlul 5.36 din Anexa A – Conformitatea cu cerințele juridice, statutare, de reglementare și contractuale: stabilește cerința de a identifica și îndeplini obligațiile care decurg din legi, reglementări și contracte.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.36: detaliază ghidul de implementare pentru menținerea unui registru al obligațiilor de conformitate, validarea cerințelor de reglementare și asigurarea păstrării structurate a dovezilor.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PL-1 – Politica și procedurile de planificare a securității: impune integrarea obligațiilor de conformitate în structurile de guvernanță și în documentație.

11.3.2 PM-1 – Planul programului de securitate a informațiilor: impune includerea controalelor de reglementare în programul general de securitate.

11.3.3 CA-7 – Monitorizare continuă: sprijină supravegherea eficacității controalelor în îndeplinirea cerințelor juridice și a celor prevăzute în politici.

11.3.4 AU-9 – Protecția informațiilor de audit: asigură că jurnalele și înregistrările de audit privind conformitatea sunt protejate și disponibile pentru inspecție.

11.4 GDPR al UE (2016/679)

11.4.1 Articolul 5 – Principii privind prelucrarea: impune legalitatea prelucrării, transparența și responsabilitatea.

11.4.2 Articolul 6 – Legalitatea prelucrării: impune existența unor temeiuri juridice adecvate pentru toate activitățile de prelucrare a datelor.

11.4.3 Articolul 24 – Responsabilitatea operatorului: stabilește responsabilitatea directă pentru asigurarea conformității cu reglementările.

11.4.4 Articolul 32 – Securitatea prelucrării: impune implementarea unor măsuri tehnice și organizatorice adecvate.

11.4.5 Articolul 33 – Notificarea încălcării: impune raportarea încălcărilor securității datelor cu caracter personal către autoritățile relevante în termen de 72 de ore.

11.5 Directiva NIS2 a UE (2022/2555)

11.5.1 Articolele 20–21: impun entităților esențiale și importante să implementeze guvernanță documentată, strategii de conformitate juridică și revizuirea continuă a riscurilor juridice.

11.6 Regulamentul DORA al UE (2022/2554)

11.6.1 Articolul 5(2) – Managementul riscurilor TIC: impune integrarea conformității juridice în funcțiile generale de management al riscurilor și supraveghere.

11.6.2 Articolul 19 – Riscul asociat terților în domeniul TIC: impune cerințe juridice specifice pentru gestionarea obligațiilor contractuale și de reglementare care implică furnizori și platforme externe.

11.7 COBIT 2019

11.7.1 APO12 – Manage Risk: include conformitatea juridică și cu reglementările ca elemente critice ale guvernanței riscurilor la nivelul organizației.

11.7.2 MEA03 – Monitor Compliance with External Requirements: definește monitorizarea continuă, gestionarea excepțiilor și pregătirea pentru audit pentru toate formele de obligații de reglementare.