					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P37S					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**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	Controlul 5	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
RGPD al UE	Articolele 5, 6, 32, 33	
Directiva NIS2 a UE	Articolele 21(2)(a), 21(2)(f), 23	
Regulamentul DORA al UE	Articolele 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Scop

1.1 Această politică definește abordarea organizației privind identificarea, respectarea și demonstrarea conformității cu obligațiile juridice, de reglementare și contractuale.

1.2 Aceasta stabilește responsabilități clare și măsuri practice pentru a sprijini organizația în îndeplinirea obligațiilor sale de conformitate, inclusiv în raport cu legislația privind protecția datelor, cadrele de securitate cibernetică, acordurile cu clienții și standardele de certificare.

1.3 Aceasta asigură că, inclusiv în absența unei echipe dedicate de conformitate, organizația poate menține operațiuni conforme din punct de vedere juridic, poate răspunde corespunzător la incidente și poate păstra capacitatea de a demonstra conformitatea în cadrul auditurilor.

1.4 Această politică este esențială pentru obținerea certificării ISO/IEC 27001:2022 și pentru îndeplinirea cerințelor externe ale clienților, autorităților de reglementare sau partenerilor.

2. Domeniu de aplicare

2.1 Această politică se aplică:

2.1.1 tuturor angajaților, contractorilor, colaboratorilor independenți și furnizorilor terți.

2.1.2 tuturor serviciilor, activităților operaționale, sistemelor și activităților de gestionare a datelor în cadrul cărora organizația trebuie să respecte cerințe legale sau contractuale.

2.1.3 tuturor locațiilor și dispozitivelor utilizate pentru prelucrarea informațiilor organizației, indiferent dacă acestea sunt la birou, la distanță sau găzduite în cloud.

2.2 Politica acoperă:

2.2.1 legislația privind protecția datelor, precum RGPD al UE.

2.2.2 reglementările de securitate cibernetică, precum Directiva NIS2 a UE.

2.2.3 obligațiile specifice sectorului, după caz.

2.2.4 contractele cu clienții, acordurile de confidențialitate și clauzele de audit.

2.2.5 certificările voluntare (de exemplu, ISO 27001) și politicile interne care trebuie aplicate pentru asigurarea conformității.

3. Obiective

3.1 Stabilirea responsabilităților: alocarea clară a responsabilităților pentru monitorizarea, actualizarea și aplicarea obligațiilor juridice, de reglementare și contractuale.

3.2 Protejarea organizației: reducerea la minimum a riscului de încălcări legale, sancțiuni financiare, incidente de securitate a datelor și prejudicii reputaționale.

3.3 Asigurarea pregătirii pentru audit: menținerea unor înregistrări verificabile care demonstrează modul în care organizația își îndeplinește obligațiile de conformitate.

3.4 Sprijinirea integrării în politici: asigurarea faptului că obligațiile juridice și de reglementare sunt aplicate consecvent în toate politicile și procesele relevante.

3.5 Gestionarea transparentă a excepțiilor: asigurarea faptului că orice excepții de la cerințele de conformitate sunt documentate, justificate și aprobate, pentru a evita expunerea juridică.

4. Roluri și responsabilități

4.1 Directorul general (GM)

4.1.1 Deține responsabilitatea generală pentru conformitatea juridică și de reglementare a organizației.

4.1.2 Menține Registrul de conformitate și se asigură că acesta este actualizat.

4.1.3 Revizuiește contractele cu clienții și se asigură că obligațiile specifice sunt urmărite și aplicate.

4.1.4 Aprobă excepțiile de la obligațiile de conformitate numai atunci când acestea sunt justificate din punct de vedere juridic și sunt însoțite de controale compensatorii.

4.2 Consilieri externi (de exemplu, consultanți juridici, IT sau de conformitate)

4.2.1 Sprijină Directorul general prin identificarea legilor, certificărilor și obligațiilor aplicabile (de exemplu, RGPD, NIS2, ISO 27001).

4.2.2 Oferă îndrumare privind interpretarea noilor reglementări sau a modificărilor aduse legislației existente.

4.2.3 Pot sprijini actualizarea politicilor, auditurile sau răspunsul la incidente atunci când există expunere juridică.

[... 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 Revizuire anuală programată

9.1.1 Această politică trebuie revizuită la fiecare 12 luni de către Directorul general.

9.1.2 Revizuirea trebuie să confirme:

9.1.2.1 relevanța în raport cu contextul juridic și contractual curent.

9.1.2.2 reflectarea corectă a acordurilor cu clienții și a obligațiilor de serviciu.

9.1.2.3 alinierea cu Registrul de conformitate și cu celelalte politici.

9.2 Actualizări determinate de evenimente

9.2.1 Este necesară o revizuire imediată dacă:

9.2.1.1 devine aplicabilă o nouă lege sau reglementare (de exemplu, o nouă cerință privind protecția datelor).

9.2.1.2 un client introduce în acordul său condiții complexe de conformitate.

9.2.1.3 are loc o încălcare sau un incident de neconformitate.

9.2.1.4 compania se extinde pe o piață sau într-un sector reglementat.

9.3 Aprobarea actualizărilor și controlul versiunilor

9.3.1 Toate actualizările trebuie documentate, supuse controlului versiunilor și aprobate de Directorul general.

9.3.2 Versiunile istorice trebuie păstrate în scopuri de audit și juridice.

9.4 Comunicarea modificărilor

9.4.1 Personalul și contractorii trebuie informați cu privire la modificările politicii în termen de 5 zile lucrătoare de la aprobare.

9.4.2 Orice furnizori afectați trebuie, de asemenea, să confirme actualizarea condițiilor înainte de continuarea furnizării serviciilor.

10. Politici conexe și interdependențe

10.1 Această politică este susținută și aplicată prin următoarele politici SME:

10.1.1 P3S – Politica de utilizare acceptabilă: previne comportamentele care pot încălca cerințe legale sau contractuale (de exemplu, partajarea neautorizată de fișiere).

10.1.2 P8S – Politica privind conștientizarea și instruirea în domeniul securității informațiilor: instruiește personalul cu privire la obligațiile de conformitate și la modul de evitare a încălcărilor.

10.1.3 P14S – Politica de păstrare și eliminare a datelor: asigură practici de gestionare a datelor conforme pe întreg ciclul de viață al informațiilor.

10.1.4 P17S – Politica de protecție a datelor și confidențialitate: îndeplinește cerințele RGPD și cerințele clienților privind gestionarea datelor.

10.1.5 P30S – Politica de răspuns la incidente: stabilește modul de răspuns la încălcările securității datelor sau la neîndeplinirea cerințelor de conformitate, inclusiv termenele de notificare a încălcărilor.

10.1.6 P36S – Politica privind rețelele sociale și comunicările externe: asigură că comunicările publice nu încalcă obligații legale sau de reglementare.

10.2 Fiecare politică conexă aplică o parte a cadrului de conformitate juridică și trebuie aplicată în mod coordonat cu celelalte.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 6.1 – Acțiuni pentru tratarea riscurilor și oportunităților: include riscurile de conformitate.

11.1.2 Clauza 8.1 – Planificare și control operațional: impune executarea proceselor care respectă cerințele legale și contractuale.

11.2 ISO/IEC 27002

11.2.1 Controlul 5.36 – Ghidează organizația în menținerea înregistrărilor obligațiilor și în asigurarea unor răspunsuri adecvate la cerințele juridice și de reglementare.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politică și proceduri: impune politici formale de conformitate.

11.3.2 PM-1 – Planul programului de securitate a informațiilor: impune integrarea conformității juridice în planificarea securității.

11.3.3 CA-1 – Evaluare, autorizare și monitorizare.

11.3.4 AU-1 – Politica de audit: impune menținerea dovezilor de conformitate.

11.4 RGPD al UE

11.4.1 Articolul 5 – Principiile prelucrării datelor, inclusiv responsabilitatea demonstrării conformității.

11.4.2 Articolul 6 – Temeiul juridic al prelucrării.

11.4.3 Articolul 32 – Securitatea prelucrării.

11.4.4 Articolul 33 – Notificarea încălcării în termen de 72 de ore.

11.5 Directiva NIS2 a UE

11.5.1 Articolul 21(2)(a) și (f) – Politici interne pentru controlul riscului și al cerințelor de reglementare.

11.5.2 Articolul 23 – Aplicare și sancțiuni pentru neconformitate.

11.6 Regulamentul DORA al UE

11.6.1 Articolul 5(2) – supravegherea gestionării riscurilor TIC.

11.6.2 Articolul 9(1) – guvernanța internă a conformității.

11.6.3 Articolul 17 – relațiile contractuale cu furnizorii de servicii TIC.

11.7 COBIT 2019

11.7.1 APO12 – Managed Risk: asigură urmărirea și tratarea riscurilor de conformitate.

11.7.2 APO13 – Managed Security: acoperă aplicarea, pe bază de risc, a cerințelor de reglementare și contractuale.

11.7.3 DSS01 – Managed Operations: impune pregătirea operațională pentru îndeplinirea obligațiilor legale.