					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P17S					Titlul documentului: **Politica de protecție a datelor și confidențialitate**							
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	
ISO/IEC 27002:2022	Controalele 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
RGPD al UE	Articolul 5, 6, 12-23, 30, 32-34	
Directiva NIS2 a UE	Articolul 21(2)(e), 21(2)(f)	
Regulamentul DORA al UE	Articolele 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Scop

1.1. Această politică definește modul în care organizația protejează datele cu caracter personal în conformitate cu obligațiile legale, cerințele de reglementare și standardele internaționale de securitate.

1.2. Aceasta asigură că datele cu caracter personal — indiferent dacă aparțin clienților, personalului sau partenerilor — sunt colectate, utilizate, stocate și șterse într-un mod legal, echitabil și securizat.

1.3. Această politică asigură, de asemenea, conformitatea cu ISO/IEC 27001:2022 și sprijină pregătirea pentru audit prin impunerea unei abordări consecvente, bazate pe risc, privind protecția vieții private.

1.4. Prin această politică, organizația demonstrează responsabilitate și consolidează încrederea clienților prin prioritizarea transparenței, a reducerii la minimum a datelor și a unei guvernanțe solide a confidențialității.

2. Domeniu de aplicare

2.1. Această politică se aplică:

2.1.1. tuturor angajaților, contractorilor sau furnizorilor de servicii care accesează, prelucrează sau gestionează date cu caracter personal;

2.1.2. oricărui sistem, aplicație sau amplasament în care datele cu caracter personal sunt stocate sau transmise;

2.1.3. tuturor datelor cu caracter personal, indiferent dacă sunt stocate electronic, pe suport hârtie, în sisteme cloud sau pe dispozitive mobile.

2.2. Această politică se aplică datelor referitoare la clienți, personal, furnizori și orice alte persoane identificabile.

2.3. Politica rămâne aplicabilă indiferent dacă datele sunt prelucrate intern sau de către furnizori terți de servicii.

3. Obiective

3.1. Asigurarea faptului că datele cu caracter personal sunt gestionate în conformitate cu legislația privind confidențialitatea și standardele de securitate, inclusiv RGPD, NIS2 și ISO 27001.

3.2. Protejarea datelor cu caracter personal împotriva accesului neautorizat, utilizării necorespunzătoare, modificării sau pierderii prin controale tehnice și organizatorice clare.

3.3. Respectarea drepturilor persoanelor vizate, inclusiv dreptul de acces, rectificare și ștergere a datelor.

3.4. Stabilirea unor roluri și responsabilități clare pentru protecția datelor în cadrul organizației.

3.5. Impunerea reducerii la minimum a datelor, a păstrării securizate și a ștergerii la timp în toate sistemele și procesele.

3.6. Reducerea riscului de neconformitate, sancțiuni legale, prejudicii reputaționale sau pierderea încrederii clienților.

4. Roluri și responsabilități

4.1. Director general (DG)

4.1.1. Aprobă această politică și asigură aplicarea acesteia.

4.1.2. Asigură resursele necesare pentru gestionarea riscurilor privind confidențialitatea și pentru răspunsul la incidente.

4.1.3. Deține responsabilitatea generală pentru conformitatea cu legislația și standardele privind confidențialitatea.

4.2. Responsabil cu protecția datelor/confidențialitatea (intern sau externalizat)

4.2.1. Menține evidența activităților de prelucrare a datelor.

4.2.2. Răspunde solicitărilor persoanelor vizate și cererilor autorităților de reglementare.

4.2.3. Sprijină evaluările de risc, instruirea și implementarea politicii.

4.2.4. Documentează incidentele de încălcare a securității și notifică autoritățile atunci când este necesar.

[... 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. Revizuiri programate

9.1.1. Această politică trebuie revizuită cel puțin o dată la 12 luni de către Responsabilul cu protecția datelor/confidențialitatea și aprobată de Directorul general.

9.1.2. Revizuirea trebuie să evalueze relevanța politicii, alinierea la reglementări și eficacitatea operațională.

9.2. Declanșatori pentru revizuirea intermediară

9.2.1. Actualizările politicii trebuie inițiate și ca răspuns la:

9.2.1.1. legi noi sau revizuite privind protecția datelor (de exemplu, RGPD, DORA);

9.2.1.2. incidente de securitate sau încălcări ale confidențialității care implică date cu caracter personal;

9.2.1.3. lansarea de sisteme, instrumente sau servicii noi care prelucrează date cu caracter personal;

9.2.1.4. constatări semnificative de audit sau recomandări ale autorităților de reglementare.

9.3. Controlul modificărilor și comunicare

9.3.1. Toate modificările aduse politicii trebuie documentate formal într-un registru al modificărilor.

9.3.2. Versiunile revizuite trebuie distribuite întregului personal și contractorilor relevanți.

9.3.3. Versiunile arhivate trebuie păstrate pentru asigurarea unei piste de audit privind conformitatea.

10. Politici conexe și interdependențe

10.1. Această politică funcționează împreună cu alte politici SME pentru a crea un cadru complet și aplicabil de protecție a confidențialității:

10.1.1. P13S – Politica de clasificare și etichetare a datelor: Asigură clasificarea corespunzătoare a datelor cu caracter personal, astfel încât măsurile de protecție a confidențialității să poată fi aplicate în funcție de risc.

10.1.2. P14S – Politica de păstrare și eliminare a datelor: Oferă reguli clare privind durata de păstrare a datelor cu caracter personal și metodele securizate de eliminare a acestora după expirare.

10.1.3. P16S – Politica de mascare și pseudonimizare a datelor: Specifică modul în care identificatorii personali trebuie transformați înainte ca datele să fie utilizate în medii care nu sunt de producție sau partajate extern.

10.1.4. P30S – Politica de răspuns la incidente: Acoperă pașii necesari pentru răspunsul la încălcarea securității datelor, inclusiv notificarea autorităților de reglementare și a persoanelor afectate în termenele prevăzute.

10.1.5. P2S – Politica privind rolurile și responsabilitățile de guvernanță: Clarifică structura de responsabilitate și rolurile de autoritate decizională aplicabile implementării și supravegherii cerințelor de confidențialitate.

10.2. Aceste politici conexe trebuie revizuite și aplicate împreună pentru a asigura acoperirea completă a cerințelor de confidențialitate la nivelul sistemelor, personalului și furnizorilor.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 5.1 – Impune conducerii de vârf să demonstreze leadership și angajament pentru protejarea datelor cu caracter personal.

11.1.2. Clauza 6.1.3 – Impune tratarea riscurilor legate de prelucrarea informațiilor cu caracter personal.

11.1.3. Clauza 8.1 – Impune implementarea controalelor operaționale pentru protejarea datelor pe întreg ciclul de viață al informației.

11.2. ISO/IEC 27002

11.2.1. Controlul 5.34 – Oferă linii directoare de implementare privind protejarea confidențialității și gestionarea în condiții de securitate a informațiilor cu caracter personal (PII).

11.2.2. Controlul 8.10 – Abordează eliminarea securizată a datelor cu caracter personal pentru a preveni divulgarea reziduală.

11.2.3. Controlul 8.11 – Sprijină utilizarea mascării și pseudonimizării pentru reducerea la minimum a datelor.

11.2.4. Controlul 8.12 – Previne scurgerile neautorizate de date prin controale privind accesul la date și utilizarea acestora.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – Atribuie roluri și responsabilități pentru gestionarea riscului privind confidențialitatea.

11.3.2. PL-5 – Impune documentarea planului de confidențialitate care acoperă utilizarea și protecția datelor.

11.3.3. AC-6 – Impune principiul privilegiului minim și controale de acces pentru datele cu caracter personal.

11.3.4. IR-4 – Impune procese de gestionare a incidentelor pentru încălcări care implică date cu caracter personal.

11.4. RGPD al UE

11.4.1. Articolul 5 – Definește principiile de bază ale prelucrării legale, echitabile și transparente a datelor.

11.4.2. Articolul 6 – Impune existența unui temei juridic valabil pentru fiecare activitate de prelucrare a datelor cu caracter personal.

11.4.3. Articolele 12–23 – Descriu drepturile persoanelor vizate, inclusiv accesul, rectificarea, ștergerea și opoziția.

11.4.4. Articolul 30 – Impune evidența activităților de prelucrare.

11.4.5. Articolul 32 – Impune măsuri tehnice și organizatorice de securitate adecvate.

11.4.6. Articolele 33–34 – Stabilesc obligațiile de notificare a încălcărilor către autorități și persoanele vizate.

11.5. NIS2 a UE

11.5.1. Articolul 21(2)(e) – Impune măsuri pentru asigurarea protecției datelor aliniate la politicile de securitate cibernetică.

11.5.2. Articolul 21(2)(f) – Impune mecanisme pentru gestionarea securității datelor cu caracter personal și a datelor confidențiale în sistemele TIC.

11.6. DORA al UE

11.6.1. Articolul 6 – Impune cadre interne de guvernanță pentru gestionarea riscului privind datele și protecția acestora.

11.6.2. Articolul 15 – Obligă entitățile financiare să se asigure că furnizorii terți protejează datele cu caracter personal și sprijină conformitatea cu reglementările.

11.6.3. Articolul 17 – Impune organizațiilor să se asigure că sistemele TIC care prelucrează date cu caracter personal sunt securizate, reziliente și monitorizate.

11.7. COBIT 2019

11.7.1. APO12 – Gestionarea riscurilor: impune identificarea și tratarea riscurilor privind confidențialitatea și protecția datelor.

11.7.2. DSS05 – Gestionarea serviciilor de securitate: impune măsuri de protecție pentru prevenirea accesului neautorizat la date cu caracter personal.

11.7.3. MEA03 – Monitorizarea conformității: impune organizațiilor să asigure conformitatea continuă cu legislația privind confidențialitatea și protecția datelor.