					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P16S					Titlul documentului: **Politica de mascare a datelor și pseudonimizare**							
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	Clauza 6.1.3, Clauza 8	Riscurile de securitate a informațiilor și controalele necesare, inclusiv mascarea/pseudonimizarea
ISO/IEC 27002:2022	Controalele 8.11, 8.12	Ghid privind mascarea și prevenirea scurgerilor de date
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Obfuscare a datelor, tehnologii de consolidare a confidențialității
Directiva NIS2 a UE	Articolul 21(2)(c)	Măsuri tehnice proporționale, pseudonimizarea ca și control
Regulamentul DORA al UE	Articolul 10(1)	Controale privind riscurile TIC, inclusiv măsuri de protecție pentru transformarea datelor
COBIT 2019	DSS05.01, DSS06	Protecția datelor, tehnici de obfuscare/pseudonimizare
GDPR al UE	Articolele 4(5), 5(1)(c), 32	Reducerea la minimum a datelor, pseudonimizarea ca și control tehnic

1. Scop

1.1. Prezenta politică stabilește cerințe obligatorii pentru utilizarea mascării datelor și a pseudonimizării în vederea protejării datelor sensibile, a datelor cu caracter personal și a datelor confidențiale în cadrul întreprinderilor mici și mijlocii (IMM-uri).

1.2. Aceste tehnici sunt obligatorii atunci când datele reale nu sunt necesare, cum ar fi în scenarii de dezvoltare, analiză sau furnizare de servicii de către terți, contribuind la reducerea riscurilor de expunere, utilizare abuzivă sau încălcare a securității datelor.

1.3. Prezenta politică sprijină direct conformitatea cu ISO/IEC 27001:2022, precum și cu cerințele europene de reglementare, cum ar fi GDPR, Directiva NIS2 și Regulamentul DORA.

1.4. Prin transformarea datelor înainte de utilizarea acestora în afara contextului lor operațional inițial, organizația limitează expunerea la răspundere și își consolidează capacitatea de a demonstra diligența necesară în materie de confidențialitate și securitate.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică tuturor datelor structurate sau nestructurate clasificate drept date cu caracter personal, confidențiale sau sensibile, indiferent dacă sunt stocate sau prelucrate:

2.1.1. În medii de producție, testare sau dezvoltare

2.1.2. Pe dispozitive locale, servere sau platforme cloud

2.1.3. De către personal intern, contractori sau furnizori terți

2.2. Politica acoperă, de asemenea, toate instrumentele de transformare a datelor (mascare, tokenizare, pseudonimizare), indiferent dacă sunt open-source, comerciale sau dezvoltate intern.

2.3. Cazurile de utilizare care intră sub incidența acestei politici includ:

2.3.1. Pregătirea seturilor de date pentru testare sau dezvoltare

2.3.2. Exportul datelor către sisteme de analiză

2.3.3. Accesul furnizorilor sau consultanților la sisteme operaționale

2.3.4. Reducerea la minimum a datelor prelucrate pentru diminuarea riscului asociat prelucrării

3. Obiective

3.1. Să se asigure că datele reale cu caracter personal sau datele sensibile nu sunt niciodată expuse în medii cu un nivel de securitate mai redus, în care acestea nu sunt esențiale.

3.2. Să se impună tehnici de mascare sau pseudonimizare atunci când identificatorii reali nu sunt strict necesari pentru îndeplinirea sarcinii.

3.3. Să se prevină accesul neautorizat sau utilizarea abuzivă a datelor prin aplicarea controalelor de transformare înainte de transferul sau prelucrarea datelor.

3.4. Să se asigure că toate procesele de mascare și pseudonimizare sunt trasabile, verificabile și aplicate prin instrumente aprobate.

3.5. Să se respecte standardele legale și de reglementare aplicabile care impun reducerea la minimum a datelor, confidențialitatea și măsurile de protecție prin transformare.

4. Roluri și responsabilități

4.1. Director general

4.1.1. Deține și aprobă prezenta politică

4.1.2. Se asigură că toate departamentele și toți furnizorii respectă cerințele privind transformarea datelor

4.1.3. Revizuiește excepțiile, evaluările de risc și jurnalele privind transformarea datelor

4.1.4. Coordonează acțiunile juridice, operaționale sau legate de furnizori în caz de încălcări

4.2. Furnizorul de suport IT / IT intern

4.2.1. Selectează și administrează instrumentele de mascare sau pseudonimizare

4.2.2. Se asigură că sunt aplicate metodele de transformare adecvate în funcție de tipul de date

4.2.3. Menține jurnale ale seturilor de date transformate și ale procedurilor de gestionare a cheilor

4.2.4. Se asigură că mascarea este efectuată înainte de utilizarea datelor în testare, de către furnizori sau în analize

[... 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

9.1.1. Prezenta politică trebuie revizuită cel puțin o dată pe an de către Directorul general pentru a se asigura că reflectă:

9.1.1.1. Actualizările reglementărilor aplicabile (de exemplu, GDPR, DORA)

9.1.1.2. Sisteme noi ale organizației sau schimburi de date cu terți

9.1.1.3. Feedbackul rezultat din audituri sau incidente care implică utilizarea datelor nemascate

9.2. Revizuiri intermediare

9.2.1. Revizuirile trebuie efectuate și atunci când:

9.2.1.1. Sunt introduse aplicații sau platforme noi care gestionează date sensibile

9.2.1.2. Un incident major evidențiază lacune în controalele actuale de transformare

9.2.1.3. Modificările nivelurilor de clasificare afectează procedurile de gestionare a datelor

9.3. Controlul versiunilor și managementul schimbărilor

9.3.1. Toate modificările politicii trebuie:

9.3.1.1. Să fie aprobate de Directorul general și documentate într-un registru al schimbărilor

9.3.1.2. Să fie comunicate în mod clar angajaților și furnizorilor de servicii afectați

9.3.1.3. Să fie arhivate în condiții de securitate, cu acces restricționat la versiunile depășite

10. Politici conexe și interdependențe

10.1. Prezenta politică trebuie aplicată împreună cu următoarele politici SME pentru a asigura o protecție consecventă și obligatorie a datelor sensibile:

10.1.1. P13S – Politica de clasificare și etichetare a datelor: Definește nivelurile de clasificare (de exemplu, „Confidențial – Personal”) care stabilesc când trebuie aplicată mascarea sau pseudonimizarea. Această politică impune reguli de transformare pe baza nivelurilor de sensibilitate a datelor.

10.1.2. P14S – Politica de păstrare și eliminare a datelor: Asigură că seturile de date transformate, inclusiv copiile de rezervă care conțin date mascate sau pseudonimizate, sunt păstrate și eliminate în conformitate cu regulile aplicabile, inclusiv ștergerea cheilor de mapare atunci când nu mai sunt necesare.

10.1.3. P17S – Politica de protecție a datelor și confidențialitate: Aliniază practicile de transformare la obligațiile mai ample privind confidențialitatea, inclusiv cerințele GDPR privind reducerea la minimum a datelor și utilizarea pseudonimizării ca măsură de protecție pentru prelucrarea datelor cu caracter personal.

10.1.4. P30S – Politica de răspuns la incidente: Acoperă procedurile de raportare și escaladare în cazul divulgării neautorizate a datelor, inclusiv utilizarea necorespunzătoare sau reversarea datelor mascate ori pseudonimizate.

10.1.5. P2S – Politica privind rolurile și responsabilitățile de guvernanță: Atribuie responsabilitatea generală pentru implementarea politicii, acceptarea riscului și aprobarea excepțiilor, în principal Directorului general.

10.2. Aceste politici formează un cadru integrat de protecție a datelor, asigurând că activitățile de mascare și pseudonimizare sprijină conformitatea cu ISO 27001 și cu cerințe de reglementare multiple.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 6.1.3: Impune tratarea riscurilor de securitate a informațiilor, inclusiv reducerea expunerii prin tehnici de transformare a datelor.

11.1.2. Clauza 8.1: Impune implementarea controalelor necesare pentru atingerea obiectivelor de securitate, inclusiv pseudonimizarea și mascarea.

11.2. ISO/IEC 27002

11.2.1. Controlul 8.11: Oferă îndrumări privind mascarea datelor sensibile în sistemele de testare și dezvoltare.

11.2.2. Controlul 8.12: Oferă strategii pentru prevenirea scurgerilor de date prin practici controlate de transformare și acces.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: Asigură confidențialitatea informațiilor prin obfuscarea datelor.

11.3.2. SC-28: Protejează informațiile în repaus și în utilizare.

11.3.3. PT-2/PT-3: Promovează utilizarea tehnologiilor de consolidare a confidențialității, inclusiv pseudonimizarea, în prelucrarea informațiilor de identificare personală (PII).

11.4. GDPR al UE

11.4.1. Articolul 4(5): Definește din punct de vedere legal pseudonimizarea și impune controale asupra cheilor de mapare și a identificatorilor.

11.4.2. Articolul 5(1)(c): Susține principiile de reducere la minimum a datelor prin mascare.

11.4.3. Articolul 32: Recunoaște pseudonimizarea ca un control tehnic care reduce riscurile privind confidențialitatea.

11.5. Directiva NIS2 a UE

11.5.1. Articolul 21(2)(c): Impune măsuri tehnice proporționale pentru reducerea la minimum a riscului de securitate a datelor, inclusiv pseudonimizarea ca parte a controlului riscului.

11.6. Regulamentul DORA al UE

11.6.1. Articolul 10(1): Impune controale privind riscurile legate de TIC, care includ măsuri de protecție prin transformarea datelor pentru continuitate și confidențialitate în timpul externalizării și dezvoltării sistemelor.

11.7. COBIT 2019

11.7.1. DSS05.01: Impune protecția activelor informaționale, inclusiv transformarea, acolo unde este posibil.

11.7.2. DSS06.06: Impune tehnici adecvate de obfuscare și pseudonimizare pentru limitarea expunerii datelor în medii cu nivel de încredere redus.