



FONDUL SOCIAL EUROPEAN PLUS (FSE+)

Programul Educație și Ocupare (PEO) 2021-2027

Prioritate: P9.Consolidarea participării populației în procesul de învățare pe tot parcursul vieții pentru facilitarea tranzițiilor și a mobilității

Obiectiv specific: ESO4.7_Promovarea învățării pe tot parcursul vieții, în special a oportunităților flexibile de actualizare a competențelor și de recalificare pentru toți, ținând seama de competențele antreprenoriale și digitale, printr-o mai bună anticipare a schimbării și a cerințelor de noi competențe bazate pe nevoile pieței muncii, precum și prin facilitarea tranzițiilor profesionale și promovarea mobilității profesionale

Titlu Apel: Competențe digitale pentru piața muncii - Regiuni mai puțin dezvoltate

Titlu proiect: TransformDigital

Cod Apel: PEO/375/PEO_P9/OP4/ESO4.7/PEO_A34

Cod proiect: 336830

Protecția datelor personale la locul de muncă - ce trebuie să știe orice angajat

În activitatea profesională de zi cu zi, utilizarea și gestionarea informațiilor au devenit parte integrantă din aproape orice domeniu de activitate. Fie că este vorba despre datele colegilor, ale clienților, ale partenerilor de afaceri sau chiar despre propriile date personale, fiecare angajat intră în contact cu informații care trebuie gestionate responsabil. În contextul transformării digitale, protecția datelor cu caracter personal nu mai reprezintă doar o obligație legală a organizațiilor, ci și o responsabilitate individuală a fiecărui angajat. Pe măsură ce documentele sunt gestionate electronic, comunicarea se desfășoară prin platforme digitale, iar aplicațiile informatice sunt utilizate în activitatea curentă, este important ca fiecare persoană să cunoască regulile de bază privind protejarea datelor personale și utilizarea responsabilă a informațiilor.

Ce sunt datele cu caracter personal?

Datele cu caracter personal reprezintă orice informație care poate conduce la identificarea directă sau indirectă a unei persoane.

Printre cele mai frecvente exemple se numără:

- numele și prenumele;
- adresa de domiciliu;
- numărul de telefon;
- adresa de e-mail;
- codul numeric personal;
- seria și numărul actului de identitate;
- date privind contractul de muncă;
- fotografii sau înregistrări video;
- informații privind salariul, concediile sau evaluările profesionale.



Protejarea acestor informații este importantă atât pentru respectarea drepturilor persoanelor, cât și pentru menținerea unui climat de încredere în cadrul organizației.

De ce este importantă protecția datelor la locul de muncă?

În prezent, majoritatea activităților implică prelucrarea unor volume mari de informații. O simplă eroare, precum transmiterea unui document către destinatarul greșit sau divulgarea accidentală a unor informații confidențiale, poate avea consecințe atât pentru persoanele vizate, cât și pentru organizație.

Respectarea regulilor privind protecția datelor contribuie la:

- protejarea drepturilor și vieții private ale persoanelor;
- creșterea încrederii dintre angajați, clienți și parteneri;
- prevenirea incidentelor de securitate;
- respectarea obligațiilor legale;
- dezvoltarea unei culturi organizaționale bazate pe responsabilitate și profesionalism.

Protecția datelor nu este doar responsabilitatea departamentului IT sau a persoanelor desemnate în acest domeniu, ci implică participarea activă a fiecărui angajat.

Cum poate contribui fiecare angajat?

Respectarea unor reguli simple poate reduce semnificativ riscul producerii unor incidente privind securitatea informațiilor.

Printre cele mai importante măsuri se numără:

- utilizarea unor parole complexe și schimbarea lor periodică;
- blocarea calculatorului atunci când postul de lucru este părăsit;
- verificarea destinatarilor înainte de transmiterea documentelor;
- evitarea distribuirii informațiilor către persoane neautorizate;
- păstrarea documentelor în spații securizate;
- raportarea imediată a incidentelor sau suspiciunilor privind securitatea datelor.

Aceste măsuri contribuie la protejarea informațiilor și la reducerea riscurilor generate de erorile umane.

Digitalizarea și responsabilitatea în utilizarea informațiilor

Transformarea digitală aduce numeroase beneficii organizațiilor, însă implică și o responsabilitate mai mare în gestionarea datelor. Platformele de colaborare, aplicațiile cloud, comunicarea online și utilizarea dispozitivelor mobile permit desfășurarea activităților într-un mod mai eficient, dar presupun și respectarea unor reguli clare privind securitatea informațiilor.



De aceea, dezvoltarea competențelor digitale trebuie să includă și cunoștințe privind utilizarea responsabilă a tehnologiei, identificarea riscurilor și adoptarea unor bune practici în gestionarea datelor cu caracter personal.

Formarea profesională contribuie și la dezvoltarea unei culturi a securității informațiilor

Competențele digitale nu înseamnă doar utilizarea eficientă a calculatorului sau a aplicațiilor informatice. Ele includ și capacitatea de a recunoaște situațiile care pot afecta securitatea informațiilor și de a acționa responsabil în gestionarea datelor personale.

Organizațiile care investesc în formarea continuă a angajaților contribuie la:

- reducerea riscului de incidente privind protecția datelor;
- creșterea gradului de conștientizare privind securitatea informațiilor;
- dezvoltarea unor comportamente responsabile în mediul digital;
- consolidarea încrederii între organizație, angajați și parteneri;
- respectarea standardelor de conformitate și a bunelor practici.

O cultură organizațională bazată pe responsabilitate și prevenție reprezintă una dintre cele mai eficiente modalități de protejare a informațiilor.

Cum contribuie proiectul „TransformDigital” la dezvoltarea competențelor digitale ale angajaților

Proiectul „TransformDigital” - ID 336830 sprijină dezvoltarea competențelor digitale ale angajaților prin programe de formare adaptate cerințelor actuale ale mediului profesional. Pe lângă utilizarea instrumentelor digitale și dezvoltarea abilităților tehnologice, participanții își consolidează cunoștințele privind utilizarea responsabilă a informațiilor, securitatea datelor și bunele practici necesare desfășurării activității într-un mediu digital. Prin aceste activități, proiectul contribuie la dezvoltarea unei culturi organizaționale orientate spre responsabilitate, profesionalism și utilizarea sigură a tehnologiei, sprijinind atât dezvoltarea competențelor individuale, cât și procesul de transformare digitală al organizațiilor.

Concluzie

Într-o economie tot mai digitalizată, protecția datelor personale reprezintă o responsabilitate comună. Fiecare angajat contribuie, prin acțiunile sale zilnice, la menținerea securității informațiilor și la protejarea drepturilor persoanelor cu care interacționează. Dezvoltarea competențelor digitale trebuie să fie însoțită de dezvoltarea unei culturi a responsabilității, în care utilizarea tehnologiei și gestionarea informațiilor se realizează în mod sigur, etic și profesionist.



**Cofinanțat de
Uniunea Europeană**



**#TransformDigital #ProtecțiaDatelor #CompetențeDigitale #SecuritateaInformațiilor
#DezvoltareProfesională**

***Proiect finanțat din Fondul Social European Plus (FSE+) prin Programul Educație și
Ocupare (PEO) 2021-2027 în cadrul apelului "Competențe digitale pentru piața
muncii - Regiuni mai puțin dezvoltate"***



AEGIS NEXTGEN