Cofinanțat de Uniunea Europeană

Programul Incluziune și Demnitate Socială 2021-2027
Prioritate: P03. Protejarea dreptului la demnitate socială
Obiectiv specific: ESO4.1, Acțiunea 3.2 Economie socială în mediul rural (FSE+)
Titlu proiect: Antreprenoriat social rural sustenabil in Regiunea Centru
Cod mySMIS2021:302211
Beneficiar: Asociația Institutul Educațional pentru Politici Sociale Margareta

Digitalizarea întreprinderilor sociale și protecția datelor

1. Digitalizarea întreprinderilor

Digitalizarea a revoluționat modul în care operează întreprinderile sociale. Prin adoptarea tehnologiilor digitale, întreprinderile își pot îmbunătăți eficiența, extinde impactul social și atrage noi surse de finanțare prin promovarea și popularizarea activităților cu caracter social pe care le desfășoară.

Beneficiile digitalizării pentru întreprinderile sociale

- O eficiență crescută. Automatizarea proceselor administrative, cum ar fi gestionarea de proiecte, contabilitatea și relațiile cu donatorii, poate economisi timp și resurse.
- Extinderea impactului. Platformele online și instrumentele digitale permit întreprinderilor sociale să ajungă la un public mai larg, să colecteze fonduri și să mobilizeze voluntari la nivel național sau global.
- Îmbunătățirea comunicării. Utilizarea de instrumente de comunicare digitală, precum e-mail, social media și videoconferințe, facilitează colaborarea cu partenerii, beneficiarii și donatorii.
- Colectarea și analiza datelor. Tehnologiile digitale permit colectarea și analiza datelor privind impactul social, ceea ce ajută la evaluarea eficacității programelor și identificarea oportunităților de îmbunătățire.
- Mobilizarea comunităților. Platformele de voluntariat online pot mobiliza comunitățile locale și internaționale în jurul cauzelor sociale.

Etape de digitalizare pentru întreprinderile sociale

1. Evaluarea nevoilor digitale. Identificarea specificelor activităților și a provocărilor cu care se confruntă întreprinderea socială pentru a determina cele mai potrivite soluții digitale.
2. Implementarea de soluții digitale. Adoptarea de software și instrumente digitale pentru automatizarea de procese, facilitarea și îmbunătățirea comunicării, colectarea datelor, organizarea și analiza de date.
3. Formarea și dezvoltarea competențelor digitale. Investiția în formarea angajaților pentru a le dezvolta abilitățile digitale necesare pentru a utiliza eficient tehnologiile.
4. Securitatea cibernetică. Protejarea datelor sensibile și a informațiilor confidențiale prin implementarea de măsuri de securitate cibernetică.
5. Monitorizarea și evaluarea impactului digital. Măsurarea efectului utilizării tehnologiilor digitale asupra eficienței, impactului social și eficienței financiare a întreprinderii.

Utilitatea digitalizării întreprinderilor sociale

- Utilizarea platformelor online pentru a colecta fonduri de la publicul larg.
- Folosirea de instrumente de marketing digital, precum social media și e-mail marketing, pentru a promova activitățile și a atrage noi susținători.
- Organizarea de activități de voluntariat online.
- Utilizarea de instrumente de analiză de date pentru a monitoriza impactul social și a identifica tendințe.
- Dezvoltarea de aplicații mobile pentru a facilita accesul la servicii și informații.

Digitalizarea întreprinderilor sociale reprezintă o oportunitate de a crește eficiența, de a extinde impactul și de a atrage noi resurse. Prin adoptarea unei abordări digitale întreprinderile sociale își pot maximiza impactul social.

2. Securitatea cibernetică și protecția datelor

Securitatea cibernetică în sectorul social este un aspect crucial. Organizațiile sociale, fie că sunt ONG-uri, fundații sau întreprinderi, gestionează o cantitate semnificativă de date personale ale beneficiarilor, colaboratorilor și voluntarilor. Aceste date sunt extrem de sensibile și necesită o protecție deosebită.

De ce este importantă securitatea cibernetică

- Protecția datelor personale. Legislația privind protecția datelor (ex. GDPR) impune obligația de a proteja datele cu caracter personal. O breșă de securitate poate duce la amenzi substanțiale și la pierderea încrederii beneficiarilor.
- Încrederea beneficiarilor. O încălcare a securității poate afecta încrederea beneficiarilor în organizație, ceea ce poate duce la scăderea numărului de colaboratori și voluntari.
- Activitate fără întreruperi. Un atac cibernetic poate întrerupe activitățile organizației, afectând astfel persoanele vulnerabile pe care le servește.
- Reputația organizației. O breșă de securitate poate afecta grav reputația organizației, ceea ce poate duce la pierderea finanțărilor și a parteneriatelor.

Cele mai comune amenințări cibernetice

- Atacuri prin e-mail sau mesaje text (Phishing) care imită comunicări legitime pentru a obține informații confidențiale.
- Software rău intenționat (Malware) care poate infecta sistemele și fura date.
- Software care criptează datele și cere o răscumpărare (Ransomware) pentru a le debloca.
- Atacuri care vizează supraîncărcarea serverelor (DDoS) pentru a le scoate din funcțiune.
- Inginerie socială. Manipularea oamenilor pentru a divulga informații confidențiale.

Măsuri de securitate cibernetică

- Pentru a preveni tentativele de phishing, verificați întotdeauna dacă domeniul adresei de e-mail al expeditorului este legitim. Nu descărcați atașamente primite de la adrese de e-mail necunoscute și nu răspundeți acestora înainte de a verifica identitatea expeditorului și motivele invocate. Evitați să vizitați/dați click pe adrese/link-uri suspecte primite pe mail, sau click pe butonul "unsubscribe" din mesajele spam/publicitare neașteptate primite de la domenii/adrese/site-uri web pe care nu aveți cont. De asemenea, întotdeauna vizitați paginile web de importanță pentru dvs. deschizând un nou tab în aplicația Edge/Chrome/Firefox/Opera și vizitând

pagina oficială, niciodată direct din mesajele primite (prin click pe un link sau prin copierea și vizitarea acelei adrese).

- Actualizarea programelor software. Menținerea programelor software și sistemelor de operare la zi cu cele mai recente patch-uri de securitate.
- Parole puternice și autentificare în doi factori. Implementarea de parole puternice și autentificarea în doi factori pentru toate conturile.
- Realizarea de copii ale datelor în mod regulat. Realizarea de copii de siguranță ale datelor și stocarea lor în două sau mai multe locuri având grijă ca datele să fie criptate dacă serverele sunt publice. Dacă accesul la date si volumul de date o recomandă, se va utiliza un sistem local de stocare asistată în rețeaua proprie (NAS - network assisted storage).
- Conștientizarea angajaților. Organizarea de traininguri pentru angajați privind cele mai comune amenințări cibernetice și cum să le evite. Angajații nu vor utiliza dispozitivele de serviciu în alte scopuri decât strict în interes de serviciu și conform regulamentului intern. Ideal nu vor folosi aplicațiile software de pe dispozitivele de serviciu în interes personal și nu vor transfera fișiere de pe și către dispozitivele utilizate în scop de serviciu.
- Politici de securitate. Implementarea unor politici de securitate clare și comunicarea acestora către toți angajații.
- Criptarea datelor sensibile atât în timpul transmiterii, cât și în timpul stocării.
- Utilizarea unui firewall pentru a proteja rețeaua organizației.
- Soluții de securitate cibernetică. Investiția într-o soluție de securitate cibernetică care să ofere protecție în timp real poate fi necesară.
- Consultarea unor experți în securitate cibernetică pentru a evalua riscurile și a implementa măsuri de securitate adecvate.

De ce este dificilă implementarea securității cibernetice

- Bugete limitate. Multe organizații sociale au bugete limitate și nu pot aloca resurse suficiente pentru securitatea cibernetică.
- Lipsa de expertiză. Multe organizații nu au personal cu cunoștințe în domeniul securității cibernetice.
- Complexitatea amenințărilor. Peisajul amenințărilor cibernetice este în continuă evoluție, ceea ce face dificilă menținerea unei securități optime.

Securitatea cibernetică nu ar trebui să fie un lux, ci o necesitate pentru orice organizație. Investiția în securitate cibernetică este o investiție în viitorul organizației și necesară pentru protecția datelor clienților pe care îi servește.

3. Legislația privind protecția datelor

Protecția datelor este un domeniu legal care se ocupă de colectarea, stocarea, utilizarea și divulgarea informațiilor personale. Scopul principal este de a proteja dreptul la viața privată al fiecărei persoane.

Legislația privind protecția datelor face referire la:

- Securitatea datelor. Protejează informațiile personale de accesul neautorizat, pierderea sau deteriorarea.
- Transparență. Oferă persoanelor fizice control asupra datelor lor personale.
- Confidențialitate. Datele personale trebuie utilizate în mod corect și legal.

Principalele acte normative în domeniu

În România, legislația privind protecția datelor este aliniată la reglementările europene, în special la Regulamentul General privind Protecția Datelor (GDPR).

Principalele acte normative sunt:

- Regulamentul (UE) 2016/679: GDPR este principalul instrument legal în materie de protecție a datelor cu caracter personal la nivelul Uniunii Europene.
- Legea nr. 190/2018: Această lege transpune GDPR în legislația națională românească și stabilește măsuri suplimentare pentru punerea în aplicare a regulamentului.

Principiile de bază ale protecției datelor

- Legalitate, echitate și transparență. Prelucrarea datelor trebuie să fie legală, echitabilă și transparentă față de persoana vizată.
- Limitarea scopurilor. Datele trebuie colectate pentru scopuri specificate, explicite și legitime și nu pot fi prelucrate ulterior într-un mod incompatibil cu aceste scopuri.

- Minimizarea datelor. Datele colectate trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate.
- Exactitate: Datele trebuie să fie exacte și, dacă este necesar, actualizate.
- Limitarea stocării: Datele nu trebuie păstrate într-o formă care permite identificarea persoanelor vizate mai mult decât este necesar pentru îndeplinirea scopurilor pentru care sunt prelucrate.
- Integritate și confidențialitate: Datele trebuie prelucrate într-un mod care asigură securitatea datelor, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii accidentale sau a deteriorării.
- Responsabilizarea: Operatorul de date este responsabil pentru respectarea GDPR și trebuie să poată demonstra conformitatea cu acesta.

Drepturile persoanelor vizate

Persoanele vizate au următoarele drepturi:

- Dreptul de acces. Dreptul de a obține confirmarea că datele cu caracter personal care îl privesc sunt sau nu sunt prelucrate și, în caz afirmativ, accesul la aceste date și la anumite informații.
- Dreptul la rectificare. Dreptul de a obține, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte.
- Dreptul la ștergerea datelor („dreptul de a fi uitat”). Dreptul de a obține ștergerea datelor cu caracter personal, fără întârzieri nejustificate.
- Dreptul la restricționarea prelucrării. Dreptul de a obține restricționarea prelucrării.
- Dreptul la portabilitatea datelor. Dreptul de a primi datele cu caracter personal într-un format structurat, utilizat în mod obișnuit și care poate fi citit automat și dreptul de a transmite aceste date către alt operator.
- Dreptul de opoziție. Dreptul de a se opune în orice moment, din motive legate de situația sa particulară, prelucrării datelor cu caracter personal.
- Dreptul de a nu face obiectul unei decizii individuale automate. Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv profilarea, care produce efecte juridice care privesc persoana vizată sau o afectează într-o măsură semnificativă similară.

Cine este afectat de legislația privind protecția datelor?

Orice organizație care colectează și prelucrează date cu caracter personal este afectată de această legislație.

Ce se întâmplă în cazul unei încălcări a legislației?

Încălcarea legislației privind protecția datelor poate duce la sancțiuni administrative și penale, precum și la daune materiale.

Importanța cunoașterii legislației privind protecția datelor

Cunoașterea legislației privind protecția datelor este esențială pentru a ne proteja drepturile și pentru a ne asigura că datele noastre personale sunt prelucrate în mod legal și corect.

4. Obligațiile unei companii în ceea ce privește protecția datelor

Regulamentul General privind Protecția Datelor (GDPR) impune companiilor o serie de obligații stricte în ceea ce privește colectarea, stocarea și prelucrarea datelor cu caracter personal. Aceste obligații sunt esențiale pentru a proteja drepturile persoanelor fizice și pentru a asigura un nivel adecvat de securitate a datelor.

Principalele obligații ale unei companii includ:

- Informarea persoanelor vizate. Compania trebuie să informeze în mod clar și transparent persoanele vizate cu privire la scopul colectării datelor, la categoriile de date prelucrate, la destinatarii datelor și la drepturile acestora.
- Obținerea consimțământului. În majoritatea cazurilor, prelucrarea datelor trebuie să se bazeze pe consimțământul liber, specific, informat și neechivoc al persoanei vizate.
- Limitarea scopurilor în care sunt colectate și prelucrate datele. Datele pot fi colectate și prelucrate doar pentru scopuri specificate, explicite și legitime.
- Minimizarea cantității de date colectate și prelucrate. Compania trebuie să colecteze și să prelucreze doar datele strict necesare pentru activitatea sa.
- Datele colectate și prelucrate trebuie să fie exacte și actualizate.
- Limitarea stocării datelor. Datele nu pot fi stocate mai mult decât este necesar pentru îndeplinirea scopurilor pentru care au fost colectate.

- Asigurarea integrității și confidențialității datelor. Compania trebuie să implementeze măsuri tehnice și organizatorice adecvate pentru a proteja datele împotriva prelucrării neautorizate sau ilegale, precum și împotriva pierderii, distrugerii accidentale sau a deteriorării.
- Notificarea în cazul unei încălcări de securitate. În cazul unei încălcări de securitate care ar putea pune în pericol drepturile și libertățile persoanelor vizate, compania trebuie să notifice autoritatea de supraveghere și, dacă este cazul, persoanele vizate.
- Compania trebuie să coopereze cu autoritatea de supraveghere în cadrul oricărei investigații.
- Numirea unui responsabil cu protecția datelor. În anumite cazuri, compania este obligată să numească o persoană responsabilă cu protecția datelor.

Consecințele nerespectării obligațiilor:

Nerespectarea obligațiilor impuse de GDPR poate atrage după sine sancțiuni administrative semnificative, care pot ajunge până la 4% din cifra de afaceri globală anuală a companiei sau 20 de milioane de euro, oricare dintre aceste sume fiind mai mare.

Cum poate o companie să se asigure că respectă GDPR:

- Pentru anumite tipuri de prelucrare, compania trebuie să efectueze o evaluare a impactului asupra protecției datelor.
- Compania trebuie să elaboreze politici și proceduri interne privind protecția datelor și să le comunice angajaților.
- Angajații trebuie să fie instruiți cu privire la obligațiile lor în materie de protecție a datelor.
- Compania trebuie să încheie contracte cu furnizorii care prelucrează date în numele său, asigurându-se că aceștia respectă GDPR.
- Compania trebuie să efectueze periodic audituri pentru a verifica dacă măsurile de protecție a datelor sunt implementate corespunzător.

5. Obligațiile individuale ale angajaților în ceea ce privește protecția datelor

Regulamentul General privind Protecția Datelor (GDPR), o legislație europeană fundamentală, impune nu doar companiilor, ci și angajaților, să

respecte anumite norme în ceea ce privește protecția datelor cu caracter personal. Aceste obligații sunt esențiale pentru a asigura confidențialitatea informațiilor și pentru a preveni incidente de securitate cibernetică.

De ce sunt importante aceste obligații

- Protejarea reputației companiei. Breșele de securitate pot avea consecințe grave asupra imaginii companiei.
- Prevenirea sancțiunilor financiare. Nerespectarea GDPR poate duce la amenzi substanțiale.
- Asigurarea încrederii clienților. O gestionare corectă a datelor contribuie la consolidarea relației cu clienții.

Obligațiile angajaților

1. **Confidențialitatea:**
   - Angajații nu trebuie să dezvăluie informații confidențiale către persoane neautorizate, fie ele colegi, parteneri sau persoane din afara companiei.
   - Parolele trebuie păstrate în siguranță, iar dispozitivele personale nu trebuie utilizate pentru a accesa sau stoca date confidențiale.
2. **Formarea continuă:**
   - Angajații trebuie să participe la toate sesiunile de instruire privind protecția datelor, pentru a fi la curent cu cele mai bune practici și cu evoluțiile legislative.
3. **Utilizarea responsabilă a tehnologiei:**
   - Mesajele electronice trebuie să fie trimise doar către destinatarii autorizați și să conțină informații relevante.
   - Utilizarea internetului la locul de muncă trebuie să fie în scop profesional și să respecte politica de utilizare a internetului a companiei.
   - Angajații trebuie să fie conștienți de riscurile asociate cu utilizarea rețelelor sociale și să evite să posteze informații confidențiale.
4. **Raportarea incidentelor:**

- În cazul în care un angajat identifică o posibilă breșă de securitate sau o pierdere de date, acesta trebuie să informeze imediat superiorul sau departamentul de securitate IT.

Consecințe ale nerespectării obligațiilor privind protecția datelor

- Măsuri disciplinare. Avertismente, suspendări sau chiar concedieri.
- Răspundere civilă. În unele cazuri, angajații pot fi trași la răspundere civilă pentru daunele cauzate companiei.
- Consecințe penale. În cazuri extreme, pot fi aplicate sancțiuni penale.

Protecția datelor este o responsabilitate comună, atât a companiei, cât și a angajaților. Prin respectarea acestor obligații, fiecare angajat contribuie la crearea unui mediu de lucru sigur, la protejarea intereselor companiei, a colaboratorilor și a clienților acesteia.

Pentru orice nelămuriri legate de provocările specifice economiei sociale sau dacă, în urma înscrierii în grupul țintă al proiectului „Antreprenoriat social rural sustenabil în Regiunea Centru," doriți să stabilim o întâlnire individuală pentru a discuta despre oricare dintre tematicile menționate, vă rog să nu ezitați să mă contactați la adresa de e-mail fecid.office@gmail.com. De asemenea, vă invit să participați la unul dintre workshopurile pe care le vom organiza în perioada următoare. Aștept cu interes mesajele dumneavoastră!