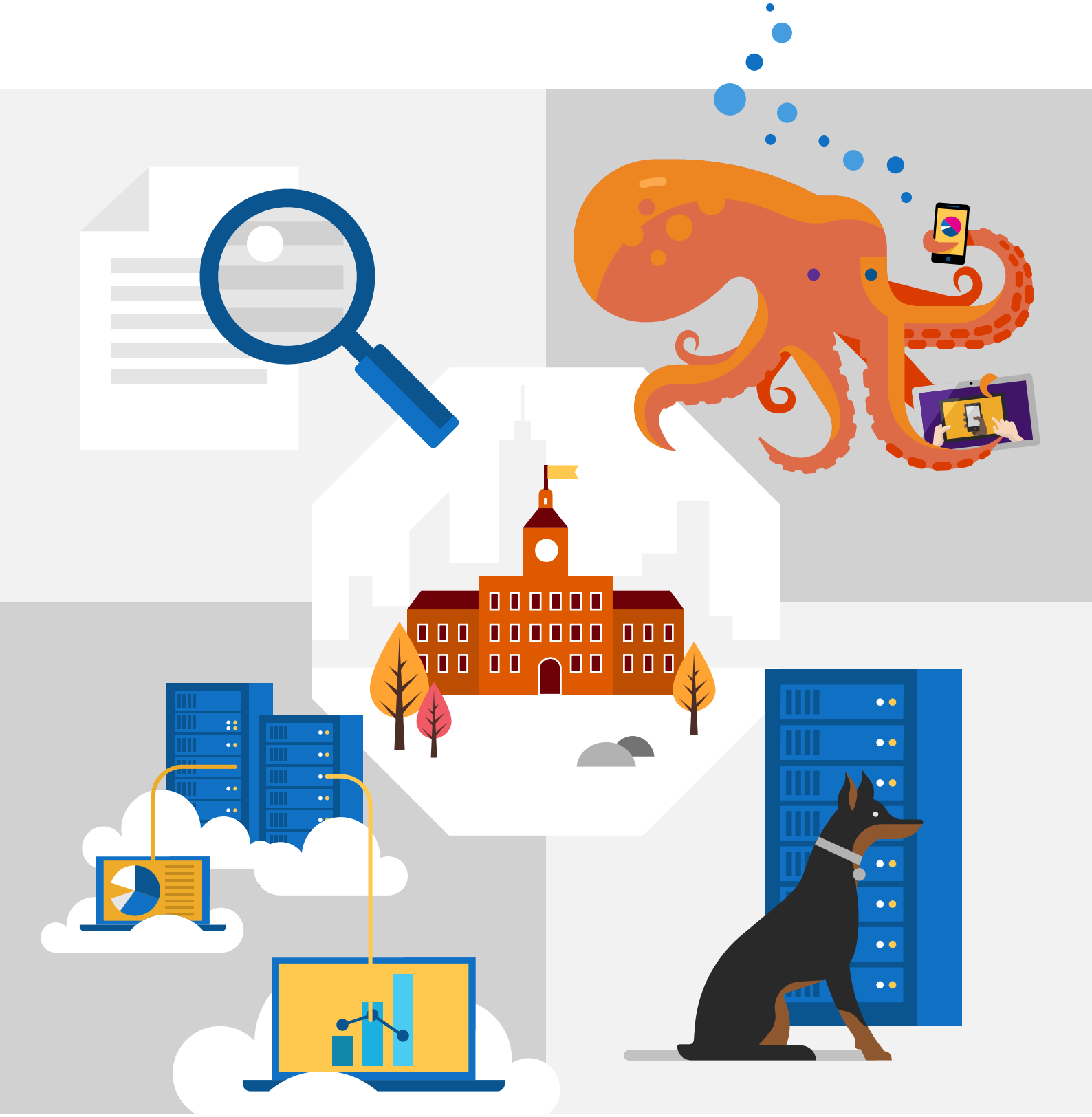


GDPR pentru învățământ

Un ghid de pornire rapidă pentru instituții de învățământ

Microsoft

Despre acest ghid

Acest ghid este conceput pentru a vă ajuta pe drumul către conformarea cu Regulamentul general privind protecția datelor (GDPR), cu exemple concrete și liste cu sarcini de lucru. Nu este complet, dar vă va oferi o idee despre procesele și factorii care trebuie luați în considerare începând cu 25 mai 2018, atunci când GDPR intră în vigoare.

GDPR se aplică instituțiilor care sunt prezente fizic în Uniunea Europeană (EU) și organizațiilor care furnizează bunuri și servicii cetățenilor UE sau care colectează și analizează date referitoare la rezidenții UE. Dacă instituția dumneavoastră se află în afara UE, puteți considera că acest ghid de conformitate GDPR conține cele mai bune practici din acest domeniu.

Învățământul se bazează pe date

La începutul fiecărui an academic, studenții noi generează volume foarte mari de date în școli și universități. Acestea se adaugă la volumele imense de date pe care aceste organizații le gestionează în calitate de proprietari de date.

Aceste date sunt esențiale pentru funcționarea școlilor și universităților. Prin urmare, trebuie implementate procese clare și bine documentate pentru fiecare înregistrare prelucrată.

Mai mult, aceste procese trebuie să se extindă dincolo de timpul petrecut de studenți în cadrul instituției. După ce aceștia părăsesc școala, bazele de date, fișierele și chiar și e-mailurile necesită politici documentate pentru protecție, retenție și prelucrare.

Definirea drumului datelor

Informațiile create și prelucrate în instituțiile academice servesc mai multor scopuri. În primul rând, este vorba despre programă, cunoștințele pe care profesorii le împărtășesc studenților, îmbunătățite de ideile pe care le generează studenții pe măsură ce studiază.

Există, de asemenea, o a doua sursă de date: informațiile pe care organizațiile le colectează cu privire la profesori și studenți, precum și la performanțele școlii. Dacă le adăugăm pe acestea la informațiile colectate prin procesele administrative, de la părinți, infirmierele din școli, guvernatori, consilieri și agenții externe, avem o sursă aparent infinită de date, care circulă în cadrul organizației, o mare parte dintre acestea fiind date cu caracter personal.

Orice administrator cunoaște faptul că acest al doilea set de date este la fel de important pentru o instituție academică precum misiunea educațională de bază. Devine parte din drumul către GDPR pe care studenții, profesorii și părinții îl parcurg pe măsură ce accesează și împărtășesc informații prin intermediul instrumentelor de studiu și serviciilor de comunicare furnizate de școli și universități.

Pentru ce sunt utilizate toate aceste date?

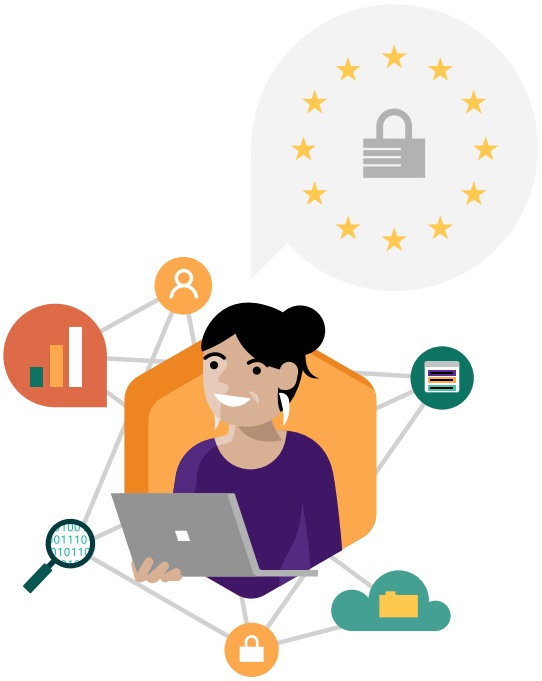
În calitate de proprietari ai datelor, sunteți deja supuși legislației existente, care impune gestionarea și prelucrarea cu grijă a datelor pe care le dețineți și le gestionați. Deși în cadrul GDPR există prevederi suplimentare cu privire la prelucrarea, analiza și partajarea acestor informații cu organismele de reglementare și de stat, pe lângă organizațiile terțe, cum ar fi furnizorii de asigurări, probabil că aveți deja implementate multiple politici privind protecția și confidențialitatea datelor.

Însă sunt acestea suficiente pentru a proteja informațiile personale și sensibile pe care le gestionați?

Introducere în GDPR

Începând cu 25 mai 2018, numeroase organizații, chiar și cele din afara Uniunii Europene (UE), vor răspunde pentru datele deținute în baza unui nou regulament UE, Regulamentul general privind protecția datelor (GDPR).

Regulamentul este conceput pentru a proteja confidențialitatea datelor tuturor cetățenilor UE și pentru a armoniza toate legile privind confidențialitatea datelor din Europa. GDPR va afecta ce date puteți deține, cum le puteți utiliza, unde le stocați și cât de mult timp pot fi stocate.



De ce este GDPR important?

Drumul unei instituții de învățământ se poate reflecta în educația studenților, marcată de momente importante, care sunt înregistrate și evaluate în fiecare etapă. Uneori, datele generate vor rămâne aceleași ani la rând, alteori se vor schimba rapid pe măsură ce studenții și personalul evoluează în cadrul instituției.

GDPR creează un cadrul legal european uniform, oferind persoanelor cu reședința în Europa drepturi asupra acestor date.

Printre modificările cheie care afectează învățământul se numără:

Confidențialitatea personală

Persoanele au dreptul:

- să își acceseze datele cu caracter personal
- să corecteze erorile din datele lor cu caracter personal
- să își șteargă datele cu caracter personal
- să se opună prelucrării datelor lor cu caracter personal
- să își exporte datele cu caracter personal

Măsuri de control și notificări

Va trebui:

- să protejați datele cu caracter personal prin măsuri de securitate adecvate
- să notificați autoritățile despre încăl cări privind datele cu caracter personal
- să documentați modul în care prelucrați datele cu caracter personal
- să țineți evidențe detaliate cu privire la prelucrarea datelor și consimțământul în acest sens*

Politici transparente

Se va aștepta de la dumneavoastră:

- să oferiți notificări clare privind colectarea datelor
- să scoateți în evidență scopurile prelucrării și utilizările
- să stabiliți politici de retenție și ștergere a datelor
- să scoateți în evidență modul în care clienții își pot exercita drepturile în baza GDPR

IT și instruire

Instituțiile de învățământ vor trebui:

- să instruiască personalul și angajații responsabili cu confidențialitatea, de exemplu administratorii de școli sau personalul IT
- să verifice și să actualizeze politicile privind datele referitoare la studenți, personal și contractori
- să angajeze un responsabil de protecția datelor (dacă este necesar)
- să creeze și să gestioneze contracte conforme cu furnizorii, inclusiv cu toți profesorii suplinitori

***GDPR include mijloace de protecție specifice pentru copii. În general, prevede că acordul copiilor trebuie să fie „explicit". GDPR prevede o vârstă legală, în context online, de 16 ani. Însă, Statele Membre UE pot stabili individual orice vârstă legală în intervalul 13-16.**

Cum vă afectează GDPR?

Cum implementați aceste reguli noi, având în vedere că, într-o instituție, datele trebuie accesate de mai multe persoane?

GDPR oferă reguli pentru protejarea și gestionarea acestor date, creând, în același timp, politici și practici corespunzătoare. Este responsabilitatea dumneavoastră să dezvoltați un cadru GDPR care funcționează pentru instituția în care activați.

Drepturi de confidențialitate personală îmbunătățite

GDPR consolidează protecția datelor pentru persoane, inclusiv pentru studenți, în cadrul UE, asigurând următoarele drepturi:

- de a accesa datele și de a corecta inexactitățile
- de a șterge datele
- de a se opune prelucrării informațiilor personale
- de a muta datele

Obligații suplimentare pentru documentarea proceselor și protejarea datelor

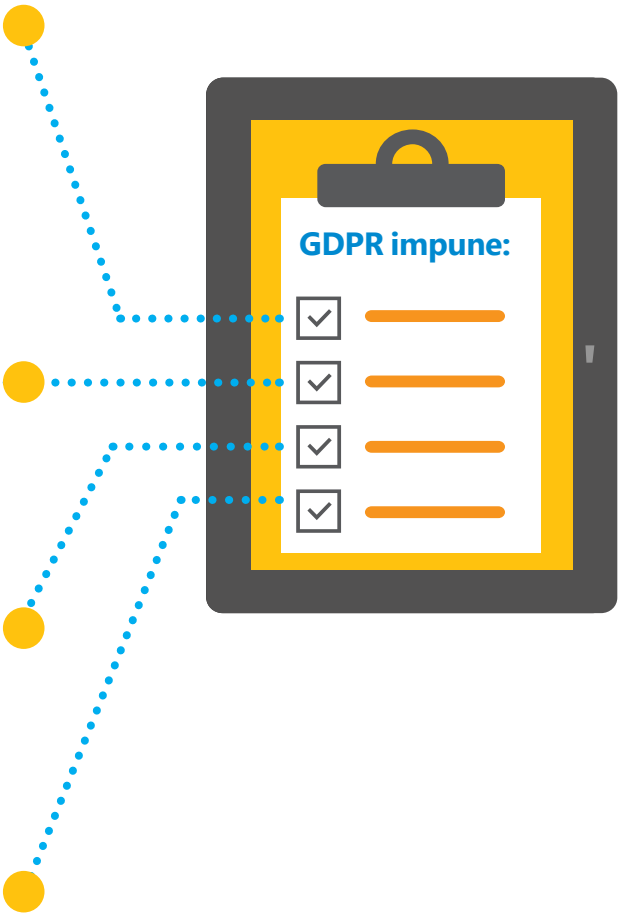
Instituțiile de învățământ care prelucrează datele cu caracter personal vor trebui să prezinte dovezi clare de conformitate.

Raportarea obligatorie a breșelor de securitate

Instituțiile de învățământ sunt obligate să raporteze breșele de securitate în decurs de 72 de ore.

Penalizări semnificative pentru neconformare

Instituțiile de învățământ riscă să primească amenzi dacă nu se conformează regulamentului. Pentru a se conforma, este important să luați în considerare câteva măsuri de protecție a datelor cu caracter personal și să fiți atenți atunci când manipulați aceste date.



Cum să începeți? Harta conformității GDPR

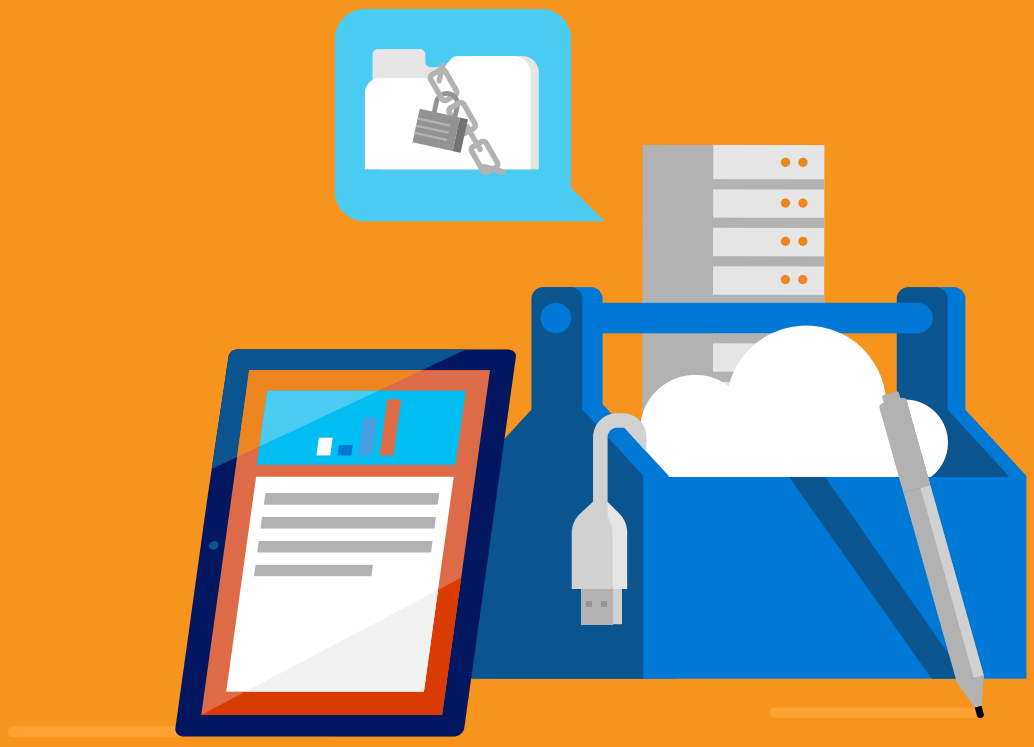
GDPR va avea un impact semnificativ asupra instituției dumneavoastră. Trebuie să actualizați politicile de confidențialitate personală, să implementați sau să consolidați mijloacele de control pentru protecția datelor și procedurile de notificare în cazul breșelor de securitate, să implementați politici foarte transparente și să investiți suplimentar în IT și instruire.

Punând la dispoziție **cel mai extins set de oferte de conformitate** dintre furnizorii de servicii cloud, Microsoft Cloud vă poate ușura drumul către conformitatea GDPR. Veți descoperi că Microsoft Cloud vă oferă cele mai multe resurse pentru îndeplinirea cerințelor GDPR.

Am dezvoltat un proces pentru implementarea GDPR, care se concentrează asupra patru pași cheie:

- **Descoperiți**. Identificați ce date cu caracter personal dețineți și unde sunt localizate
- **Gestionați**. Administrați modul în care sunt utilizate și accesate datele cu caracter personal
- **Protejați**. Implementați controale de securitate pentru a preveni, detecta și răspunde la vulnerabilități și breșe de securitate
- **Raportați**. Mențineți documentele necesare, gestionați solicitările de date și furnizați notificări cu privire la breșe

Instrumentele și resursele Microsoft vă pot ajuta în fiecare etapă a implementării conformității GDPR.



Descoperiți

Gestionați

Raportați

Protejați

Descoperiți

Identificați ce date cu caracter personal dețineți și unde sunt localizate.

Descoperiți ce dețineți

Datele cu caracter personal sunt adesea păstrate în locații multiple, inclusiv în e-mailuri, documente, baze de date, suporturi portabile, metadate, fișiere cu jurnale și copii de rezervă.

Prima sarcină este să identificați unde sunt colectate și stocate datele cu caracter personal.

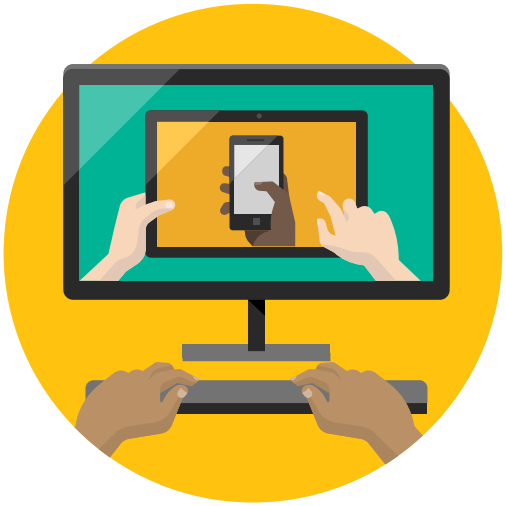
Date existente

Provocare

Pe lângă depozitarea și protejarea datelor existente într-un mod conform cu GDPR, ar trebui să documentați, de asemenea, modul în care prelucrați datele cu caracter personal, de exemplu 1. consimțământ, 2. contract, 3. legalitate, 4. sănătate, 5. comun, 6. cauză legitimă.

Sarcini de lucru

- identificați ce date cu caracter personal sunt colectate și stocate.
- descoperiți locațiile în care sunt stocate datele. Asigurați-vă că includeți furnizorii de servicii cloud și gazdele terțe, cum ar fi site-urile web și centrele de servicii comune. Nu uitați datele analogice, cum ar fi dosarele păstrate în dulapuri.
- organizați și etichetați datele existente în funcție de sensibilitate, utilizare, proprietar, administratori și utilizatori.
- studiați motivele GDPR pentru prelucrare.
- verificați procesul de consimțire și reînnoiți-l, dacă este cazul.



Dispozitive și locații existente

Provocare

Datele cu caracter personal sunt adesea stocate și accesate de pe o gamă largă de dispozitive. Printre aceste dispozitive se numără servere, computere desktop, laptopuri, tablete, dispozitive smartphone, computere personale și medii cloud gestionate și negestionate. Dispozitivele personale și mobile pun îndeosebi probleme la descoperirea datelor.

Sarcini de lucru

- inventariați toate dispozitivele care ar putea conține date cu caracter personal.
- auditați dispozitivele personale și mobile care nu aparțin instituției dumneavoastră.

Cerințele GDPR

GDPR impune ca organizațiile să identifice datele existente și unde sunt acestea păstrate.

După ce inventariați toate datele, inclusiv locațiile, dispozitivele și utilizatorii, pot fi configurate sisteme pentru a colecta date noi pe măsură ce apar.

Utilizatori existenți

Provocare

GDPR impune reguli stricte cu privire la prelucrarea datelor cu caracter personal și la modul în care poate fi realizat acest lucru. Înainte de a împărtăși date cu caracter personal, va trebui să vă asigurați că cei ce au acces la acestea au drepturi în acest sens, atât în interiorul, cât și în exteriorul școlii.

Sarcini de lucru

- identificați și listați toți utilizatorii, inclusiv studenții, personalul și toți contractorii care pot accesa datele.

Subcontractori existenți

Provocare

Datele cu caracter personal trebuie accesate doar de persoane autorizate. Aceasta se aplică atât celor din interiorul organizației, cât și celor din afara organizației. Gândiți-vă la toți contractorii, inclusiv serviciile de catering, serviciile de curățare și asistenții externi, care lucrează cu instituția dumneavoastră.

Aveți responsabilitatea de a vă asigura că persoanele autorizate să acceseze date, denumite procesatori în GDPR, respectă legislația. Aceasta înseamnă că vor stoca date cu caracter personal într-o manieră sigură, le vor utiliza doar în scopul solicitat de dumneavoastră și le vor șterge atunci când nu mai sunt necesare.

Sarcini de lucru

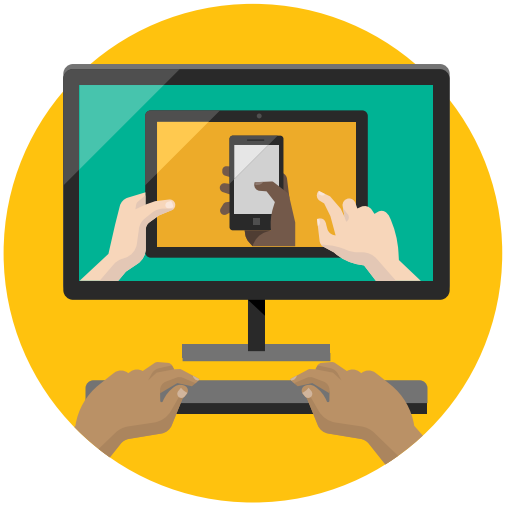
- identificați și listați toți subcontractorii din directorul de utilizatori.
- verificați conformitatea GDPR.
- semnați un contract de conformitate GDPR.
- verificați dacă datele pot fi accesate centralizat la nivel local.

Gestionați

Administrați modul în care sunt utilizate și accesate datele cu caracter personal.

Gestionați datele cu caracter personal

Primul pas în gestionarea datelor cu caracter personal este să definiți de ce trebuie să le colectați. Întrebați-vă cum ajută acest lucru în procesul de educație. Gândiți-vă cum ar trebui colectate, unde vor fi stocate, ce entități vor sprijini procesul, cine ar trebui să le acceseze și cum veți permite modificarea și ștergerea acestora.



Gestionarea datelor noi

Provocare

GDPR permite utilizarea datelor necesare pentru a vă îndeplini misiunea. Dacă misiunea dumneavoastră este definită clar, necesitatea de a procesa datele cu caracter personal asociate va crește.

Atunci când studenții se înregistrează, veți dori să fiți transparenți cu privire la datele cu caracter personal pe care le colectați. Mai exact, va trebui să știți de ce aveți nevoie de aceste date, cât de mult le veți păstra, unde le veți stoca și cum vor fi accesate de dumneavoastră și de ceilalți. Acolo unde este cazul, acordul pentru prelucrarea datelor trebuie solicitat, obținut și stocat, drept dovadă. Studenții sub vârsta legală vor avea nevoie de acordul părinților. Atunci când angajați personal, va trebui să furnizați informații clare cu privire la modul în care datele cu caracter personal sunt prelucrate.

Sarcini de lucru

- definiți-vă clar misiunea.
- listați subiecții datelor.
- stabiliți ce date personale sunt necesare.
- automatizați colectarea de date și fiți responsabili.
- clarificați clauzele GDPR din contracte împreună cu partenerul responsabil cu resursele umane și verificați procesele de consimțire și reînnoire, dacă sunt relevante.

Gestionarea dispozitivelor

Provocare

În mediile educaționale, dispozitivele sunt variate și sunt distribuite în rândul mai multor utilizatori. Puteți vedea computere personale ale profesorilor, dispozitive smartphone și tablete ale studenților, computere din sălile de curs, dispozitive personale, aplicații private, aplicații și locații cloud nemonitorizate, dispozitive ale subcontractorilor, memorii USB și dosare din hârtie depozitate în dulapuri.

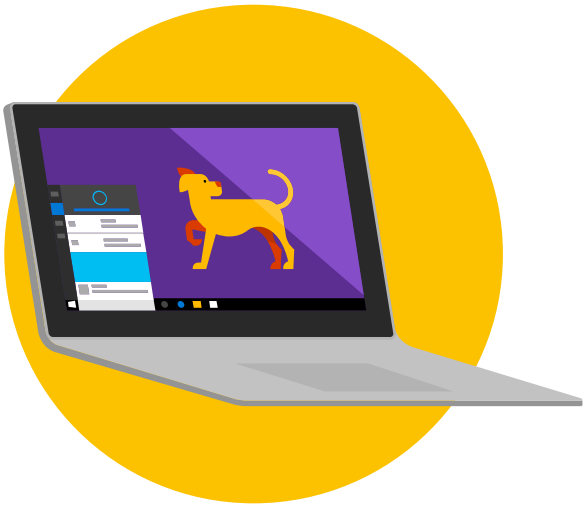
Pentru a respecta regulile stricte ale GDPR cu privire la securizarea datelor cu caracter personal, va trebui să gestionați atât dispozitivele, cât și personalul, studenții și contractorii, într-un mod eficient.

Sarcini de lucru

- dezvoltați politici cu privire la utilizarea dispozitivelor.
- educați personalul și studenții și aduceți-le la cunoștință că există GDPR.
- auditați și înregistrați evenimentele.

Cerințele GDPR

GDPR guvernează modul în care datele cu caracter personal sunt utilizate și accesate.



Gestionarea utilizatorilor

Provocare

Dacă procesul de descoperire vă oferă informații cu privire la baza de date de utilizatori, procesul de gestionare vă ajută să organizați utilizatorii în liste inteligente, permițându-vă să stabiliți permisiuni, politici de conectare securizată și să monitorizați accesul.

Atunci când utilizatorii părăsesc instituția dumneavoastră, accesul acestora la resursele școlii trebuie să fie blocat rapid pentru a evita posibilele scurgeri.

Sarcini de lucru

- organizați utilizatorii în grupuri de securitate.
- definiți permisiuni și politici.
- implementați politici.
- educați studenții, personalul și contractorii cu privire la utilizarea corectă a datelor.

Gestionarea site-ului web

Provocare

Activitățile online reprezintă o parte esențială a promovării destinate atragerii de personal și studenți. Aveți responsabilitatea de a asigura securitatea pe platformele online pe care le utilizați.

Sarcini de lucru

- auditați datele pe care site-ul dumneavoastră web le colectează automat.
- listați modulele cookie proprii și pe cele terțe.
- verificați formularele online pentru a vă asigura că sunt complet sigure.
- verificați procesele de consimțire pentru conformitatea GDPR.
- creați o declarație de confidențialitate care menționează:
  - ce informații sunt colectate
  - cine le colectează
  - cum sunt colectate
  - de ce sunt colectate
  - cum vor fi utilizate
  - cu cine vor fi împărtășite
  - ce efect vor avea asupra persoanelor vizate
  - dacă utilizarea acestora poate determina persoanele să se opună sau să se plângă

Protejați

Implementați controale de securitate pentru a preveni, detecta și răspunde la vulnerabilități și breșe de securitate.

Protejați utilizatorii, datele și dispozitivele

Securitatea este unul dintre elementele esențiale din lumea computerizată.

Cerințele GDPR includ protecția fizică, securitatea rețelelor, securitatea spațiilor de stocare, securitatea computerelor, gestionarea identității, controlul accesului, criptarea și reducerea riscurilor. Căutați o modalitate de a monitoriza sisteme, de a identifica breșe, calculați impactul eventualelor breșe și răspundeți acestora.

Date

Provocare

GDPR nu este o destinație: este un drum continuu. Trebuie să vă asumați în permanență răspunderea, să răspundeți rapid atunci când este necesar și să vă protejați datele cu caracter personal atunci când circulă în cadrul instituției dumneavoastră.

Sarcini de lucru

- criptați datele și e-mailul.
- protejați datele de pe dispozitive (MAM).
- stocați datele în siguranță.
- adăugați drepturi la fișierele și mesajele de e-mail individuale.
- monitorizați intruziunile, infectările cu viruși, furturile și comportamentul anormal.

Dispozitive, locații și aplicații

Provocare

Dispozitivele și aplicațiile au acces la aproape fiecare aspect al datelor dumneavoastră. Pot fi localizate în rețeaua locală (LAN), pe dispozitivele mobile, pe dispozitivele din alte locații, cum ar fi de acasă sau din campus, și pe dispozitivele și aplicațiile din cloud. Fiecare dispozitiv și aplicație necesită o atenție specifică.

Sarcini de lucru

- protejați rețeaua LAN cu antivirus, firewall și cu mijloace fizice de protecție.
- criptați dispozitivele, discurile și unitățile USB.
- educați studenții și personalul cu privire la cele mai bune practici pentru computerele personale.

Cerințele GDPR

GDPR stabilește liniile directoare pentru a implementa controale de securitate pentru a preveni, detecta și răspunde la vulnerabilități și breșe de securitate.

Utilizatori

Provocare

După ce utilizatorii sunt definiți și organizați în grupuri de securitate cu permisiuni și politici stabilite, puteți adăuga măsuri de protecție suplimentare, controlul accesului și gestionarea identității, pentru a atinge conformitatea GDPR.

Sarcini de lucru

- revizuiți politicile privind parolele și opțiunile de autentificare.
- educați și informați.

Testare

Provocare

După ce implementați măsurile tehnice și organizaționale pentru a proteja datele cu caracter personal, va trebui să testați și să evaluați în mod regulat eficiența acestora, pentru a vă asigura că sunt adecvate.

Sarcini de lucru

- facilitați testările regulate.
- evaluați eficiența măsurilor de securitate.

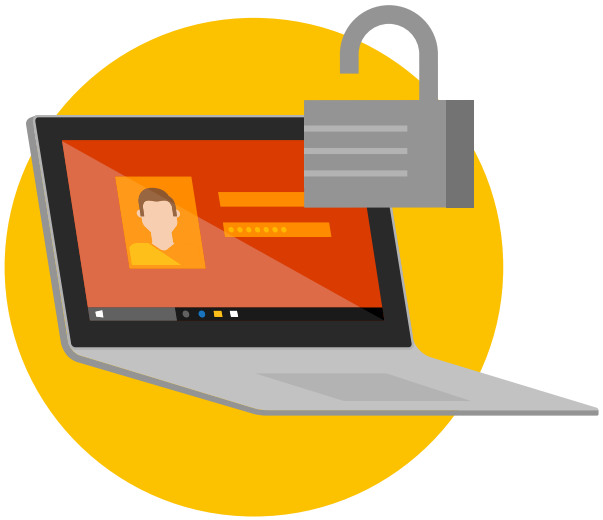
Raportați

Dați curs solicitărilor de date, raportați breșele de securitate și păstrați documentația necesară.

Raportarea în urma auditurilor și breșelor de securitate

Un principiu cheie al GDPR este responsabilitatea. Va trebui să creați căi clare de audit pentru procesare, clasificări și terți cu acces la datele cu caracter personal, inclusiv măsuri de securitate organizaționale și tehnice și perioade de retenție a datelor. Este posibil să trebuiască să efectuați evaluări ale impactului protecției datelor (DPIA).

O DPIA impune organizațiilor să identifice și să analizeze impactul unei activități de procesare propuse cu privire la protecția datelor cu caracter personal.



Căi de audit

Provocare

GDPR vă cere să fiți responsabili pentru protejarea și procesarea adecvată a datelor cu caracter personal. Înregistrările dumneavoastră trebuie să conțină natura fiecărei solicitări efectuate de un subiect, de exemplu, pentru a vizualiza sau rectifica datele cu caracter personal, și rezoluția care a urmat.

Sarcini de lucru

- păstrați înregistrările solicitărilor de date ale subiecților pentru a demonstra conformitatea cu cerințele GDPR.
- monitorizați și înregistrați momentele în care datele cu caracter personal intră și ies din UE.
- monitorizați și înregistrați datele trimise către furnizori de servicii terți, cum ar fi contractorii IT sau furnizorii de servicii de învățământ.
- mențineți căi de audit pentru a demonstra conformitatea GDPR.
- monitorizați și înregistrați fluxurile de date cu caracter personal către furnizorii de servicii terți.
- facilitați DPIA.

Breșe de securitate

Provocare

Organizațiile vor trebui să notifice autoritățile aferente în 72 de ore de la identificarea unei breșe.

Sarcini de lucru

- activați jurnale și rapoarte.
- răspundeți în intervalul de timp cerut.
- mențineți un jurnal separat cu modificările datelor cu caracter personal în caz de dezastre și restaurați copii de rezervă.

Cerințe GDPR

Organizațiile vor trebui să notifice autoritățile aferente în 72 de ore de la identificarea unei breșe.

Concluzie

Încrederea este un element central al misiunii Microsoft de a ajuta toate persoanele și organizațiile de pe planetă să realizeze mai multe. Acest lucru este extrem de important în instituțiile care pregătesc următoarea generație de studenți pentru a-și descoperi și îndeplini scopul în societate.

Compania Microsoft este dedicată principiilor încrederii în cloud – prin **securitate, confidențialitate, transparență** și **conformitate**. GDPR intră în vigoare pe 25 mai 2018, iar portofoliul Microsoft extins de servicii cloud îndeplinește cerințele riguroase de securitate și confidențialitate ale clienților noștri din învățământ, asigurând îndeplinirea obligațiilor noastre în calitate de procesator de date.

Oferta Microsoft de productivitate în cloud, Office 365 A1, este gratuită pentru clienții din învățământ. Aceasta oferă conformitate GDPR și instrumente esențiale de protecție a informațiilor, permițând eDiscovery, administrarea drepturilor, prevenirea pierderii datelor, criptarea, arhivarea avansată a e-mailurilor și capacitățile de protejare a documentelor. Clienții care au nevoie de analiza îmbunătățită a riscurilor, reducerea amenințărilor, criptarea și controlul datelor pot lua în considerare abonamentele plătite **Office 365 A3 sau A5** pentru cerințele GDPR specifice.

Clienții care caută soluții de gestionare a arhivei, guvernării și descoperirii datelor pentru sistemul lor IT pot să valorifice **Microsoft 365 Education**. Acesta oferă o experiență simplă și sigură pentru gestionarea utilizatorilor, datelor și dispozitivelor de la un singur tablou de control, care protejează identitatea, aplicațiile, datele și dispozitivele cu securitate inteligentă îmbunătățită de învățarea automată.

Începeți astăzi folosind **Instrumentul de evaluare** GDPR pentru a revizui nivelul general de pregătire. și, dacă sunteți deja client Microsoft Cloud, utilizați **Managerul de conformitate** pentru a avea o vedere de ansamblu asupra infrastructurii dvs. de protecție și conformitate a datelor pentru Office 365, Dynamics 365 și Azure.

Instrumente și linkuri asociate

Am compilat următoarea listă de instrumente pentru a vă ajuta să parcurgeți drumul către GDPR.

Descoperiți

- **Office 365 Advanced eDiscovery** sau **Căutarea de conținut** vă vor ajuta să căutați informații existente.
- **etichetarea datelor din Office 365** permit clasificarea datelor în cadrul organizației pentru administrare.
- **listele SharePoint** reprezintă un instrument flexibil pentru organizarea și etichetarea datelor.
- **administrarea conturilor de utilizator din Office 365** vă ajută să organizați utilizatorii.
- **Microsoft Intune for Education** vă ajută să enumerați și să gestionați o serie de dispozitive.
- **System Center** este o soluție ideală pentru lista și administra serverele cu diferite sisteme de operare și soluții găzduite în cloud.
- **Azure Search** vă va ajuta să adăugați funcționalități de căutare avansate în mediul dumneavoastră curent.
- **Catalogul de date Azure** înregistrează, descoperă, înțelege și consumă surse de date.
- **Cloud Discovery** analizează jurnalele dumneavoastră de trafic în comparație cu catalogul Cloud App Security, care conține peste 15.000 de aplicații din cloud care sunt clasificate și punctate în funcție de peste 60 de factori de risc, pentru a vă furniza vizibilitate continuă pentru utilizarea în cloud, sistemele de IT invizibile și pentru a evalua riscurile sistemelor IT invizibile pentru organizația dumneavoastră.
- **Guvernarea avansată a datelor (ADG)** vă ajută să identificați, clasificați și să gestionați automat datele cu caracter personal și datele sensibile și să aplicați politici de retenție și ștergere.

Gestionați

- **utilizați grupuri de securitate** în Office 365 pentru a seta un singur set de permisiuni în toate aplicațiile Office 365.
- **atașamentele inteligente din Outlook** împiedică informațiile să părăsească instituția.
- utilizați **sfaturile pentru e-mail din Office 365** pentru a evita greșelile frecvente.
- **prevenirea pierderilor de date din Office 365** împiedică informațiile să părăsească unitatea.
- crearea de **fluxuri** automate dintre aplicații va optimiza și securiza fluxurile de date.
- **Intune for Education** vă ajută să gestionați politici, aplicații și setări pentru dispozitivele din sălile de curs
- **Azure AD** (Azure Active Directory) este directorul bazat pe cloud și serviciul de gestionare a identității de la Microsoft.
- utilizați **PowerApps** pentru a crea rapid aplicații mobile cu scopul de a alimenta direct bazele de date.
- aplicați **etichete** datelor cu caracter personal și gestionați **guvernarea datelor** în Office 365.
- **Azure Information Protection:** controlați și securizați e-mailul, documentele și datele sensibile pe care le partajați în afara companiei.
- încorporarea **Microsoft Forms** (Office 365) poate securiza introducerea datelor prin intermediul formularelor online și permit consimțirea solicitărilor conforme cu GDPR.
- **Office 365 Teams** permite instituțiilor să centralizeze și să coordoneze toate comunicațiile necesare pentru politicile GDPR.

Raportați

- **Centrul de autorizare Microsoft** este sursa ideală de informații despre GDPR și conformitate.
- **Manager de conformitate** Microsoft vă ajută să executați evaluări ale riscurilor și simplifică procesul de conformitate oferind acțiuni recomandate, colectare de dovezi și pregătire pentru audit.
- **auditarea și înregistrarea din Azure** vă oferă înregistrări electronice ale activităților suspicioase și vă ajută să detectați modele care pot indica încercările de penetrare sau penetrările externe reușite ale rețelei, precum și atacurile interne.
- **Securescore.office.com** este un instrument de analiză de securitate care vă va ajuta să înțelegeți ce ați făcut, pentru a reduce riscurile pentru date în Office 365 și pentru a vă arăta ce puteți face pentru a reduce și mai mult respectivele riscuri. Este o sursă ideală de cunoștințe despre auditare, înregistrare și despre multe alte caracteristici de securitate din Office 365.
- **jurnalul de audit unificat** furnizează perspective asupra datelor transferate către terți.

Protejați

- **prevenirea pierderilor de date din Office 365 (A3)** permite crearea de reguli care împiedică tipurile dorite de informații să părăsească unitatea.
- **Azure Information Protection:** Controlați și securizați e-mailul, documentele și datele sensibile pe care le partajați în afara companiei. Clasificare ușoară și etichete și permisiuni încorporate, care vă permit să îmbunătățiți întotdeauna protecția datelor cu ajutorul Azure Information Protection, indiferent unde sunt acestea stocate sau cu cine sunt partajate.
- **Customer Lockbox** poate permite controlorilor să demonstreze că există proceduri explicite implementate pentru accesul la conținutul clienților în timpul operațiilor de service.
- **AppLocker** ajută administratorii să creeze și să implementeze politici de control al aplicațiilor, restricționând accesul utilizatorilor neautorizați la aplicații care ar putea supune datele cu caracter personal unor riscuri.
- **Microsoft Advanced Threat Analytics** (ATA) este o platformă locală care vă permite să protejați instituția de mai multe tipuri de atacuri cibernetice specifice avansate și de amenințări interne.
- **Office 365 Threat Intelligence.**
- **Intune for Education** este o soluție simplă dar puternică pentru implementarea politicilor, aplicațiilor și setărilor de securitate pentru dispozitivele din sălile de curs.
- **Windows Defender Advanced Threat Protection,** disponibil în Windows 10 Education, este un serviciu de securitate care permite clienților să detecteze, să investigheze și să răspundă la amenințări avansate din rețelele acestora.
- **Azure Backup** și **Azure Disaster Recovery** îmbunătățesc disponibilitatea.
- **Criptare unitate BitLocker** este o caracteristică de protejare a datelor care se integrează în sistemul de operare și contracarează amenințările cu furtul de date sau expunerea datelor cauzată de pierderea, furtul sau scoaterea necorespunzătoare din uz a computerelor.
- utilizați **autentificarea multi-factor** din Office 365 și Windows 10 cu Windows Hello.

Notă: aceasta nu este o listă completă de instrumente și servicii Microsoft disponibile pentru a sprijini cei patru pași cheie. Pentru o prezentare detaliată a modului în care toate serviciile și produsele Microsoft Cloud pot ajuta clienții să își îndeplinească obligațiile GDPR, descărcați documentul electronic **Accelerați conformitatea GDPR cu Microsoft Cloud**

Acest document electronic este un comentariu cu privire la GDPR, așa cum îl interpretează Microsoft, la data publicării. Am petrecut mult timp analizând GDPR și credem că i-am gândit bine intențiile și înțelesul. Însă aplicarea GDPR se face în mare măsură în funcție de situație și nu toate aspectele și interpretările GDPR sunt clar definite.

Drept urmare, acest document electronic este furnizat în scop informativ și nu trebuie să se considere că oferă consiliere juridică sau că determină modul în care GDPR ți se poate aplica ție sau organizației tale. Vă încurajăm să colaborați cu specialiști calificați pentru a discuta despre GDPR, despre modul în care se aplică organizației dumneavoastră și despre cele mai bune moduri de asigurare a conformității.

MICROSOFT NU OFERĂ NICIO GARANȚIE EXPRESĂ, IMPLICITĂ SAU PREVĂZUTĂ DE LEGE CU PRIVIRE LA INFORMAȚIILE DIN ACEST DOCUMENT ELECTRONIC. Acest document electronic este furnizat „ca atare”. Informațiile și opiniile exprimate în acest document electronic, inclusiv adresele URL și alte referințe la site-uri web de pe internet, se pot modifica fără notificare prealabilă.

Acest document nu vă oferă niciun drept legal de proprietate intelectuală asupra niciunui produs Microsoft. Puteți copia și utiliza acest document electronic doar în scopuri de referință internă.

Publicat în martie 2018 versiunea 1.0