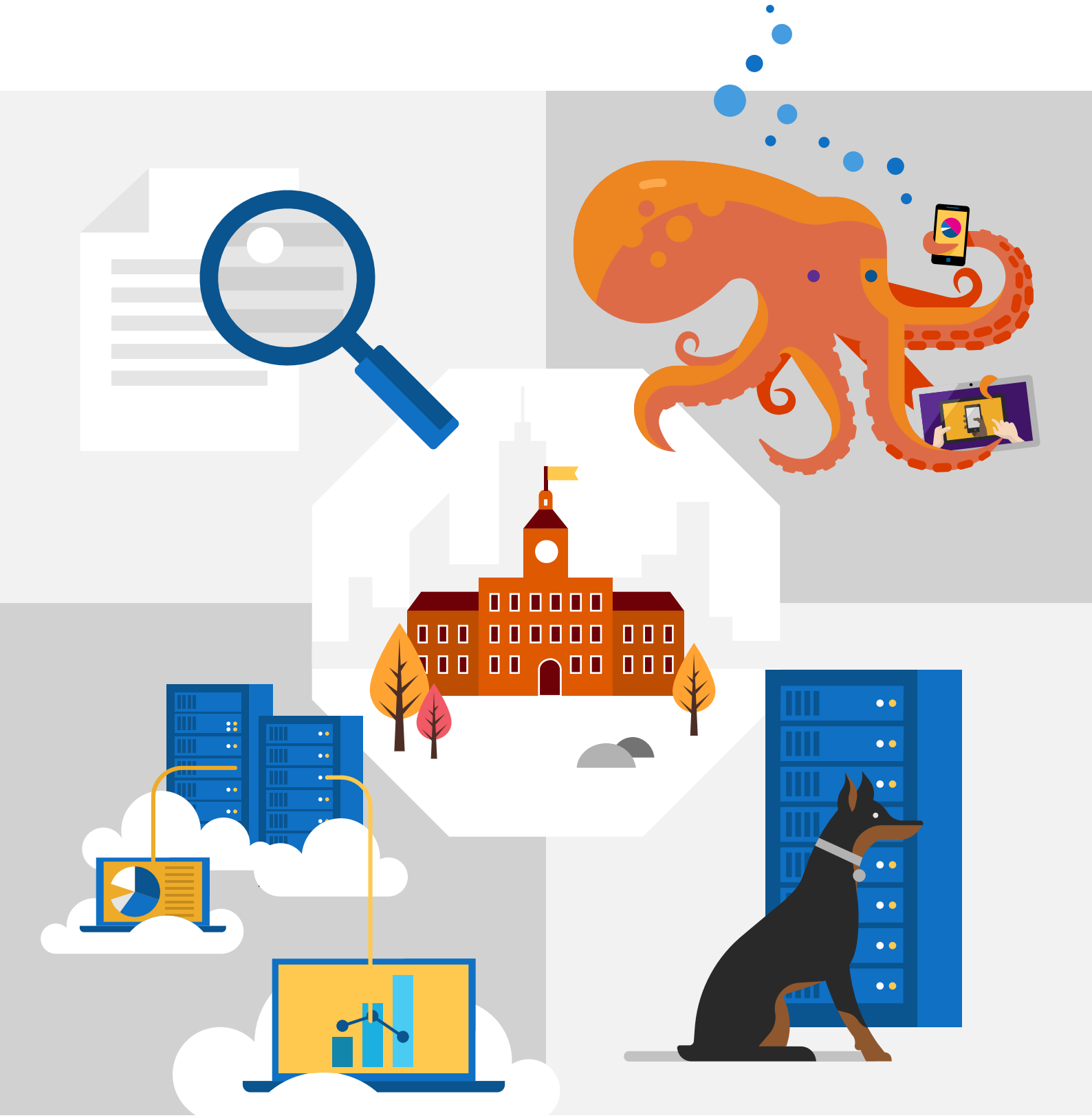


Il GDPR nel settore dell'istruzione

Guida rapida per le istituzioni educazionali

Microsoft

Finalità di questa guida

La presente guida intende accompagnarti nel viaggio verso la meta della conformità al GDPR - il Regolamento generale sulla protezione dei dati - con esempi concreti e utili promemoria delle misure da prendere. Sebbene non tratti di tutti gli aspetti della nuova normativa, ti darà una buona indicazione dei processi e dei fattori da considerare dopo il 25 maggio 2018 - data in cui il GDPR avrà piena efficacia.

Il GDPR si applica alle istituzioni che hanno una presenza fisica nell'Unione europea (Ue), e inoltre alle organizzazioni che forniscono prodotti e servizi ai cittadini dell'Ue, o che raccolgono e analizzano i dati correlati a soggetti residenti nell'Ue. Se la tua istituzione ha sede al di fuori dell'Ue, considera questa guida per la conformità al GDPR come un approccio incentrato sulle procedure più valide.

Il mondo dell'istruzione è legato indissolubilmente ai dati

All'inizio di ogni nuovo anno scolastico o accademico, i nuovi studenti generano un volume ingente di dati presso scuole, istituti superiori e università. Questi dati vanno ad aggiungersi alla grande mole di informazioni già detenute da queste istituzioni educazionali, nella loro veste di titolari del trattamento dei dati.

Tuttavia, queste informazioni sono fondamentali per l'operatività di scuole e atenei. Di conseguenza, è necessario formulare e attuare processi chiari e ben documentati per ciascun dato oggetto di trattamento.

Tali processi, inoltre, non devono abbracciare unicamente il periodo di iscrizione degli studenti presso il tuo istituto. Anche in fase successiva, infatti, i database, i file e persino i flussi di comunicazioni e-mail richiederanno prassi documentate ai fini della protezione, della conservazione e del trattamento dei dati.

Il percorso dei dati

Le informazioni generate e trattate presso le istituzioni accademiche adempiono a molteplici finalità.
Innanzitutto il curriculum, le conoscenze che gli educatori condividono con gli studenti, integrato dalle idee e le proposte di questi ultimi mentre sviluppano gradualmente il loro apprendimento.
Esiste poi un secondo insieme di dati: le informazioni raccolte dalle organizzazioni riguardo a insegnanti e studenti, nonché all'andamento e ai risultati delle istituzioni didattiche. Non per ultimo, vi sono le informazioni scaturite dagli iter di natura amministrativa - da genitori, infermieri e dirigenti scolastici, consulenti e agenzie esterne. Insomma, come puoi ben capire, attraverso la tua organizzazione passa un flusso verosimilmente infinito di informazioni, che nella maggior parte dei casi rappresentano dati personali.

Come ogni amministratore ben sa, per qualunque istituzione accademica questo secondo insieme di dati è importante quanto la missione educativa fondamentale. Diventa parte integrante del viaggio alla meta del GDPR, che studenti, corpo insegnanti, docenti e genitori intraprendono allorché accedono e condividono informazioni mediante gli strumenti didattici e i servizi di comunicazione forniti da scuole e università.

Cosa fai di tutti questi dati?

In qualità di titolare del trattamento sei già tenuto, ai sensi delle normative in vigore, ad assicurare una gestione e un trattamento attenti dei dati che possiedi e amministri. Sebbene il GDPR introduca nuove disposizioni che disciplinano come, perché e con chi occorra condividere, trattare e analizzare parte di tali dati - ad esempio enti statali e di regolamentazione, e altri terzi quali gli assicuratori - probabilmente avrai già istituito numerose procedure per la protezione dei dati e la privacy.

Ma questi criteri sono adeguati per tutelare le informazioni personali e sensibili che gestisci?

Il nuovo regolamento GDPR

Dal 25 maggio 2018 molte organizzazioni, persino quelle non aventi sede nell'Unione europea (Ue), saranno responsabili per la totalità dei loro dati, dopo l'attivazione della nuova normativa Ue chiamata Regolamento generale sulla protezione dei dati (GDPR).
Questo regolamento intende proteggere la privacy di tutti i dati dei cittadini dell'Ue e, inoltre, armonizzare i vari ordinamenti legali che vigono in ambito europeo per la privacy dei dati.

Il GDPR enuncia principi specifici riguardo alla natura dei dati che detieni, alle modalità con cui ne esegui il trattamento, alla sede dove li conservi e al periodo massimo consentito per la loro conservazione.

Perché il GDPR è importante?

Il viaggio delle istituzioni educazionali verso la conformità può riflettere l'iter di apprendimento degli studenti, con tappe fondamentali registrate formalmente e valutate a ogni stadio. Talvolta i dati non subiranno variazioni per anni e anni, mentre in altri casi andranno soggetti a rapide modifiche, con gli spostamenti e i trasferimenti di studenti e personale nella tua istituzione.Il GDPR istituisce un contesto legale congruo in tutta Europa, conferendo ai soggetti residenti in ambito europeo taluni diritti sui dati che li riguardano.

Le modifiche salienti per il settore dell'istruzione comprendono quanto segue:

Privacy personale

Gli individui hanno il diritto di:

- Accedere ai propri dati personali
- Correggere errori nei propri dati personali
- Cancellare i propri dati personali
- Contestare l'elaborazione dei propri dati personali
- Esportare i propri dati personali

Controlli e notifiche

Sarai tenuto a:

- Proteggere i dati personali con misure di sicurezza appropriate
- Segnalare alle autorità le violazioni dei dati personali
- Documentare le tue modalità del trattamento dei dati personali
- Conservare la documentazione dettagliata sul trattamento dei dati e sul relativo consenso*

Criteri di trasparenza

Ti sarà chiesto di:

- Fornire chiare notifiche in merito alla raccolta dei dati
- Delineare le finalità del trattamento e i casi di utilizzo
- Definire i criteri per la conservazione e l'eliminazione dei dati
- Descrivere in termini generali come i clienti possono esercitare i diritti che il GDPR riconosce loro

IT e formazione

Le istituzioni educazionali saranno tenute a:

- Formare il personale e i dipendenti che si occupano di privacy, come i dirigenti scolastici o lo staff di IT
- Controllare e aggiornare i propri criteri relativamente a studenti, organico e appaltatori
- Avvalersi di un Responsabile della protezione dei dati (se richiesto)
- Creare e amministrare contratti conformi, con tutti i fornitori e gli insegnanti supplenti

***Il GDPR prevede misure di protezione specifiche per i minori. In generale, dispone che il consenso dei minori debba essere "esplicito". Ai sensi del GDPR, l'età minima per il consenso on-line è 16 anni. Tuttavia, gli stati membri dell'Ue avranno la facoltà di variare l'età del consenso, tra 13 e 16 anni.**

Quali sono gli effetti del GDPR per te?

Come potrai assicurare il rispetto delle nuove regole, visto che ogni giorno svariate persone devono poter accedere ai dati nell'ambito della tua organizzazione?

Il GDPR fornisce le necessarie per amministrare e proteggere tali dati, formulando allo stesso tempo criteri e procedure uniformi. Spetta a te generare un assetto imperniato sul GDPR che faccia fronte alle esigenze della tua istituzione.

Diritti di privacy potenziati

Il GDPR accentua la tutela dei dati individuali, compresi gli studenti, all'interno dell'Ue. Lo fa garantendo loro il diritto di:

- Accedere ai propri dati e rettificarne le inesattezze
- Cancellare i propri dati
- Contestare l'elaborazione delle proprie informazioni
- Trasferire i propri dati

IPiù responsabilità per la documentazione dei processi e la protezione dei dati

Le istituzioni educazionali che trattano dati personali dovranno comprovare in modo chiaro la loro conformità.

Obbligo di notifica delle violazioni dei dati

Le istituzioni educazionali sono tenute a notificare le violazioni dei dati entro 72 ore.

Ingenti sanzioni per l'inadempienza

Le istituzioni educazionali rischiano potenziali sanzioni finanziarie, in caso di mancata risposta. A garanzia dell'ottemperanza, è importante considerare molteplici misure a protezione dei dati personali e procedere con la dovuta cautela al loro trattamento.

Da dove iniziare? Una mappa per la conformità al GDPR

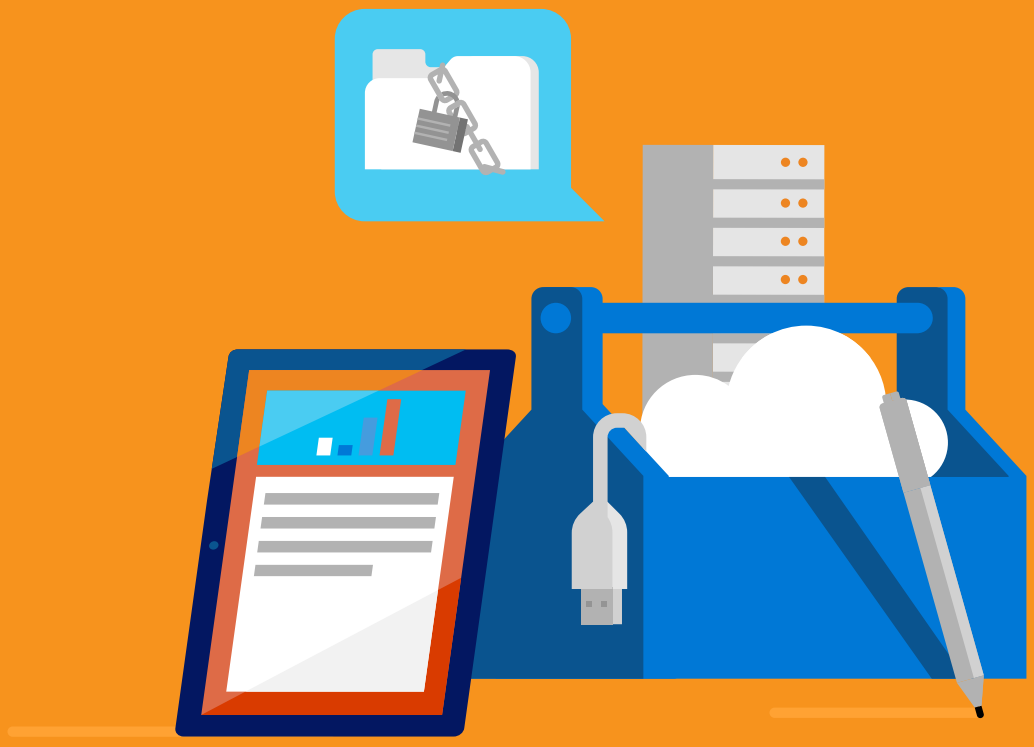
Il GDPR avrà conseguenze di rilievo per la tua istituzione. Richiede infatti l'aggiornamento delle procedure in materia di privacy individuale, l'attuazione o il consolidamento delle misure di controllo per la protezione dei dati, nonché la notifica in caso di violazione dei dati, l'applicazione di policy altamente trasparenti e ulteriori investimenti in IT e formazione.

Grazie alla gamma più completa di soluzioni per la conformità offerta da qualsiasi provider di servizi cloud, Microsoft Cloud può facilitarti nel raggiungimento della meta della conformità GDPR. Scoprirai infatti che Microsoft Cloud offre il massimo numero di risorse in assoluto per adempiere alle disposizioni del nuovo Regolamento.

Abbiamo sviluppato un iter specifico per l'attuazione dei requisiti GDPR, incentrato su quattro stadi chiave:

- **Scoprire.** Identifica i dati personali che detieni e la loro ubicazione
- **Gestire.** Controlla le modalità di utilizzo e di accesso ai dati
- **Proteggere.** Stabilisci controlli di sicurezza per prevenire, rilevare e reagire in caso di vulnerabilità e violazioni dei dati
- **Notificare.** Conserva la necessaria documentazione e gestisci le richieste dei dati e le notifiche delle violazioni

Gli strumenti e le risorse Microsoft possono aiutarti a tutti questi stadi, mentre implementerai la tua conformità al GDPR.



Scoprire

Gestire

Notificare

Proteggere

Scoprire

Identifica i dati personali che detieni e la loro ubicazione.

Scopri quali dati detieni

Spesso i dati personali vengono conservati presso sedi multiple, ad esempio all'interno di comunicazioni e-mail, documenti, database, media removibili, metadati, file di registro e file di backup.

Pertanto, come prima cosa devi identificare dove vengono raccolti e conservati i dati personali.

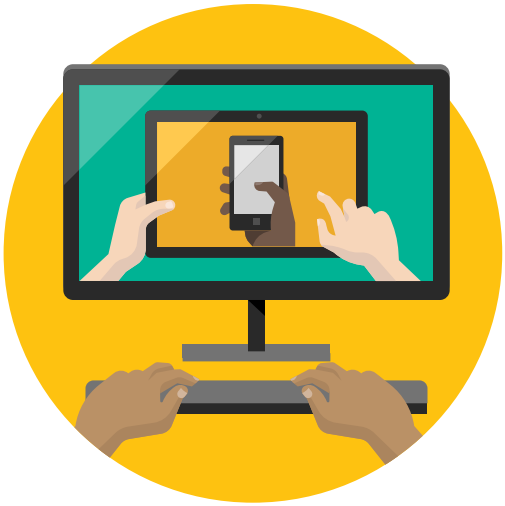
Dati attuali

La sfida

In aggiunta alla conservazione e alla protezione dei dati in essere nel rispetto delle disposizioni del GDPR, sarà tua responsabilità documentare le modalità di trattamento per i dati personali, ad es. 1. consenso, 2. contratto, 3. obbligo legale, 4. interessi vitali, 5. interesse pubblico, 6. legittimo interesse.

Cose da fare

- Individua quali dati personali correnti vengano raccolti e conservati.
- Scopri le sedi in cui vengono conservate le informazioni. Assicurati di includere i fornitori di servizi cloud e hosting di terzi, come siti web e centri di servizi condivisi. Non dimenticare neppure i dati analogici, come i documenti cartacei archiviati fisicamente.
- Organizza e classifica i dati attuali in base a: natura sensibile, utilizzo, titolarità, amministratori e utenti.
- Documenta i principi GDPR per il trattamento.
- Verifica l'iter di consenso e rinnovalo, se pertinente.



Dispositivi e sedi attuali

La sfida

La conservazione e l'accesso ai dati personali avvengono di frequente su tutta una serie di dispositivi. Tra le apparecchiature usate possono esservi server, computer desktop e laptop, tablet, smartphone, computer provati e ambienti cloud gestiti e non gestiti. I dispositivi personali e mobili rappresentano una sfida particolarmente sentita per la protezione dei dati.

Cose da fare

- Esegui un inventario di tutti i dispositivi che potrebbero contenere dati personali e preparane un elenco.
- Procedi a una revisione dei dispositivi personali e mobili non di proprietà della tua organizzazione.

I requisiti del GDPR

Il GDPR dispone che le organizzazioni identifichino i dati in essere, nonché la loro ubicazione.

Quando avrai creato un inventario di tutti i dati - comprendente sedi, dispositivi e utenti - sarà possibile impostare i sistemi per la racconta immediata di tutte le nuove informazioni.

Utenti attuali

La sfida

Il GDPR impone norme rigorose riguardo alle persone autorizzate a trattare i dati, alle tipologie di dati personali trattabili e, inoltre, a come e quando tale trattamento possa avvenire. Prima di condividere i dati personali, dovrai verificare che chiunque possa accedervi sia autorizzato a visionarli, sia all'interno sia all'esterno della tua istituzione

Cose da fare

- Identifica tutti gli utenti, inclusi studenti, staff e appaltatori, con potenziale accesso ai dati.

Subappaltatori attuali

La sfida

La divulgazione o l'accesso ai dati personali deve avvenire solo da parte di soggetti debitamente autorizzati. Ciò vale sia internamente sia esternamente all'organizzazione. Pensa dunque a tutti gli appaltatori che lavorano con la tua istituzione, come servizi di ristorazione, imprese di pulizia e assistenti esterni.

È tua responsabilità assicurare che le persone autorizzate ad accedere ai dati - i responsabili del trattamento secondo la terminologia enunciata nel GDPR - si attengano alla legislazione. In altre parole, essi dovranno conservare i dati personali in sicurezza, usarli unicamente per le finalità prestabilite ed eliminarli quando diventano superflui.

Cose da fare

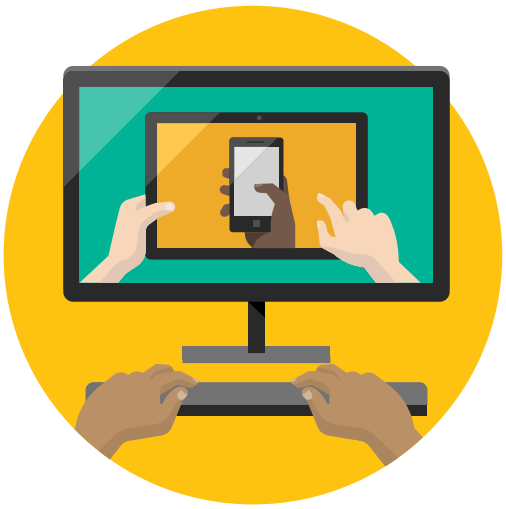
- Identifica e includi tutti i subappaltatori nell'elenco degli utenti.
- Verifica la conformità nei riguardi del GDPR.
- Sottoscrivi un contratto di conformità per il GDPR.
- Mentre ti trovi ancora sul posto, verifica se sia possibile accedere centralmente ai dati.

Gestire

Controlla le modalità di utilizzo
e di accesso ai dati.

Gestione dei dati personali

Per gestire i dati personali, dovrai per prima cosa definire i motivi per cui è necessario procedere alla loro raccolta. Domandati come ciò contribuisca a impartire l'insegnamento. Considera come tali dati andrebbero raccolti, dove verranno conservati, quali persone giuridiche supporteranno questo processo, chi dovrebbe accedere alle informazioni e in che modo consentirai la loro modifica ed eliminazione.



Gestione dei nuovi dati

La sfida

Il GDPR autorizza l'uso dei dati necessari per concretizzare la tua missione. Se questa missione è definita il modo chiaro, la tua esigenza di trattare i dati personali attinenti aumenterà.
Al momento delle iscrizioni, dimostra trasparenza nei riguardi degli studenti specificando quali dati personali saranno raccolti. Nello specifico, dovrai sapere perché questi dati sono necessari, per quanto tempo li conserverai e dove, e come tu e altre persone vi accederete. Se pertinente, un consenso dovrà essere richiesto, ottenuto e conservato per attestare l'autorizzazione al trattamento dei dati.
Per gli studenti che non hanno raggiunto l'età del consenso sarà necessario il consenso genitoriale. Al momento di assumere nuove personale, dovrai fornire chiare informazioni circa le modalità di trattamento dei dati.

Cose da fare

- Definisci con chiarezza la tua missione.
- Compila un elenco dei tuoi interessati.
- Stabilisci quali siano i dati personali necessari.
- Automatizza la raccolta dei dati e responsabilizzati.
- Chiarisci le clausole del GDPR nei contratti con il tuo partner di Risorse Umane e verifica il consenso e rinnova i processi, se del caso.

Gestione dei dispositivi

La sfida

Nel settore dell'istruzione vengono utilizzati dispositivi di tipo eterogeneo, distribuiti fra numerose tipologie di utenti. A titolo di esempio, pensa ai computer privati degli insegnanti, gli smartphone e i tablet degli studenti, i computer usati in classe, ma anche a dispositivi personali, applicazioni private, applicazioni e sedi cloud non monitorate, dispositivi di proprietà dei tuoi subappaltatori, chiavi USB e dossier cartacei archiviati fisicamente.

Per adempiere alle disposizioni rigorose del GDPR in materia di sicurezza dei dati personali, tutti questi dispositivi - e inoltre lo staff didattico, gli studenti e gli appaltatori - dovranno essere amministrati con coerenza.

Cose da fare

- Formula dei criteri relativamente all'uso dei dispositivi.
- Sensibilizza staff e studenti e mettili al corrente del nuovo GDPR.
- Revisiona e registra gli eventi.

I requisiti del GDPR

Il GDPR disciplina le modalità di utilizzo e di accesso ai dati.

Gestione degli utenti

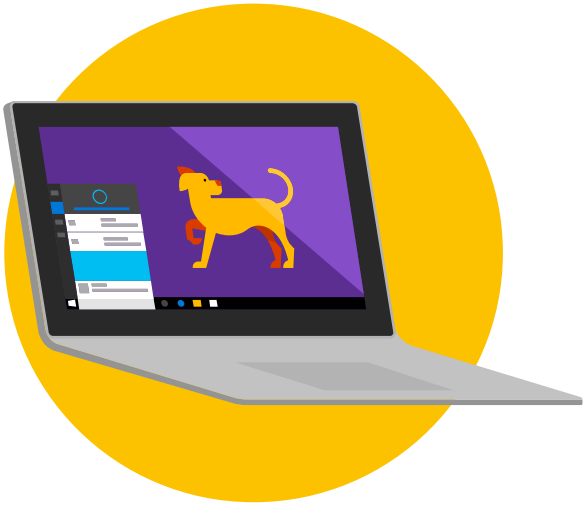
La sfida

Mentre l'iter di scoperta accresce la tua visibilità nei riguardi del database utenti, lo stadio di gestione ti aiuta a organizzare questi ultimi in liste intelligenti, impostando le autorizzazioni, stabilendo i criteri per la registrazione e tracciando l'accesso.

Quando un utente lascia la tua istituzione, il suo accesso alla totalità delle risorse scolastiche deve cessare tempestivamente, a scanso di fughe di informazioni.

Cose da fare

- Organizza gli utenti in gruppi di sicurezza.
- Definisci autorizzazioni e criteri.
- Introduci le nuove procedure.
- Sensibilizza studenti, staff e appaltatori in merito all'utilizzo corretto dei dati.



Gestione del tuo sito web

La sfida

Le attività on-line sono parte integrante degli sforzi promozionali per attirare nuovo personale e studenti. È tuo dovere garantire la sicurezza su tutte le piattaforme on-line di cui ti avvarrai.

Cose da fare

- Procedi a un audit dei dati che il tuo sito web raccoglie in modo automatico.
- Compila una lista dei tuoi cookie e di quelli di terzi.
- Verifica la totale sicurezza della modulistica on-line.
- Attesta la conformità delle procedure di consenso rispetto al GDPR.
- Crea un'informativa privacy, documentando:
  - Quali informazioni vengono raccolte
  - Chi è incaricato della loro raccolta
  - Come vengono raccolte
  - Perché vengono raccolte
  - Come saranno utilizzate
  - Con chi saranno condivise
  - Quali effetti vi saranno per i soggetti interessati
  - Se è probabile che l'uso previsto sfoci in obiezioni o reclami da parte degli interessati

Proteggere

Stabilisci controlli di sicurezza per prevenire, rilevare e reagire in caso di vulnerabilità e violazioni dei dati.

Protezione di utenti, dati e dispositivi

La sicurezza rappresenta una delle massime priorità nel nostro mondo telematizzato.

I requisiti enunciati nel GDPR per la sicurezza includono misure fisiche di protezione, sicurezza delle reti, sicurezza durante la conservazione, sicurezza dei computer, controllo di identità e accesso, crittografia e mitigazione del rischio. Esamina le prassi con cui monitori i sistemi, rilevi le violazioni e calcoli il loro impatto, e il modo in cui reagisci e ripristini la tua operatività successivamente alle situazioni problematiche.

Dati

La sfida

Il GDPR non è la meta: è un percorso di perfezionamento continuo. Esige invariabilmente da te responsabilizzazione, attivazione tempestiva e la protezione dei dati personali - a tutti gli stadi del passaggio dei dati attraverso la tua istituzione.

Cose da fare

- Crittografa dati e mail.
- Proteggi i dati sui dispositivi (MAM).
- Conserva i dati al sicuro.
- Aggiungi diritti di accesso ai singoli file e messaggi e-mail.
- Monitora intrusioni, infezioni, furti e comportamenti anomali.

Dispositivi, sedi e applicazioni

La sfida

Dispositivi e applicazioni interessano pressoché tutti gli aspetti dei tuoi dati. Possono essere parte della tua rete locale (LAN), oppure dispositivi mobili e presso altre sedi - a domicilio, sul campus, o ancora dispositivi e applicazioni cloud. Ogni dispositivo o applicazione richiede la tua attenzione specifica.

Cose da fare

- Salvaguarda la LAN con programmi antivirus, firewall e protezioni fisiche.
- Crittografa dispositivi, dischi e chiavi USB.
- Sensibilizza gli studenti e lo staff nei riguardi della migliora pratica per i loro computer privati.

I requisiti del GDPR

Il GDPR enuncia linee guida per stabilire controlli di sicurezza tesi a prevenire, rilevare e rispondere ad eventuali vulnerabilità e violazioni dei dati.

Utenti

La sfida

Quando avrai definito i tuoi utenti e li avrai classificati in gruppi di sicurezza, con tutte le autorizzazioni e i criteri del caso, potrai aggiungere misure di protezione supplementari—controllo di accesso e di identità—per risultare conforme al GDPR.

Cose da fare

- Riesamina i criteri per le password e le opzioni per la registrazione.
- Sensibilizza e promuovi la consapevolezza.

Verifiche

La sfida

Una volta attuate le misure tecniche e organizzative per proteggere i dati personali, dovrai procedere periodicamente a test, verifiche e valutazioni della loro efficacia in modo da mantenerle sempre adeguate e corrette.

Cose da fare

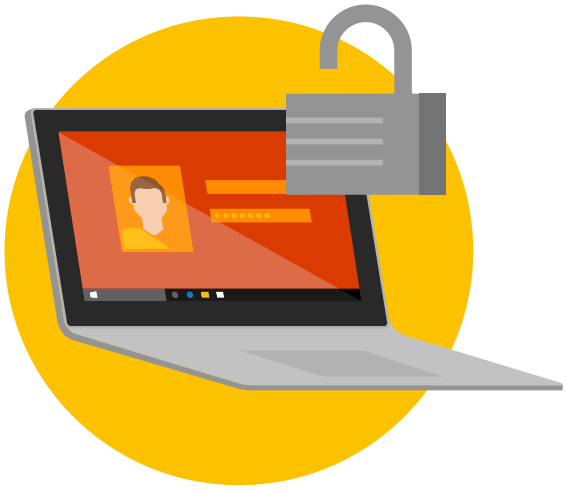
- Agevola l'esecuzione di regolari verifiche.
- Valuta l'efficacia delle misure di sicurezza.

Notificare

Rispondi alle richieste attinenti ai dati, notifica le violazioni dei dati e conserva tutta la necessaria documentazione.

Notifica degli audit e delle violazioni dei dati

Uno dei principi chiave del GDPR è la responsabilizzazione, la cosiddetta "accountability". Dovrai creare chiari iter di revisione in merito al trattamento, alle classificazioni e ai soggetti terzi che hanno accesso ai dati personali, includendovi misure di sicurezza di natura organizzativa e tecnica, e periodi di conservazione per i dati. È possibile che tu debba eseguire Valutazioni di impatto sulla protezione dei dati (DPIA).
Esse richiedono alle organizzazioni di identificare e analizzare l'impatto di un'attività di trattamento proposta sulla protezione dei dati personali.



Tracciabilità dei dati

La sfida

In base al GDPR, sei chiamato a rispondere della salvaguardia e del corretto trattamento dei dati personali. Le informazioni che registri devono specificare la natura di ogni singola richiesta avanzata da un interessato - ad esempio per visionare o rettificare i suoi dati personali - e l'esito finale di tale procedura.

Cose da fare

- Registra e conserva le richieste degli interessati, a comprova del tuo rispetto dei requisiti enunciati nel GDPR.
- Traccia e registra i flussi di dati personali dall'interno all'esterno dell'Ue e viceversa.
- Traccia e registra i dati inviati a fornitori terzi di servizi, come società informatiche o servizi educazionali.
- Mantieni aggiornati iter di revisione che dimostrino la tua conformità nei riguardi del GDPR.
- Traccia e registra i flussi dei dati personali verso fornitori di servizi terzi.
- Agevola l'esecuzione delle DPIA.

Violazioni dei dati

La sfida

Le organizzazioni dovranno notificare, entro 72 ore dal momento in cui ne vengono conoscenza, le violazioni dei dati alle autorità competenti.

Cose da fare

- Attiva registri e report.
- Rispondi entro la tempistica specificata.
- Tieni un registro separato delle modifiche apportate ai dati personali, nell'eventualità di un disastro e della necessità di ripristinarli dai file di backup.

I requisiti del GDPR

Le organizzazioni dovranno notificare, entro 72 ore dal momento in cui ne vengono conoscenza, le violazioni dei dati alle autorità competenti.

Conclusioni

La fiducia è cruciale per la missione di Microsoft: consentire a ogni persona e organizzazione di ottenere il massimo. E nelle istituzioni che preparano la prossima generazione di studenti a individuare il loro personale ruolo e contribuire attivamente allo sviluppo della società, la fiducia è un vero e proprio imperativo.

Microsoft è impegnata a dimostrare i propri principi di fiducia nel cloud, in termini di sicurezza, privacy, trasparenza e conformità. Con l'entrata in vigore del GDPR il 25 maggio 2018, l'ampia gamma di servizi cloud Microsoft affronterà le rigorose norme di sicurezza e privacy dei nostri clienti nel settore dell'istruzione, e garantirà che tu possa adempiere ai tuoi obblighi di responsabile del trattamento dei dati.

Office 365 A1, la soluzione Microsoft per la produttività cloud, è gratuita per gli utenti nel settore dell'istruzione. Fornisce strumenti essenziali per la conformità al GDPR e la tutela delle informazioni, con eDiscovery, controllo dei diritti, prevenzione della perdita dei dati, crittografia, archiviazione e-mail avanzata e conservazione delle necessarie informazioni per finalità legali. Per i clienti che richiedono funzionalità potenziate di analisi del rischio, mitigazione delle minacce, crittografia dei dati e controllo, i piani a pagamento Office 365 A3 o A5 possono supportare requisiti GDPR di tipo specifico.

Gli utenti alla ricerca di soluzioni per gestire archiviazione dati, governance e scoperta per la loro complessiva infrastruttura IT possono avvalersi di Microsoft 365 Education. Avranno un'esperienza semplice e sicura con cui amministrare utenti, dati e dispositivi da un singolo dashboard, che protegge identità, applicazioni, dati e dispositivi con sicurezza intelligente e potenziata grazie all'apprendimento automatico.

Comincia subito: lancia lo strumento GDPR Assessment e vaglia il tuo generale grado di prontezza. Se se già cliente Microsoft Cloud, ti invitiamo a utilizzare Compliance Manager per una visuale olistica della protezione dei dati e la conformità della tua organizzazione per Office 365, Dynamics 365 e Azure.

Strumenti e link correlati

Abbiamo compilato il seguente elenco di strumenti per affiancarti nel tuo viaggio verso la conformità GDPR.

Scoprire

- La funzione di Office 365 **eDiscovery avanzata** o **Ricerca contenuto** ti supporterà nella localizzazione delle informazioni correnti.
- **Etichettatura dati in Office 365** permette di classificare i dati della tua intera organizzazione ai fini della governance.
- Le liste **SharePoint** rappresentano uno strumento flessibile con cui organizzare ed etichettare i dati.
- **Gestione account utenti** di Office 365 ti aiuterà a organizzare i tuoi utenti.
- **Microsoft Intune for Education** facilita l'elencazione e la gestione di svariati dispositivi.
- **System Center** rappresenta la soluzione ideale per elencare e amministrare i server con vari sistemi operativi (OS) e soluzioni con hosting nel cloud.
- **Azure Search** ti assiste aggiungendo funzionalità di ricerca avanzata al tuo ambiente informatico esistente.
- **Azure Data Catalog** registra, rivela, comprende e consuma le fonti dei dati.
- **Cloud Discovery** analizza i tuoi registri di traffico rispetto al catalogo Cloud App Security di oltre 15.000 applicazioni cloud, ordinate e classificate in base a più di 60 fattori di rischio, per darti sempre piena visibilità sull'utilizzo del cloud, shadow IT e il rischio di quest'ultima per la tua organizzazione.
- **Advanced Data Governance** (ADG) ti aiuta a identificare, classificare e gestire automaticamente i dati personali e sensibili, e inoltre ad applicare i criteri per la conservazione e l'eliminazione delle informazioni.

Gestire

- Usa **Gruppi di sicurezza** in Office 365 e imposta un unico insieme di autorizzazioni per la totalità delle app Office 365.
- Gli **allegati intelligenti Outook** bloccano l'uscita delle informazioni dalla tua istituzione.
- Utilizza i **suggerimenti di Office 365 per le mail** ed evita gli errori più comuni.
- La **prevenzione della perdita dei dati con Office 365** impedisce che le informazioni lascino la tua sede.
- Creando **Flussi** automatizzati tra le applicazioni, potrai ottimizzare e rendere sicuri i flussi di dati.
- **IIntune for Education** facilita la gestione di procedure, applicazioni e impostazioni per i dispositivi destinati all'uso in classe.
- **Azure AD** (Azure Active Directory) è la directory cloud e il servizio di controllo identità di Microsoft.
- Serviti delle nostre **PowerApps** per creare rapidamente applicazioni mobili per l'immissione diretta nei database.
- Applica **etichette** ai dati personali e gestisci la **governance dei dati** in Office 365.
- **Azure Information Protection**: Controlla e coadiuva la sicurezza di e-mail, documenti e dati sensibili condivisi all'esterno della tua organizzazione.
- Incorporando i **moduli Microsoft** (Office 365) potrai garantire la sicurezza dell'immissione dei dati tramite la modulistica on-line e, inoltre, autorizzare richieste di consenso ottemperanti al GDPR.
- **Office 365 Teams** permette alle istituzioni di centralizzare e coordinare tutte le necessarie comunicazioni che riguardano il GDPR.

Notificare

- Il **Microsoft Trust Center** è la fonte ideale dove ricercare informazioni sul GDPR e la conformità.
- Microsoft **Compliance Manager** ti assiste nell'esecuzione delle valutazioni del rischio e semplifica l'iter di conformità, fornendoti azioni raccomandate, raccogliendo le evidenze e accertando il tuo grado di preparazione agli audit.
- Le funzionalità di **audit e registrazione in Azure** generano un registro elettronico delle attività sospette, permettendoti di rilevare i modelli potenzialmente indicativi di penetrazione esterna della rete, tentata o riuscita, e inoltre di attacchi dall'interno.
- **Securescore.office.com** è uno strumento analitico studiato per la sicurezza, con cui capirai meglio cosa hai fatto per ridurre il rischio riguardo ai tuoi dati in Office 365. Inoltre, ti mostrerà come meglio procedere per mitigare ulteriormente tale rischio. Rappresenta la fonte di consultazione ottimale per quanto concerne revisioni, registrazioni e molte altre funzionalità di Office 365.
- Il **registro audit unificato** fornisce informazioni in merito ai dati trasferiti a terzi.

Nota: L'elenco non include la totalità degli strumenti e dei servizi Microsoft a sostegno dei quattro stadi chiave illustrati in questa sede. Per una panoramica completa sul ruolo di tutti i servizi e i prodotti Microsoft Cloud nel supportare la conformità dei clienti per il GDPR, scarica l'e-book Accelera il percorso verso la conformità al GDPR con Microsoft Cloud

Proteggere

- **Office 365 (A3)** e la sua **Prevenzione della perdita dei dati** consentono di creare regole per bloccare l'uscita dalla tua sede di determinate tipologie di informazioni selezionati di lasciare la tua sede.
- **Azure Information Protection**: Controlla e coadiuva la sicurezza di e-mail, documenti e dati sensibili condivisi all'esterno della tua organizzazione. Da facili classificazioni a etichette e autorizzazioni embedded, Azure Information Protection potenzia invariabilmente la tutela dei dati, ovunque si trovino o con chiunque vengano condivisi.
- **Customer Lockbox** permette ai titolari del trattamento di comprovare le loro procedure esplicite per l'accesso ai contenuti dei clienti, durante la prestazione dei servizi.
- **AppLocker** assiste gli amministratori al momento di creare e implementare criteri di controllo per le applicazioni, nonché limitare l'accesso non autorizzato alle applicazioni in grado di mettere a repentaglio i dati personali.
- **Microsoft Advanced Threat Analytics (ATA)** è una piattaforma installata in loco che aiuta la tua scuola a tutelarsi da varie tipologie di attacchi mirati e avanzati - ad opera di ciber-criminali, o provenienti dall'interno.
- **Office 365 Threat Intelligence.**
- **IIntune for Education** è una soluzione semplice ma potente per l'attuazione delle procedure di sicurezza, e inoltre di applicazioni e impostazioni per i dispositivi usati in classe.
- **Windows Defender Advanced Threat Protection**, disponibile in Windows 10 Education, è un servizio di sicurezza con cui i clienti aziendali possono rilevare, indagare e rispondere a minacce di livello avanzato sulle loro reti.
- **Azure Backup e Azure Disaster Recovery** incrementano la disponibilità.
- La funzionalità **BitLocker per crittografia dei drive** protegge i dati e si integra con il tuo sistema operativo, affrontando le minacce dei furti di dati o l'esposizione in caso di smarrimento, furto o smaltimento inidoneo dei computer.
- Usa l'**Autenticazione multifattoriale** in Office 365 e Windows 10 con Windows Hello.

Il presente e-book è un commento sul GDPR basato sulla sua interpretazione da parte di Microsoft alla data di pubblicazione. Microsoft ha esaminato e analizzato in dettaglio il nuovo Regolamento, e ritiene di aver espresso in modo meditato i suoi intenti e il suo significato. L'applicazione del GDPR, tuttavia, è di natura altamente specifica e, inoltre, non tutti gli aspetti e le interpretazioni della normativa sono definiti in modo chiaro.

Di conseguenza, questo e-book viene fornito unicamente a titolo informativo. Gli utenti non devono affidarsi alla presente pubblicazione quale consulenza legale, ovvero al momento di stabilire la potenziale applicabilità del GDPR alle loro personali circostanze e organizzazioni. Si invita l'utente a consultare un professionista qualificato per discutere del GDPR, della sua specifica applicabilità alla sua organizzazione, e di come meglio garantire la conformità.

MICROSOFT NON AVANZA ALCUNA GARANZIA, ESPLICITA, IMPLICITA O PRESCRITTA DALLA LEGGE, RELATIVAMENTE ALLE INFORMAZIONI CONTENUTE IN QUESTO E-BOOK. Il presente e-book viene fornito "così com'è". Le informazioni e opinioni riportate in questo documento, inclusi URL e riferimenti ad altri siti Internet, sono salvo modifiche senza preavviso.

Data di pubblicazione: marzo 2018 Versione 1.0